Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Le Conseil fédéral

La responsabilité civile des fournisseurs de services Internet

Rapport du Conseil fédéral du 11 décembre 2015

Condensé

La jurisprudence ne s'est pas encore penchée sur tous les aspects de la responsabilité civile des fournisseurs Internet (que nous désignerons simplement par le terme de « fournisseurs » dans la suite de ce rapport). Quant à la doctrine, elle est partagée sur de nombreux points qu'elle n'a cependant pas encore tous examinés de manière approfondie. L'objectif principal du présent rapport est donc de dresser un état des lieux du droit applicable aujourd'hui. Cette réflexion s'articule autour de trois axes: les actions défensives (action en suppression et en cessation de l'atteinte, action en constatation, etc.; voir ch. 3), les actions réparatrices (dommages-intérêts, réparation du tort moral, etc.; voir ch. 4) et les droits à l'information (ch. 5). La part du lion revient au type d'action le plus important dans la pratique, l'action défensive. Un bref chapitre se penche sur l'exécution des décisions sur les plans national et international (ch. 6). Le rapport se referme sur une appréciation générale de la situation juridique actuelle et sur les perspectives d'évolution du droit (ch. 7).

Actions défensives

Dans ce qui est a priori encore le seul arrêt rendu par la plus haute instance judiciaire du pays en matière de responsabilité d'un fournisseur (arrêt Tribune de Genève), le Tribunal fédéral a conclu qu'il était possible d'introduire une action en cessation de l'atteinte contre l'hébergeur d'un blog (dans le cas d'espèce, la Tribune de Genève) même si celui-ci ne savait rien des contenus illicites (légitimation passive). Dans leurs motivations, les juges suprêmes se sont fondés sur l'art. 28, al. 1, CC selon lequel toute personne ayant participé à une atteinte à la personnalité peut être poursuivie. Pour le reste, ils ont estimé qu'il appartenait au législateur de réparer les conséquences que l'application du droit actuel pourrait avoir pour Internet et pour les hébergeurs de blogs. Cette décision a été reçue fraîchement par la doctrine. Les auteurs ont certes approuvé l'action en cessation de l'atteinte contre la Tribune de Genève. Ils ont toutefois critiqué le fait que, en admettant globalement la légitimation passive de tous les participants à une atteinte à la personnalité, le Tribunal fédéral n'ait pas posé de limites. Ils ont aussi jeté un regard critique sur le fait qu'une partie des frais ait été mise à la charge de l'hébergeur du blog alors que celui-ci n'avait a priori pas été mis en demeure au préalable et n'avait donc pas eu la possibilité de reconnaître le bien-fondé de la demande volontairement.

La portée de cet arrêt (qui n'a pas été publié dans le Recueil officiel des arrêts du Tribunal fédéral) et sa transposabilité à d'autres domaines du droit que celui du droit de la protection de la personnalité doivent encore être clarifiées. Il apparaît que le champ d'application personnel de la légitimation passive, en matière d'action défensive, est au moins aussi large dans le domaine du droit de la concurrence et du droit de la propriété intellectuelle que dans celui du droit de la personnalité et de la protection des données.

Le droit en vigueur offre aux tribunaux les instruments nécessaires pour restreindre l'étendue de la légitimation passive à un cercle de personnes correspondant à ce qui est souhaitable. Les mesures provisionnelles, notamment, doivent tenir compte du principe de proportionnalité. L'exigence d'un lien de causalité adéquate pourrait aussi être utilisée comme critère pour limiter le champ de la légitimation passive.

Le Conseil fédéral a rejeté l'idée de restreindre légalement la légitimation passive de certaines catégories de fournisseurs, en raison de la difficulté d'englober dans une seule norme les nombreux cas de figure techniques possibles et en constante évolution.

Actions réparatrices

Les actions réparatrices, en plus des aspects de l'illicéité et de la causalité déjà examinés dans le cadre des actions défensives, doivent répondre aux critères de la faute et du dommage. Un élément central, pour élever des prétentions à l'égard d'un fournisseur, est de savoir s'il a agi intentionnellement ou par négligence, autrement dit si l'on peut lui reprocher une violation de son devoir de diligence. Même s'il n'est pas toujours aisé de répondre à ces questions, cette tâche doit demeurer du ressort des tribunaux. Cette difficulté se pose d'ailleurs dans bien d'autres domaines.

Inversement, la codification d'un système de notification et de retrait de contenu illicite ou la définition d'une règle d'exclusion de la responsabilité pourraient avoir des effets pervers: les (petits) fournisseurs ne disposent généralement pas des connaissances juridiques permettant d'effectuer une appréciation juridique de l'atteinte. Ainsi, il est à craindre qu'ils pèchent par excès de zèle en supprimant des contenus à tout-va, avec les répercussions que l'on imagine sur la liberté d'expression des utilisateurs. Par ailleurs, en cas d'exclusion de la responsabilité, ils n'auraient plus d'incitation à développer et à mettre en œuvre des améliorations techniques pour empêcher les atteintes manifestes. Pour le Conseil fédéral, il n'y a donc pas besoin de légiférer en matière d'action réparatrice. La diligence requise est une question qui doit être appréciée par les tribunaux dans chaque cas d'espèce et qui ne se prête pas à une normalisation légale. Les principes décrits dans le rapport peuvent être utiles pour l'appréciation concrète des cas d'espèce.

Droits à l'information

L'examen des droits à l'information à l'égard des fournisseurs vise à déterminer si et, si oui, à quelles conditions une personne ayant subi une atteinte peut exiger que le fournisseur révèle le nom du titulaire d'une adresse IP par l'intermédiaire de laquelle un acte illicite a été commis. À défaut d'une « action contre inconnu » en droit civil, cette identification est la condition sine qua non pour pouvoir remonter à l'auteur de l'atteinte. Or, le code civil ne connaît pas ce type de droit à l'information pour le moment. C'est pourquoi la procédure pénale revêt un rôle central puisque, à l'inverse de la procédure civile, elle peut être ouverte contre un auteur inconnu. Ainsi, dans certaines circonstances, le droit pénal est utilisé pour déterminer l'identité de l'auteur avant d'agir contre lui dans le cadre d'une procédure civile. La question de savoir si cette démarche est encore possible après la jurisprudence Logistep du Tribunal fédéral (ATF 136 II 508) est controversée et n'a pas encore obtenu de réponse de la part des juges suprêmes.

Par ailleurs, les données ne peuvent être fournies que si elles sont conservées en quantité et pour une durée suffisantes. La question de la conservation et de la durée de conservation des adresses IP pouvant servir à identifier les titulaires d'une connexion à Internet est un point délicat au regard de la protection des données.

Aujourd'hui, il faut qu'un comportement soit répréhensible sur le plan pénal pour justifier la levée du secret des télécommunications, soit de l'anonymat sur Internet. Le Conseil fédéral estime que cette pesée d'intérêts doit être maintenue, sinon l'on risquerait de perdre une ligne directrice claire et de vider le secret des télécommunications de sa substance. Il faut donc renoncer a priori à l'introduction d'un instrument supplémentaire relevant du droit civil. Les

règles spéciales dans le domaine du droit d'auteur, qui sont élaborées dans le cadre des travaux consécutifs au rapport de l'AGUR12, ne sont pas abordées dans le présent rapport.

Exécution des décisions

Les règles du code de procédure civile ne soulèvent en principe pas de problèmes d'application particuliers par rapport à la situation spécifique des fournisseurs. À propos de l'arrêt Tribune de Genève du Tribunal fédéral, quelques auteurs ont tout de même critiqué le fait qu'une partie des frais ait été mise à la charge de l'hébergeur du blog, alors qu'il n'est pas établi clairement s'il avait été mis en demeure ou pas. Avant l'unification de la procédure civile au niveau fédéral, plusieurs codes de procédure cantonaux contenaient des dispositions selon lesquelles les frais devaient être mis à la charge du demandeur lorsque la demande n'avait pas été provoquée par l'attitude du défendeur et que celui-ci en reconnaissait immédiatement le bien-fondé. Le législateur fédéral a cependant renoncé à introduire cette règle dans le code de procédure civile. En vertu de l'art. 107, al. 1, let. b, e et f, de ce dernier, les tribunaux ont toutefois la possibilité de répartir les frais selon leur libre appréciation et, par exemple, de les mettre à la charge du demandeur qui a eu gain de cause mais qui aurait omis de mettre en demeure le défendeur avant d'introduire l'action. Cette règle permet de tenir compte adéquatement des circonstances particulières du cas d'espèce. En revanche, une nouvelle norme spéciale selon laquelle les frais devraient être mis à la charge du demandeur s'il n'a pas mis en demeure le fournisseur et si ce dernier a immédiatement reconnu le bien-fondé de la demande, ne semble pas appropriée. De toute manière, la question de la répartition des frais sera abordée à une plus large échelle dans le cadre de la prochaine évaluation globale du code de procédure civile.

Les dispositions du droit suisse en matière de for et de droit applicable dans les affaires internationales paraissent adéquates. L'exécution des décisions à l'étranger demeure certes fréquemment source de difficultés, mais ces problèmes sont de nature générale et ne sauraient être résolus au moyen d'une règlementation unilatérale de la Suisse. La voie des traités d'entraide judiciaire est plus pertinente. Il est par exemple possible d'y convenir de la transmission directe par voie postale des actes devant être notifiés à l'étranger, ce qui accélère sensiblement les procédures civiles. Des traités de ce type ont déjà été conclus avec quelques États qui accueillent le siège social d'exploitants de plateformes bien connus. En outre, la Suisse est en négociation avec l'UE et les autres États parties à la Convention de Lugano au sujet d'un éventuel traité parallèle au règlement européen sur la signification et la notification des actes, lequel prévoit aussi la transmission des actes par voie postale. Dans ces circonstances, il est actuellement préférable de s'abstenir de développer unilatéralement une législation propre à la Suisse.

Appréciation générale

Les conclusions du présent rapport tendent à montrer qu'une législation générale, couvrant tous les domaines du droit, ne s'impose pas pour le moment en matière de responsabilité civile des fournisseurs. Le rapport du Conseil fédéral, qui procède à un examen détaillé de la situation juridique et de la jurisprudence et qui en tire des conclusions, contribuera toutefois à l'évolution du droit et, par conséquent, à l'amélioration de la sécurité juridique.

Table des matières

Table des matières détaillée

1 Introduction

1.1 Mandat

A l'occasion de l'adoption du rapport « Cadre juridique pour les médias sociaux »[1], le Conseil fédéral a chargé le Département fédéral de justice et police (DFJP), le 9 octobre 2013, de voir s'il convient de légiférer sur la responsabilité civile des fournisseurs de services Internet et, si tel est le cas, de préparer un projet de consultation avant la fin 2015. Par la décision du Conseil fédéral du 6 juin 2014, le DFJP a en outre été invité à mettre en œuvre les propositions du groupe de travail chargé d'améliorer la gestion collective des droits d'auteur et des droits voisins (AGUR12), quoique sous réserve de la coordination avec les travaux en cours portant sur la responsabilité civile générale des exploitants de plateformes et des fournisseurs.

Pour répondre au premier mandat mentionné, un groupe de travail interdépartemental a été mis sur pied sous l'égide de l'Office fédéral de la justice (OFJ), avec des représentants de l'Office fédéral de la communication (OFCOM), de l'Institut fédéral de la propriété intellectuelle (IPI) et du Secrétariat d'Etat à l'économie (SECO). Le présent rapport se fonde sur les travaux de ces experts.

1.2 Objet et but

Le présent rapport repose sur une compréhension de la « responsabilité civile » au sens large. Il se penche aussi bien sur des actions défensives (action en suppression et en cessation de l'atteinte, action en constatation, etc.) que sur les actions réparatrices (dommages-intérêts, réparation du tort moral, remise du gain, publication de jugements, etc.) et les droits à l'information. Toutes les dispositions légales du droit suisse énonçant des exigences de ce type ont été prises en compte (par ex. le code civil [CC][2], le code des obligations [CO][3], la loi fédérale du 19 juin 1992 sur la protection des données [LPD][4], la loi du 9 octobre 1992 sur le droit d'auteur [LDA][5], la loi du 28 août 1992 sur la protection des marques [LPM][6] et la loi fédérale du 19 décembre 1986 contre la concurrence déloyale [LCD][7]). Par souci de simplification, l'objet du rapport sera désigné ci-après par « responsabilité des fournisseurs ».

Les prétentions contractuelles ne sont pas traitées ici, car elles ne soulèvent pas de problèmes particuliers, pour autant qu'on puisse en juger[8]. L'éventuelle responsabilité pénale des fournisseurs n'est pas non plus abordée. Le droit pénal est toutefois évoqué là où il permet une meilleure compréhension de la situation juridique en droit civil.

Le présent rapport a pour but de déterminer s'il y a lieu de légiférer dans le domaine de la responsabilité civile des fournisseurs. A cet effet, dans un premier temps, la situation juridique

---

1 Rapport du Conseil fédéral en réponse au postulat Amherd 11.3912 du 29.9.2011 « Cadre juridique pour les médias sociaux » de l'automne 2013, à consulter sous: www.bakom.admin.ch > Thèmes > Société de l'information > Rapports et publications.
2 RS 210.
3 RS 220.
4 RS 235.1.
5 RS 231.1.
6 RS 232.11.
7 RS 241.
8 On notera que des prétentions contractuelles peuvent naître d'autres prétentions relevant de la responsabilité délictuelle (par ex. un fournisseur qui, sur demande d'un tiers lésé, supprime des contenus viole par là même, dans certaines circonstances, le contrat qui le lie à ses clients).

actuelle en Suisse[9] est décrite, telle qu'elle ressort de la doctrine et de la jurisprudence, dans la mesure où ces dernières ont abordé la question. Suit un examen de la situation juridique et des perspectives d'évolution du droit[10]. Il en ressort, pour terminer, la conclusion du Conseil fédéral selon laquelle il n'y a pas lieu de légiférer, si l'on met à part le projet de modernisation du droit d'auteur. La situation juridique en Europe et aux Etats-Unis est prise en compte sous la forme d'une comparaison des différentes législations.

1.3 Objectifs d'une règlementation en matière de responsabilité des fournisseurs

1.3.1 Introduction

Une règlementation de la responsabilité des fournisseurs devrait permettre que les parties prenantes puissent faire valoir leurs droits efficacement et reconnaître de manière suffisante quelles sont leurs obligations. A cet égard, l'Etat se trouve face à la mission ambitieuse de trouver un équilibre entre les intérêts des personnes (potentiellement) lésées par la communication en ligne, afin qu'elles puissent faire valoir efficacement leurs droits, et les intérêts des parties prenantes à la communication (les fournisseurs et leurs clients). Tous les participants peuvent invoquer des droits fondamentaux, qui doivent être sauvegardés dans toute la mesure du possible et pondérés les uns par rapport aux autres. Ce faisant, il faut également respecter les directives contraignantes du droit international[11].

Etant donné que la communication dépasse les frontières, il existe un certain intérêt à ce que la règlementation ne diverge pas outre mesure des prescriptions applicables à l'étranger, et ce pour des motifs économiques autant que dans l'optique des personnes lésées. De plus, il est dans l'intérêt de tous que la situation juridique soit la plus claire possible. La sécurité juridique n'est pas utile uniquement à ceux qui sont en proie à un conflit concret, mais aussi aux autorités judiciaires appelées à établir la jurisprudence et, de façon générale, elle sert les intérêts du site économique et de l'espace de vie qu'est la Suisse[12].

1.3.2 Sauvegarde des droits (fondamentaux) des parties prenantes

a) Droits de la personnalité et droits à la protection des données des personnes lésées

Lors de la communication en ligne, les intérêts individuels des personnes concernées peuvent être touchés de nombreuses manières. Il convient de noter que la communication en ligne risque bien plus que les médias traditionnels de porter atteinte à la sphère privée (notamment en raison de la capacité accrue à emmagasiner et à diffuser l'information)[13]. On citera à titre d'exemple l'atteinte aux intérêts individuels par les exploitants de plateformes de médias sociaux et par des tiers[14]. On mentionnera notamment les atteintes à la protection des données

---

9 Ch. 3 ss.
10 Ch. 7.
11 Voir ch. 1.3.2.
12 Voir ch. 1.3.3.
13 Cour EDH, 5.5.2011, n° 33014/05, Comité de rédaction de *Pravoye Delo* et Shtekel c. Ukraine, ch. 63, consultable sous : hudoc.echr.coe.int/fre.
14 Pour plus de détails, voir le rapport du Conseil fédéral « Cadre juridique pour les médias sociaux » (note 1), 20 ss.

et à la personnalité (c'est-à-dire, outre les atteintes à l'honneur, par ex. la cyberintimidation et le cyberharcèlement, ainsi que les atteintes à l'intégrité sexuelle).

Ces positions juridiques sont protégées non seulement par le droit civil (par ex. art. 28 CC) et le droit pénal, mais aussi par des droits fondamentaux spécifiques (par ex. art. 10 et 13 de la Constitution [Cst.][15]). L'Etat a en particulier le devoir de fournir aux personnes concernées des moyens légaux suffisants pour la protection de leur droit au respect de la vie privée et familiale (art. 8 de la Convention du 4 novembre 1950 de sauvegarde des droits de l'homme et des libertés fondamentales [CEDH][16]). Même si seul l'Etat est directement tenu de respecter les droits fondamentaux, ceux-ci doivent être réalisés dans l'ensemble de l'ordre juridique (art. 35, al. 1, Cst.). Les autorités étatiques doivent veiller à ce qu'ils soient aussi réalisés dans les relations qui lient les particuliers entre eux, dans la mesure où ils s'y prêtent (art. 35, al. 3, Cst.).

Ainsi, la Cour européenne des droits de l'homme (Cour EDH) demande que l'Etat prenne des mesures suffisantes pour remédier aux atteintes graves aux intérêts individuels. Les devoirs des Etats concernent non seulement l'application et l'imposition du droit au cas par cas, mais aussi la création de règles de droit qui permettent d'assurer une protection des droits de la personnalité qui soit efficace dans la pratique. C'est pourquoi la Cour EDH a critiqué la situation juridique en Moldavie, où le code civil ne prévoit aucun dédommagement approprié, même en cas d'atteintes particulièrement graves à la sphère privée (par ex. par la publication de séquences vidéo filmées dans un sauna à l'insu des participantes)[17]. De la même manière, le législateur finlandais a été réprimandé pour avoir omis d'édicter une législation efficace afin de protéger la sphère privée, puisqu'un fournisseur n'a pas pu être contraint de communiquer les données d'un inconnu qui avait publié une annonce choquante sur un site de rencontre en ligne au nom d'un garçon de douze ans[18].

b) Liberté économique et droits de propriété des personnes lésées

Il convient également de tenir compte de la liberté économique et des droits de propriété, qui sont notamment protégés par la LCD et le droit d'auteur[19].

Dans ces domaines également, les Etats ont un devoir de protection. Le droit à la propriété et le droit à la liberté économique sont garantis par les art. 26 et 27 Cst. Outre la protection offerte par la Constitution, la Cour EDH reconnaît également que la propriété intellectuelle dans le cadre de la protection de la propriété (premier Protocole additionnel à la CEDH, qui n'a pas été ratifié par la Suisse) est garantie et que les Etats parties à la CEDH ont certaines obligations de protection à cet égard[20].

---

15 RS 101.
16 RS 0.101.
17 Cour EDH, 5.7.2011, n° 41588/05, Avram c. Moldavie.
18 Cour EDH, 2.12.2008, n° 2872/02, K.U. c. Finlande.
19 Pour des informations détaillées, voir le rapport final de l'AGUR12 de novembre 2013, qui peut être consulté à l'adresse www.ipi.ch > Droit d'auteur > AGUR12.
20 Cour EDH, 19.2.2013, n° 40397/12, Neij et Peter Sunde Kolmisoppi c. Suède (Pirate Bay).

c) Liberté d'expression et d'information de tiers et liberté économique des fournisseurs

Lorsqu'on fait respecter les droits des particuliers et entreprises lésés, il convient de garder à l'esprit les droits de l'homme de la partie adverse, à savoir la liberté d'expression (art. 16 Cst. et art. 10 CEDH) et la liberté économique (art. 27 Cst.).

Internet joue un rôle central dans la promotion de la liberté d'opinion[21]. La liberté d'opinion est garantie par l'art. 16 Cst., l'art. 10 CEDH et l'art. 19 du Pacte international du 16 décembre 1966 relatif aux droits civils et politiques[22]. Le champ de protection de ces droits se recoupe dans une large mesure[23] et englobe aussi bien la liberté d'exprimer son opinion que le droit d'accéder à l'information permettant de se forger une opinion[24]. La Cour européenne a déjà eu à plusieurs reprises l'occasion de se prononcer sur la portée de la liberté d'opinion en lien avec les obligations des fournisseurs et sur d'autres questions apparentées. Sa jurisprudence est donc mentionnée dans le présent rapport en différents endroits[25].

Les droits fondamentaux des fournisseurs et de leur clientèle peuvent certes être restreints afin de protéger des droits individuels d'autrui, mais dans le respect de la proportionnalité. Ainsi, la Cour EDH considère que ce serait aller trop loin que d'introduire une obligation légale étendue de notification préalable des personnes concernées par une publication envisagée[26]. Un problème essentiel pour la Cour est le fait qu'une obligation de ce type n'affecterait pas que des publications contraires au droit, mais aussi, inévitablement, des communications conformes au droit – y compris des rapports politiques, auxquels la jurisprudence de Strasbourg reconnaît un degré de protection particulier[27].

Cette réflexion peut revêtir un caractère général: les mesures de précaution visant à protéger les personnes lésées contre des atteintes à leurs droits ne devraient pas conduire à ce que, par crainte d'éventuels désavantages (par ex. juridiques ou financiers), on renonce à une communication conforme au droit. Dans ce contexte, on prendra également en considération l'interdiction de la censure prévue par le droit constitutionnel (art. 17, al. 2, Cst.). Elle interdit non seulement à l'Etat de mettre en place son propre système de censure, mais lui impose également une certaine retenue lorsqu'il impose des obligations aux particuliers. Ainsi, il peut y avoir atteinte indirecte à la liberté des médias lorsque des particuliers (par ex. un éditeur ou un fournisseur d'hébergement) doivent *de facto* exercer une censure pour ne pas être tenus pour responsables d'avoir omis de procéder aux contrôles requis par l'Etat[28].

Dans la perspective des droits fondamentaux, une surveillance par les fournisseurs peut être délicate, en particulier s'il se peut que des publications conformes au droit soient interdites par intérêt personnel ou en raison de précautions excessives. La Cour EDH l'a affirmé en lien avec les interventions de propriétaires ou d'éditeurs dans les processus de publication. L'Etat ne

---

[21] Cour EDH, 10.3.2009, n° 3002/0323676/03 et 3002/0323676/03, Times Newspapers Ltd c. Royaume-Uni, ch. 27.

[22] Approuvé par l'Assemblée fédérale le 13.12.1991; RS 0.103.2.

[23] Il existe une différence en ce qui concerne les déclarations en lien avec l'économie, évoquées à l'art. 27 Cst., et qui sont toutefois également garanties par la CEDH à l'art. 10, cf. *Kley/Tophinke*, St. Galler Kommentar, ad art. 16 n° 7.

[24] Voir ATF 130 I 369 consid. 2.

[25] Voir ch. 3.2.6 b) et dd), ch. 4.2 et ch. 5.2.

[26] Cour EDH, 10.5.2011, n° 48009/08, Mosley c. Royaume-Uni.

[27] Cour EDH, 11.3.2014, n° 20877/10, Yaman Akdeniz c. Turquie, ch. 28.

[28] Sur l'effet horizontal indirect de l'interdiction de la censure entre particuliers, voir notamment *Krüsi,* 279 ss, en particulier 282 s.

doit pas concevoir les règles en matière de responsabilité civile ou pénale de manière à ce qu'elles favorisent la censure privée.

> « De manière bien compréhensible, les éditeurs sont motivés par des considérations de profit, et l'engagement de leur responsabilité quant au contenu de leurs publications entraîne souvent une ingérence patrimoniale dans le processus éditorial. Afin de permettre à la presse d'exercer sa fonction de "chien de garde", il est important que les normes de responsabilité des maisons d'édition en matière de publications soient telles qu'elles n'incitent pas les éditeurs à censurer ce qu'ils publient. La considération de l'effet dissuasif liée à la responsabilité revêt une certaine pertinence s'agissant de trouver la juste norme en la matière. »[29]

Ces principes revêtent une importance particulière dans le domaine des publications en ligne. Selon la déclaration commune de 2011 des trois rapporteurs spéciaux pour la liberté d'expression de l'Organisation des Nations Unies, de l'Organisation pour la sécurité et la coopération en Europe et de l'Organisation des Etats Américains[30], une règlementation légale tenant compte du caractère particulier d'Internet est nécessaire. Selon les rapporteurs spéciaux, nul ne doit être tenu pour responsable sur le plan légal pour les contenus produits par des tiers sur Internet, à moins qu'il ne se soit approprié le contenu concerné ou qu'il ait omis d'obéir à une injonction de retrait d'un tribunal.

De l'avis de la Cour européenne, les Etats sont tenus de jouer un rôle actif dans la règlementation des responsabilités sur Internet. Ils doivent instaurer un cadre légal suffisant, qui décrive de manière suffisante les limites de ce qui est permis (par ex. restitution de propos de source étrangère), de manière à ce que les auteurs de contributions (par ex. journalistes ou blogueurs) puissent s'exprimer sans crainte[31]. Elle demande également une définition suffisamment précise et offrant la plus grande sécurité juridique possible en ce qui concerne la responsabilité des fournisseurs, des exploitants de moteurs de recherche ou des personnes mettant des liens sur leurs pages.

1.3.3 Besoin de sécurité juridique de la société de l'information

Les acteurs de la communication et les personnes concernées par la communication en ligne ne sont pas les seuls à avoir besoin d'une règlementation qui offre une sécurité juridique et soit harmonisée au niveau international. C'est un enjeu de taille pour la société tout entière.

La Stratégie du Conseil fédéral de 2012 pour une société de l'information en Suisse[32] souligne l'importance des technologies de l'information et de la communication pour la place économique et l'espace de vie qu'est la Suisse. Il faut notamment, sur le plan juridique, des conditions cadres propices, qui favorisent les investissements. Les particuliers aussi bien que les entreprises doivent pouvoir utiliser Internet de manière responsable, en ayant conscience des aspects sécuritaires, et se prémunir contre les dangers d'Internet. Pour y parvenir, il

---

[29] Cour EDH, 3.12.2013, n° 64520/10, Ungváry et Irodalom KfT c. Hongrie, ch. 74.

[30] Voir Déclaration commune sur la liberté d'expression et d'Internet, consultable sous www.osce.org/fom/78309 et le résumé en français sous merlin.obs.coe.int/iris/2011/8/article2.fr.html.

[31] Cour EDH, 5.5.2011, n° 33014/05 Comité de rédaction de *Pravoye Delo* et Shtekel c. Ukraine, ch. 64.

[32] A consulter sous: www.bakom.admin.ch > Thèmes > Société de l'information.

convient de définir le plus clairement possible les responsabilités, les droits existants et leur mise en œuvre.

2 Définitions (personnes concernées par la responsabilité des fournisseurs)

2.1 Remarques préliminaires

Pour la règlementation des obligations dans la communication en ligne, le rôle joué par les parties prenantes est essentiel. Dans un souci de simplification, on retiendra les principes suivants: plus un acteur peut, par son activité, influer sur les contenus, plus il faudra lui reconnaître une responsabilité juridique en cas de diffusion de contenus illicites.

Les catégories en question n'ont, pour autant qu'on puisse en juger, pas (encore) été définies de manière générale et contraignante en droit suisse. Cependant, il existe différentes approches de description abstraite des rôles, qu'on trouve dans des rapports officiels, des projets de lois, des actes législatifs internationaux et des décisions judiciaires, ainsi que dans la doctrine.

2.2 Tentatives de définition des termes par le passé

La responsabilité pénale et civile des fournisseurs a déjà été abordée dans différents rapports officiels et projets de loi. Les définitions de termes qui y sont proposées peuvent servir ici de point de départ.

2.2.1 Commission d'experts Cybercriminalité

a) Catégories d'acteurs de la communication en réseau selon le rapport

Le rapport de la commission d'experts « Cybercriminalité » du DFJP de juin 2003 contient une classification des différents acteurs de la communication en ligne. En se basant sur l'exemple du world wide web (WWW), le rapport cite les acteurs suivants aux pages 29 ss.[33]:

- **Le fournisseur de contenus (*content provider*):** il diffuse sur Internet ses propres contenus ou des contenus repris de tiers et utilise son propre serveur ou celui d'un fournisseur d'hébergement.
- **Le fournisseur d'hébergement de sites (*hosting provider*):** il met à la disposition des fournisseurs de contenus un serveur web, sur lequel ces derniers peuvent offrir leurs propres sites. Selon les possibilités, en ayant accès à une page web, le client peut aussi mettre à exécution ses propres programmes, qu'il y a hébergés. En fonction des circonstances, le fournisseur d'hébergement offre de l'espace à d'autres services, par ex. la messagerie électronique. Cette dernière prestation se caractérise par le fait que d'ordinaire, le fournisseur d'hébergement ne participe pas à la sauvegarde

[33] Le rapport peut être consulté sous: www.ofj.admin.ch > Sécurité > Projets législatifs en cours > Projets législatifs terminés > Cybercriminalité.

d'informations sur son serveur. Il s'agit de déroulements de programme automatisés que seul le fournisseur de contenus ordonne ou contrôle.

- **Le fournisseur de réseaux (*network provider*):** grâce à son réseau de communication, le fournisseur de réseaux est relié avec divers fournisseurs d'accès, d'autres fournisseurs de réseaux ainsi qu'avec de gros clients potentiels qui n'ont pas besoin d'un propre fournisseur d'accès. Le transport des données se fait par l'intermédiaire de ces réseaux; il repose également sur l'automatisation des programmes.
- **Le fournisseur d'accès (*access provider*):** il permet aux utilisateurs finaux ou aux entreprises d'accéder à Internet par l'intermédiaire du téléphone ou par un accès à large bande (ADSL, Cablemodem, Wireless Local Loop, Satellit, ligne louée, etc.). En général, le fournisseur d'accès alloue dynamiquement à l'utilisateur final une adresse Internet qui n'est pas permanente. Les entreprises et les utilisateurs finaux qui veulent aussi fournir des contenus reçoivent toutefois d'ordinaire une adresse ou un bloc d'adresses fixes à partir du domaine d'adresses que gère le fournisseur d'accès. Ces processus se déroulent également de manière automatique, c'est-à-dire sans intervention manuelle du fournisseur d'accès.

b) Définitions dans l'avant-projet de modification du code pénal [CP][34] de 2004

L'avant-projet de modification du code pénal concernant la responsabilité pénale des prestataires en matière d'infractions commises par le canal des médias électroniques (cybercriminalité) (AP-CP)[35], mis en consultation en octobre 2004 et qui reposait sur le rapport de la commission d'experts Cybercriminalité, proposait des définitions légales des rôles principaux dans le CP:

- **Fournisseurs d'hébergement et exploitants de moteurs de recherche (art. 27, al. 3, AP-CP):** un fournisseur d'hébergement est « *la personne qui aura mis à disposition, selon un procédé automatisé, des informations d'autrui sur un réseau de communications électroniques* » (1re phrase).

  La 2e phrase assimilait les exploitants de moteurs de recherche (comme Google) aux fournisseurs d'hébergement sur le plan du droit pénal: « *La mise à disposition d'un répertoire intégrant des informations d'autrui selon un procédé automatisé est considérée comme mise à disposition d'informations d'autrui.* »

- **Fournisseur d'accès (art. 27, al. 4, AP-CP: simple fourniture d'accès)**: celui « *qui se borne à fournir l'accès à un réseau de communications électroniques* » ne devait pas être punissable. La 2e phrase assimilait à la simple fourniture d'accès le stockage intermédiaire temporaire exigé par des impératifs techniques (dit *« caching »*): « *Le stockage automatique et temporaire d'informations d'autrui suite à la consultation d'un site est considéré comme une fourniture d'accès.* »

Les travaux sur l'avant-projet de loi n'ont pas été poursuivis, car le Conseil fédéral, une fois la consultation achevée, était parvenu à la conclusion que la règlementation générale en vigueur portant sur la responsabilité pénale des fournisseurs suffisait pour combattre efficacement la

[34] RS 311.0.

[35] L'avant-projet de loi peut être consulté sous: www.ofj.admin.ch > Sécurité > Projets législatifs en cours > Projets législatifs terminés > Cybercriminalité.

cybercriminalité[36]. Selon lui, la législation en vigueur, sur la base du droit pénal des médias et des principes généraux concernant l'auteur d'une infraction et la participation, permettait de poursuivre efficacement les infractions commises sur des réseaux de communication électronique, tels qu'Internet, ou via un téléphone mobile. Une règlementation spécifique serait vite dépassée compte tenu de l'évolution technologique rapide qui caractérise les cyber-réseaux et pourrait avoir pour conséquence d'exonérer largement les prestataires de leur responsabilité pénale, y compris là où elle se justifie.

2.2.2 Description des rôles dans le rapport sur les médias sociaux

Le rapport du Conseil fédéral « Cadre juridique pour les médias sociaux » de septembre 2013[37] contient une description des rôles en lien avec l'utilisation des médias sociaux. Le concept du Cadre juridique pour les médias sociaux se fonde – dans la perspective de la responsabilité juridique notamment – sur les catégories suivantes:

- **Fournisseurs de contenu:** ils proposent leurs propres contenus ou ceux d'autrui sur une infrastructure technique. Leur rôle se rapproche, dans le domaine des médias traditionnels (par ex. presse écrite), de la fonction de l'auteur (en lien notamment avec l'art. 28, al. 1, CP) ou de la personne responsable de la publication si celle-ci a lieu à l'insu de l'auteur ou contre sa volonté (art. 28, al. 3, CP). Si un fournisseur choisit les contenus à publier (par ex. commentaires sur une contribution à un blog) sur un organe rédactionnel qu'il exploite (par ex. un blog ou un site web), entre également en ligne de compte le rôle du rédacteur responsable (lequel, selon les dispositions des art. 28, al. 2, et 322bis CP, pourrait être poursuivi pour ne s'être pas opposé à une publication constituant une infraction).
- **Exploitants de plateformes:** ils mettent à la disposition des utilisateurs un cadre destiné à l'échange de contenus créés ou repris par ces derniers. Ils assument la responsabilité quant à l'architecture et au design de la plateforme de communication et ils choisissent les possibilités d'interaction et de diffusion des contenus. Dans les conditions d'utilisation, ils peuvent indiquer quels contenus ou quels comportements ne sont pas souhaités ou pas autorisés. Cependant, ils n'opèrent qu'un contrôle rédactionnel léger en comparaison des médias traditionnels. Alors que ceux-ci chargent généralement un comité de rédaction de sélectionner les contenus avant la publication *(ex-ante)*, sur les médias sociaux, le contrôle s'effectue après la publication *(ex-post)*, et les contenus non conformes aux conditions d'utilisation ou critiqués par d'autres utilisateurs ne sont retirés qu'après coup. Les exploitants de plateformes, contrairement aux fournisseurs d'hébergement et aux fournisseurs d'accès, ne constituent pas une catégorie juridiquement définie. La définition doit dans tous les cas mettre en lumière le fait que les exploitants de plateformes ont plus d'influence sur le contenu que les simples exploitants d'une infrastructure technique, qui assurent la sauvegarde et la mise à disposition automatisée des fichiers d'autrui (ce que font traditionnellement les fournisseurs d'hébergement).
- **Hébergeurs:** ils mettent à disposition contre rémunération une infrastructure technique (espace mémoire, capacité de calcul, capacités de transmission) pour la mise en ligne

[36] Le communiqué de presse peut être consulté sous: www.ofj.admin.ch > Sécurité > Projets législatifs en cours > Projets législatifs terminés > Cybercriminalité.

[37] Voir note 1.

automatisée de données. Les exploitants de plateformes ont souvent recours à leurs services. Comme la plupart des exploitants de plateformes occupant une place importante sur le marché suisse, la majorité des hébergeurs ont leur siège à l'étranger. Leur responsabilité n'est en général pas engagée sur les aspects rédactionnels, mais selon la constellation[38], ils sont techniquement en mesure de supprimer de leurs ordinateurs des contenus non souhaités.

- **Fournisseurs d'accès:** ils ne proposent pas d'infrastructure pour le stockage des données, mais uniquement la liaison technique avec les serveurs des hébergeurs (ou une partie de cette liaison). Contrairement à ces derniers (et aussi aux exploitants de plateformes), ce sont des fournisseurs de services de télécommunication au sens de la loi du 30 avril 1997 sur les télécommunications [LTC][39], car ils assurent la transmission d'informations entre au moins deux autres parties (art. 3, let. b, LTC), à savoir dans le domaine des médias sociaux entre les exploitants de plateformes et les utilisateurs. Les utilisateurs suisses recourent généralement aux services d'un fournisseur d'accès établi en Suisse (par ex. Swisscom). Les fournisseurs d'accès ne sont souvent pas en mesure de supprimer des contenus non souhaités (car ceux-ci ne sont pas sauvegardés sur leurs serveurs). Un fournisseur d'accès peut certes bloquer de manière ciblée l'accès à certains contenus. L'effet d'un tel blocage est toutefois toujours limité à ses clients.
- **Médias traditionnels et autres services de médias:** les médias traditionnels aident souvent les médias sociaux à attirer l'attention, à acquérir de nouveaux membres et à augmenter les recettes publicitaires. De leur côté, les médias sociaux sont de plus en plus utiles aux médias traditionnels en leur fournissant des contenus et des nouveautés. Du fait de ces interactions, la limite entre communication privée et communication publique est souvent floue pour les utilisateurs. De nombreux médias traditionnels sont eux-mêmes présents sur les médias sociaux ou reliés à de grands réseaux sociaux, tels que Facebook.
- Les **moteurs de recherche** constituent d'autres relais puisqu'ils renvoient les utilisateurs vers des contenus publiés non seulement dans les médias traditionnels mais aussi sur les réseaux sociaux. Il existe également des collaborations économiques, notamment pour l'échange et l'exploitation des données relatives aux utilisateurs à des fins commerciales ou autres.

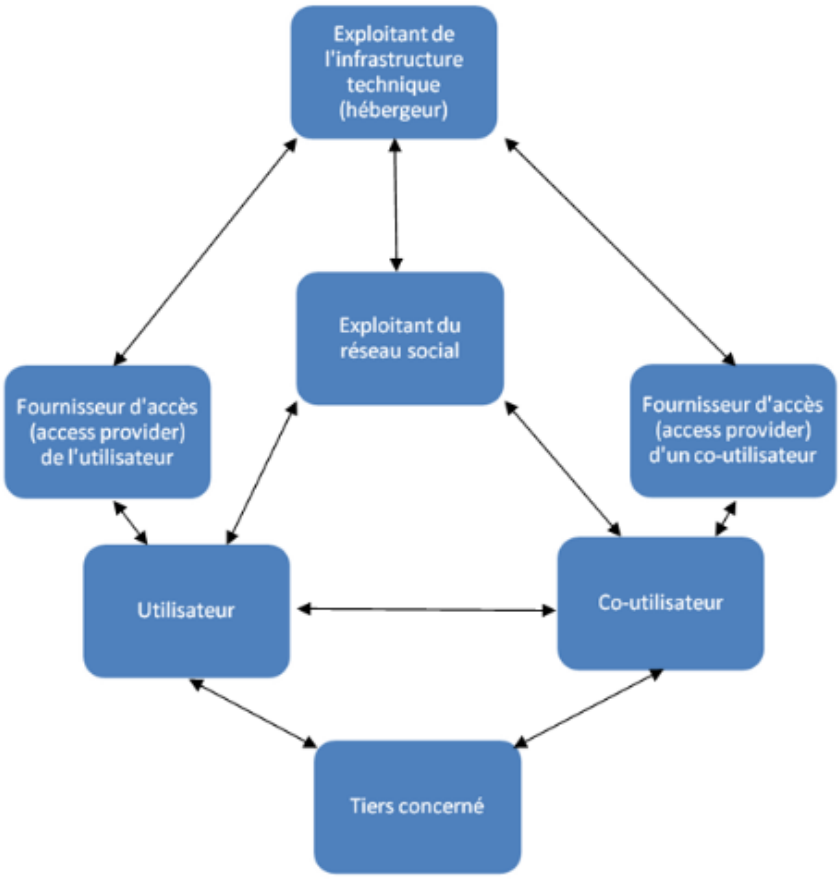
On soulignera que les frontières entre ces fonctions sont souvent poreuses[40]. Ainsi, les exploitants de plateformes peuvent intervenir également en tant qu'hébergeurs. Les différents acteurs qui interagissent dans l'utilisation des réseaux sociaux peuvent néanmoins être représentés graphiquement comme suit:

---

38 L'hébergeur ne peut parfois pas supprimer des contenus isolés sur un serveur qu'il loue, il ne peut que mettre hors service le serveur loué dans son intégralité.

39 RS 784.10.

40 Voir à ce sujet les explications données ci-avant sur les parties prenantes à la communication sur Internet dans le rapport de la commission d'experts « Cybercriminalité » (note 33), 29 ss.



2.2.3 Description des rôles dans le projet de LSCPT

a) Remarque préliminaire

Le projet de nouvelle loi fédérale sur la surveillance de la correspondance par poste et télécommunication (LSCPT)[41], actuellement en examen au Parlement (état septembre 2015), comprend quant à lui une description générale et abstraite des parties prenantes à la communication en ligne. Les définitions soumises au débat sont intéressantes, dans la mesure où elles complètent celles figurant dans l'AP-CP de 2004 et dans le rapport sur les médias sociaux de 2013 puisque d'autres catégories sont ajoutées.

b) Fournisseurs de services de communication dérivés (P-LSCPT, art. 2, let. c)

Les obligations de surveillance de la télécommunication en vertu du projet de LSCPT de 2013 (P-LSCPT) ne s'appliquent pas seulement aux fournisseurs d'accès (et donc aux « *fournisseurs de services de télécommunication, au sens de l'art. 3, let. b, [LTC]* »). D'autres personnes se trouvent également, à un moment ou un autre, en possession de données en lien avec la correspondance par poste et télécommunication qui peuvent s'avérer intéressantes pour les autorités de poursuite pénale dans le cadre de la lutte contre la

41 FF 2013 2483

criminalité. C'est pourquoi l'art. 2, let. c, P-LSCPT s'applique également aux « *fournisseurs de services qui se fondent sur des services de télécommunication et qui permettent une communication unilatérale ou multilatérale (fournisseurs de services de communication dérivés)* ». Cette règlementation répond à une question controversée soulevée lors de la consultation, à savoir si les fournisseurs de services Internet tels que les fournisseurs d'hébergement devraient figurer dans le champ d'application de la loi.

Selon les explications données dans le message, les fournisseurs de services de communication dérivés comprennent:

- les fournisseurs de services Internet qui permettent une *communication unilatérale*, rendant possible le chargement de documents (par ex. Google docs ou Microsoft office.live.com);
- les fournisseurs de services Internet qui permettent une *communication multilatérale*, rendant possible la communication entre usagers (par ex. Facebook).

La disposition inclut « *les fournisseurs d'espace de stockage d'e-mails, les différents types de fournisseurs d'hébergement (hosting providers) qui fournissent, par exemple, un hébergement d'applications ou services e-mail (p. ex. .gmx), un hébergement ‹colocation de serveurs› ou ‹serveur housing› avec accès (p. ex. Green.ch et Colt), un hébergement ‹Facility Management› sans service de communication (colocation pure) ou des services ‹cloud›, les plates-formes de chat, les plates-formes d'échange de documents et les fournisseurs de services de téléphonie par Internet du type peer-to-peer (p. ex. Skype peer-to-peer)* »[42]. La définition dans le projet de loi est formulée de manière ouverte, afin de permettre la prise en compte de développements technologiques à venir. Le Conseil fédéral devra par conséquent concrétiser cette disposition dans les dispositions d'exécution.

c) Classement des catégories selon la LSCPT

Le classement par catégories prévu dans le P-LSCPT ne vise pas à attribuer une responsabilité juridique dans les cas où la communication porte sur des contenus illicites. Les catégories peuvent, à première vue, être intégrées dans le schéma du rapport sur les médias sociaux, lequel est toutefois plus nuancé. La catégorie de la LSCPT « fournisseurs de services de communication dérivés » inclut aussi bien le fait de fournir un espace de stockage pour la sauvegarde automatisée (hébergement) que la fonction d'exploitant de plateforme, celui-ci entretenant un lien plus étroit avec les contenus de la communication que les simples prestataires techniques. Le Conseil fédéral devra régler les détails dans les dispositions d'exécution.

2.3 Définitions établies à l'étranger

Pour terminer, nous présentons à titre d'exemples quelques définitions contenues dans des règlementations étrangères.

[42] Message du 27.2.2013 concernant la loi fédérale sur la surveillance de la correspondance par poste et télécommunication (LSCPT), FF 2013 2379.

2.3.1 Union européenne

La directive 2000/31/CE (directive sur le commerce électronique)[43] contient à l'art. 2 des définitions des acteurs concernés:

- **Services de la société de l'information:** « *les services au sens de l'article premier, paragraphe 2, de la directive 98/34/CE, telle que modifiée par la directive 98/48/CE* »[44]. Un « service » est, dans ce contexte, « *tout service presté normalement contre rémunération, à distance par voie électronique et à la demande individuelle d'un destinataire de services* ».

  On entend par:

  - **« service à distance »:** un service fourni sans que les parties soient simultanément présentes;
  - **« service par voie électronique »:** un service envoyé à l'origine et reçu à destination au moyen d'équipements électroniques de traitement (y compris la compression numérique) et de stockage de données, et qui est entièrement transmis, acheminé et reçu par fils, par radio, par moyens optiques ou par d'autres moyens électromagnétiques;
  - **« service fourni à la demande individuelle d'un destinataire de services »:** un service fourni par transmission de données sur demande individuelle.
- **Prestataire:** « *toute personne physique ou morale qui fournit un service de la société de l'information* ».
- **Prestataire établi:** « *prestataire qui exerce d'une manière effective une activité économique au moyen d'une installation stable pour une durée indéterminée. La présence et l'utilisation des moyens techniques et des technologies requis pour fournir le service ne constituent pas en tant que telles un établissement du prestataire* ».
- **Destinataire du service:** « *toute personne physique ou morale qui, à des fins professionnelles ou non, utilise un service de la société de l'information, notamment pour rechercher une information ou la rendre accessible* ».
- **Consommateur:** « *toute personne physique agissant à des fins qui n'entrent pas dans le cadre de son activité professionnelle ou commerciale* ».

Dans la section « Responsabilité des prestataires intermédiaires » (art. 12 à 15) se trouvent des définitions du simple transport (qui concerne typiquement les fournisseurs d'accès), du *caching* et de l'hébergement.

- **Simple transport** (« *mere conduit* », art. 12): service de la société de l'information consistant à transmettre, sur un réseau de communication, des informations fournies par un utilisateur ou à fournir un accès au réseau de communication, à condition que le prestataire ne soit pas à l'origine de la transmission, ne sélectionne pas le

[43] Directive 2000/31/CE du Parlement européen et du Conseil du 8.6.2000 relative à certains aspects juridiques des services de la société de l'information, et notamment du commerce électronique, dans le marché intérieur («directive sur le commerce électronique»), JO L 178 du 17.7.2000, p. 1; voir également ch. 3.3.1 a) bb).

[44] Directive 98/34/CE du Parlement européen et du Conseil du 22.6.1998 prévoyant une procédure d'information dans le domaine des normes et règlementations techniques et des règles relatives aux services de la société de l'information, JO L 204 du 21.7.1998, p. 37, modifiée pour la dernière fois par le règlement (UE) n° 1025/2012 du 25.10.2012, JO L 316 du 14.11.2012, p. 12.

destinataire de la transmission et ne sélectionne ni ne modifie les informations faisant l'objet de la transmission. Le stockage automatique, intermédiaire et transitoire des informations transmises est également inclus, pour autant qu'il serve uniquement à l'exécution de la transmission sur le réseau de communication et que sa durée n'excède pas le temps généralement nécessaire à la transmission.

- ***Caching*** (art. 13): service de la société de l'information consistant en un stockage automatique, intermédiaire et temporaire de l'information fait dans le seul but de rendre plus efficace la transmission ultérieure de l'information à la demande d'autres destinataires du service.
- **Hébergement** (art. 14): service de la société de l'information consistant à stocker des informations fournies par un destinataire du service.

2.3.2 Etats-Unis

Le *Digital Millennium Copyright Act (DMCA)*[45] s'adresse au fournisseur de services (« *service provider* ») et comprend la définition suivante:

- ***Service provider*** **(fournisseur de services)**

  (A) As used in subsection (a), the term "service provider" means an entity offering the transmission, routing, or providing of connections for digital online communications, between or among points specified by a user, of material of the user's choosing, without modification to the content of the material as sent or received.

  (Le terme « service provider » désigne l'entité qui propose la transmission, le routage ou l'établissement de connexions pour des communications numériques en ligne, entre deux ou plusieurs points spécifiés par un utilisateur, d'informations choisies par l'utilisateur, sans modifier le contenu des informations envoyées ou reçues.)

  (B) As used in this section, other than subsection (a), the term "service provider" means a provider of online services or network access, or the operator of facilities therefor, and includes an entity described in subparagraph (A).

  (Contrairement au paragraphe (a), le terme « service provider » désigne un fournisseur de services en ligne ou d'un accès au réseau, ou l'opérateur d'infrastructures destinées à cette fin, et inclut l'entité évoquée au sous-paragraphe (A).)

Le DMCA définit en outre certains actes, tels que « *transitory digital network communications* » (les communications transitoires sur réseau numérique), « *system caching* » (le cache système) et « *information residing on systems or networks at direction of users* » (l'information détenue sur des systèmes ou réseaux à l'intention des utilisateurs).

Les définitions figuraient également dans le projet de loi visant à mettre fin au piratage en ligne, *Stop Online Piracy Act (SOPA)*, qui n'a pas été poursuivi en raison des controverses liées à l'accord de lutte contre la contrefaçon et le piratage (ACTA)[46]:

- ***Internet advertising service*** (service de publicité par Internet): un service qui, contre rémunération, vend, achète, assure le courtage de, insère, vérifie, élimine ou facilite de

[45] 17 U.S.C. § 512 (*Digital Millennium Copyright Act*), voir également ch. 3.3.2.

[46] Voir www.ige.ch > Infos juridiques > Domaines juridiques > Contrefaçon et piraterie > ACTA; voir au sujet du SOPA également le ch. 3.3.2.

toute autre manière le placement de publicité, y compris un résultat de recherche, un lien ou un placement payé ou sponsorisé, qui est restitué sous une forme visible, pour quelque durée que ce soit, sur un site Internet.

- ***Internet protocol allocation entity*** (instance d'attribution des adresses IP): s'agissant d'une adresse IP particulière, l'instance, le registre Internet local ou le registre Internet régional auquel est attribué le plus petit bloc d'adresses IP possible contenant cette adresse ou auquel elle est attribuée ou assignée par un registre Internet local ou régional, ou par une autre autorité chargée de l'attribution des adresses IP, en fonction de la banque de données publiquement disponible pertinente d'attributions et d'assignations, s'il en existe une.
- ***Internet search engine*** (moteur de recherche): un service fourni via Internet qui recherche, sonde, classe ou indexe des informations ou des sites web disponibles ailleurs sur Internet et, sur la base de la recherche ou de la sélection faite par un utilisateur sous la forme de termes, de concepts, de catégories, de questions ou d'autres données, renvoie à l'utilisateur une ressource, telle qu'une liste de localisateurs de ressources uniformes sous la forme de liens hypertextes, d'une localisation, d'une visualisation, ou du téléchargement de l'information ou des données disponibles sur Internet en lien avec cette recherche ou cette sélection.
- ***Nonauthoritative domain name serveur*** (serveur de noms de domaine ne faisant pas autorité): un serveur qui ne contient pas des copies complètes de domaines, mais qui utilise un fichier cache compris dans des requêtes antérieures de serveurs de noms de domaines, pour lesquelles le serveur a reçu une réponse faisant autorité par le passé.
- ***Owner; operator*** (propriétaire; opérateur): ces termes, utilisés en lien avec un site Internet, désignent, dans le premier cas, tout propriétaire jouissant d'un intérêt majoritaire et dans le second cas, toute personne en position d'autorité pour opérer un tel site Internet.
- ***Payment network provider*** (fournisseur de réseau de paiement): (A) en général: une entité qui fournit directement ou indirectement les services du propriétaire, une infrastructure et des logiciels pour exécuter ou faciliter une inscription au débit, au crédit, ou une autre transaction de paiement. (B) une « *depository institution* » (institution dépositaire) (qui est le terme défini à la section 3 du *Federal Deposit Insurance Act*) ou une « *credit union* » (coopérative de crédit) qui entame une transaction de paiement ne doit pas être considérée comme un fournisseur de réseau de paiement uniquement parce qu'elle propose ou fournit un service de ce type.
- ***Service provider*** (fournisseur de service): tel que défini à la section 512(k)(1) du titre 17 du *United States Code*[47], un fournisseur de service qui gère un système de noms de domaines ne faisant pas autorité.

2.3.3 Evaluation des règlementations dans l'UE et aux Etats-Unis

Il apparaît que les définitions dans la directive sur le commerce électronique de l'UE se fondent sur les prestations fournies et ne définit pas plus avant les catégories de prestataires. Dans le projet de *Stop Online Piracy Act (SOPA)*[48], qui est resté inachevé, il était prévu d'évoquer, outre les fournisseurs classiques, d'autres acteurs tels que les services de paiement, qui

[47] *Digital Millennium Copyright Act*.
[48] Voir ch. 2.3.2 et 3.3.2.

permettent le financement de services sur Internet. Il convient de prendre note de ce développement. Il montre comment évolue le paysage d'Internet et comment des acteurs tels que les exploitants de services de paiement, par exemple, ou des serveurs DNS non autoritaires gagnent en importance.

2.4 Conclusion: définition des rôles dans le présent rapport

En raison des développements techniques rapides, le classement des fournisseurs dans des catégories fixes pose problème. L'évaluation juridique des rôles des différents acteurs devrait se faire sur une base aussi neutre que possible sur le plan technologique. Un critère central est la « proximité avec le contenu » : dans quelle mesure un acteur a-t-il une maîtrise du contenu qu'il rend accessible en ligne ? Quelles sont les possibilités qu'il a d'influer sur le contenu, de le modifier, de le supprimer ou de le bloquer ? Dans quelle mesure est-il souhaitable, sur le plan politique, qu'il fasse usage – éventuellement de manière plus systématique - de ces possibilités ?

Dans un souci de simplification, il est opportun de se fonder sur les définitions contenues dans les projets de loi et rapports mentionnés ci-avant. Elles sont également utilisées dans la jurisprudence et la doctrine. Il convient donc de prendre pour point de départ la **triade établie:**

- **fournisseur de contenu**
- **fournisseur d'hébergement**
- **fournisseur d'accès**

De manière générale, le terme de « fournisseur » désignera, dans le présent rapport, les deux dernières catégories. En effet, il faut garder à l'esprit la différence fondamentale entre les fournisseurs de contenu et les autres acteurs au niveau de la proximité avec le contenu transmis: les fournisseurs d'hébergement et les fournisseurs d'accès apportent une *prestation automatisée* pour les fournisseurs de contenu (et d'autres acteurs). Contrairement aux fournisseurs de contenu, les fournisseurs d'hébergement ne s'occupent pas – et encore moins les fournisseurs d'accès – de la mise en ligne de contenus qu'ils ont eux-mêmes élaborés ou choisis. Toutefois, il existe aussi des fournisseurs de contenu chez lesquels les contenus sont générés automatiquement et non pas produits intentionnellement au cas par cas par une intervention humaine. Ces agrégateurs de contenus, comme on les appelle, sont certes moins proches du contenu que les autres fournisseurs de contenu, mais ils en sont plus proches que les fournisseurs d'hébergement ou d'accès.

C'est pourquoi on soulignera la nécessité d'être conscient que les frontières entre ces catégories sont poreuses et que les formes mixtes ou particulières sont nombreuses (par ex. plateformes de réseaux sociaux, exploitants de moteurs de recherche). Par ailleurs, il est difficile de classer un certain nombre d'acteurs dans les définitions ci-dessus. C'est notamment le cas de ceux qui mettent des liens sur leurs pages ou des services qui jouent le rôle d'intermédiaire entre fournisseurs de publicité et fournisseurs de contenus[49].

Différents fournisseurs sont notamment attribués à la catégorie des *fournisseurs d'hébergement* par la doctrine et la jurisprudence alors que leurs services vont au-delà de l'hébergement traditionnel. Les fournisseurs d'hébergement traditionnels mettent à disposition

[49] Voir la question 3 de l'interpellation Stöckli 12.4202 « Swisscom. Gestion des contenus protégés par les droits d'auteur ».

contre rémunération une infrastructure technique (espace mémoire, capacités de calcul, capacités de transmission) pour la mise en ligne automatisée de données[50], mais n'entretiennent que des contacts indirects avec les données et doivent être considérés comme étant distants du contenu. Les plateformes de médias sociaux, telles que Facebook et Twitter ou encore YouTube, qui mettent à la disposition de leurs utilisateurs un cadre pour l'échange de contenus qu'ils ont eux-mêmes créés ou repris, sont déjà plus proches du contenu. Elles décident des possibilités d'interaction et de diffusion de contenus, mais ne vérifient généralement pas de manière préventive les énormes quantités de données que leurs utilisateurs mettent en ligne à toute heure du jour et de la nuit[51]. Les plateformes de vente aux enchères se comportent de manière similaire avec les offres de leurs utilisateurs. Les exploitants de plateformes de blogs, qui peuvent exercer une influence sur le choix des auteurs, ou de forums d'opinion, qui comptent souvent des membres enregistrés, ont davantage de maîtrise des contenus. Il est plus facile d'avoir une vue d'ensemble des données mises en ligne et d'exercer sur elles une influence. Sur les forums, il existe souvent un personnel d'encadrement (modérateurs). Enfin, les portails d'information ou les exploitants de blogs ont une importante capacité à contrôler les commentaires de leurs lecteurs. Ces possibilités d'influence rédactionnelle, très variables, doivent toujours être prises en compte dans l'examen des droits et des obligations des fournisseurs d'hébergement.

3 Actions défensives (action en prévention et en cessation de l'atteinte, etc.)

3.1 Responsabilité des fournisseurs en cas de contenu illicite

3.1.1 Exclusion des fournisseurs de contenu du champ de l'étude

Nous n'approfondirons pas les actions possibles contre le fournisseur qui viole le droit par ses *propres* contenus, c'est-à-dire le fournisseur de contenus qui porte directement atteinte aux droits d'autrui ou les lèse de toute autre manière. L'examen des prétentions suit alors la voie normale et ne pose a priori pas de problèmes[52]. Une deuxième question doit être étudiée de plus près: il importe d'examiner si une action est possible (aussi) contre le fournisseur d'accès ou d'hébergement dans les cas où les utilisateurs de ses prestations ont violé le droit. En d'autres termes, celui-ci participe-t-il à l'acte illicite[53] ?

[50] Voir également à ce sujet le ch. 2.2.2.

[51] Voir également à ce sujet le ch. 2.2.2 sur le rapport du Conseil fédéral sur les médias sociaux. YouTube fait par exemple état de 300 heures de matériel vidéo chargées chaque minute (www.youtube.com/yt/press/fr/statistics.html, par ex. aussi *Fountoulakis/Francey*, medialex 2014, 182).

[52] Voir *Hug*, medialex 2014, 56.

[53] La participation est définie de manière diverse selon les dispositions examinées; voir art. 28, al. 1, CC: participer; art. 66, let. d, de la loi du 25.6.1954 sur les brevets (LBI; RS 232.14): inciter, collaborer, favoriser, faciliter; art. 50, al. 1, CO: instigateur, complice. Sur la portée des dispositions, voir le ch. 3.2 et en particulier le ch. 3.2.5 a) concernant le droit de la propriété intellectuelle.

3.1.2 Le comportement illicite: une action ou une omission ?

La question de savoir si la participation du fournisseur d'accès ou d'hébergement à la violation du droit relève d'une action ou d'une omission est d'une certaine importance en droit[54]. Le fournisseur a-t-il activement causé l'acte illicite d'un tiers en proposant et en exploitant ses services ou bien faut-il plutôt lui reprocher de ne pas avoir empêché cet acte – d'avoir donc omis d'agir ? Les auteurs de doctrine ne s'accordent pas sur ce point[55].

Dans l'arrêt télékiosque (ATF 121 IV 109), un responsable des PTT avait été déclaré coupable de complicité de publications obscènes et de pornographie, du fait qu'il fournissait les prestations nécessaires à l'utilisation du télékiosque 156. Au considérant 3b, le Tribunal fédéral s'est penché sur la distinction entre action et omission:

> « On vient de voir que la complicité est concevable sous ces deux formes, mais une pure omission ne serait punissable que si l'intéressé avait l'obligation juridique d'agir. Il a été constaté en fait que le recourant avait ordonné l'introduction du télékiosque 156 et que c'est donc sur son ordre que les installations téléphoniques nécessaires à la réalisation de l'infraction ont été fournies. La mise à disposition de ces installations constitue une prestation positive. Que cette prestation ait pu être licite si elle s'était accompagnée de mesures de précaution n'a pas pour effet de transformer l'action en une omission. Il est fréquent que l'on reproche à une personne la manière dont elle a agi et, en définitive, des omissions dans son action; dans ces cas délicats, la jurisprudence a admis, dès lors que l'on discerne action et omission, qu'il fallait traiter le cas comme une action. »

---

[54] Selon la vue prédominante en matière de responsabilité civile dans le domaine extracontractuel, une omission ne peut être illicite que si la loi prévoit une obligation d'agir dans l'intérêt du lésé (principe « de l'omission licite »; ATF 115 II 15, consid. 3b; BSK OR I-*Kessler*, ad art. 41 n° 37). Il est indispensable que cette obligation d'agir donne au responsable une position de garant, de sorte qu'il ait à répondre de l'atteinte (voir par ex. *Fellmann/Kottmann*, Haftpflichtrecht I, n° 347). L'obligation d'agir n'est pas le seul élément de l'illicéité de l'atteinte: l'omission doit entraîner l'atteinte à un bien juridique absolu ou – en cas de simple dommage matériel – la violation d'une norme de protection spécifique (voir ATF 124 III 297, consid. 5b et c; BSK OR I-*Kessler*, ad art. 41 n° 38). La doctrine ne s'est guère exprimée sur l'opportunité d'examiner l'existence de cette obligation d'agir en cas d'action défensive. Lorsqu'elle le fait, c'est pour préconiser que la licéité de l'omission soit examinée (voir *Fellmann/Kottmann*, Haftpflichtrecht I, n° 611; *Aebi-Müller*, n° 22). L'obligation d'agir pourrait aussi être déduite du principe général de l'interdiction de créer un danger pour autrui (*neminem laedere*). Ce principe veut que celui qui crée ou entretient une situation dangereuse doit prendre les mesures nécessaires pour éviter un dommage (voir ATF 126 III 113, consid. 2.a/aa; BSK OR I-*Kessler*, ad art. 41 n° 19a). Il ne semble pas y avoir en Suisse de jurisprudence de droit civil sur la question de savoir si la fourniture d'accès et d'hébergement pourrait être considérée comme la création d'une situation dangereuse. On trouve l'opinion contraire dans la doctrine, l'argument étant qu'il s'agit d'une prestation ordinaire, usuelle dans notre société et ne donnant en général pas lieu à des infractions (« *tatunüblich* ») (voir *Rosenthal*, Internet-Provider-Haftung – ein Sonderfall?, n° 91, où il se réfère à une décision du président du tribunal pénal de Bâle-Ville du 31 janvier 2003, parue dans: sic! 2003, 960 ss; *Frech*, 334; la question est par contre laissée explicitement ouverte dans *Weber*, E-Commerce, 508 s.; tendance à admettre qu'il y a création d'une situation dangereuse dans: *Briner*, sic! 2006, 397 ss et *Rohn*, 199).

[55] Pour une action: *Rosenthal*, Internet-Provider-Haftung – ein Sonderfall?, n° 78; le même, sic! 2006, 511 ss; pour une omission: *Briner*, sic! 2006, 391, 397. La majeure partie des auteurs laisse la question ouverte en précisant que le critère décisif selon lequel on apprécie le comportement du fournisseur est dans les deux cas la diligence, par ex. : *Weber*, E-Commerce, 508 s., 516 s. ; *Frech*, 326 s.; *Rohn*, 82; *Fountoulakis/Francey*, medialex 2014, 179.

Le Tribunal fédéral a en l'occurrence considéré la participation du responsable comme une « action ». En droit pénal, on parle de subsidiarité de l'omission[56]. Les actes commis par négligence comprennent toujours une abstention de la diligence nécessaire[57].

Ces réflexions peuvent aussi s'appliquer aux fournisseurs d'accès et d'hébergement, qui fournissent et entretiennent l'infrastructure nécessaire à la publication et à la transmission des données[58]. Au nom de l'unité du droit, il faudrait partir du principe qu'il s'agit là d'une action tant du fournisseur d'hébergement que du fournisseur d'accès. Dans ce qui est à notre connaissance le seul arrêt en Suisse sur la responsabilité de droit civil d'un hébergeur de blogs, le Tribunal fédéral ne s'est pas prononcé explicitement et semble avoir lui aussi présumé qu'il s'agissait d'une action[59].

3.2 Droit suisse

3.2.1 Aperçu

Dans les chapitres qui suivent, nous allons présenter les actions défensives possibles contre les fournisseurs pour des violations du droit par les utilisateurs de leurs prestations, par domaine du droit. La présentation commencera par la norme de principe relative au droit de la personnalité et aux prétentions relevant du droit de la protection des données et du droit de la concurrence. On parlera ensuite des droits de la propriété intellectuelle. La question de la « légitimation passive » est à chaque fois au cœur de ces réflexions. La légitimation passive est la qualité de celui qui, dans le contexte d'une prétention litigieuse, a des obligations de droit matériel et qui peut en conséquence être partie au procès en tant que défendeur[60]. Dans les chapitres qui suivent, nous examinerons dans chaque cas si une prétention de droit matériel peut être élevée contre les fournisseurs.

3.2.2 Protection de la personnalité

a) Remarques générales

Selon l'art. 28, al. 1, CC, celui qui subit une atteinte illicite à sa personnalité peut agir en justice contre toute personne qui y participe. Il peut requérir le juge, conformément à l'art. 28*a*, al. 1, CC:

> « 1. d'interdire une atteinte illicite, si elle est imminente [action en prévention de l'atteinte] ;
>
> 2. de la faire cesser, si elle dure encore [action en cessation de l'atteinte] ;
>
> 3. d'en constater le caractère illicite, si le trouble qu'elle a créé subsiste [action en constatation de l'atteinte]. »

---

[56] ATF 115 IV 199, consid. 2.a. Selon cet arrêt, il faut toujours examiner en premier lieu si le prévenu a eu un comportement actif qui soit conforme à la typicité de l'infraction, contraire au droit et fautif. Le comportement ne constitue pas une omission si l'on peut et doit établir un lien entre lui et une action.

[57] Voir aussi *Seelmann*, 105; *Roberto*, n° 06.10; sur la négligence, voir pour plus de détails le ch. 4.1.1 d).

[58] Par ex. *Rosenthal*, Internet-Provider-Haftung – ein Sonderfall?, n° 78, le même, sic! 2006, 511 ss.

[59] Arrêt du Tribunal fédéral 5A_792/2011 du 14.1.2013; plus de détails sur cet arrêt au ch. 3.2.2 c) ; sur la différence entre l'action et l'omission, voir en outre la note 266.

[60] Voir *Staehelin/Staehelin/Grolimund*, 159.

Enfin, selon l'art. 28*g*, al. 1, CC, celui qui est directement touché dans sa personnalité par la présentation que font des médias à caractère périodique de faits qui le concernent a le droit de répondre. Les publications sur Internet peuvent être assimilées à des médias à caractère périodique si elles s'adressent régulièrement à un public comparable[61].

La protection de la personnalité repose sur une clause générale. La jurisprudence et la doctrine ont fait des catégories et des listes de biens de la personnalité protégés, sans prétention à l'exhaustivité[62]. Les droits de la personnalité se réfèrent notamment à la personnalité physique, dont les biens juridiques majeurs sont l'intégrité corporelle et la liberté de mouvement, à la personnalité affective (ou émotionnelle), qui englobe le respect de la vie affective, à la personnalité sociale, dont le droit à l'honneur et le droit au caractère privé de l'information sont deux aspects et, enfin, à la personnalité économique, qui recouvre le droit de développer une activité économique.

La protection de la personnalité, régie par les art. 28 ss CC, sert à préserver l'individu contre les atteintes par des tiers, qu'il y ait faute de ceux-ci ou non[63]. L'action au sens de l'art. 28*a* CC repose sur l'existence d'une atteinte illicite à la personnalité. L'art. 28, al. 2, CC dispose qu'une atteinte est illicite dès lors qu'elle n'est pas justifiée par un des trois motifs qu'il énumère[64]. Le fait qu'il s'agisse d'une atteinte à la personnalité laisse entendre qu'il s'agit essentiellement d'une action. Une omission ne peut, selon une partie de la doctrine, que très rarement être qualifiée d'atteinte à la personnalité[65]. L'illicéité de l'omission doit alors être examinée et motivée tout particulièrement[66].

Les exemples d'atteinte à la personnalité sur Internet sont légion, surtout dans les médias sociaux[67]. Pour ce qui est de déterminer si un contenu porte atteinte à la personnalité de quelqu'un, on peut se fonder sur les principes généraux.

b) Légitimation passive en cas d'atteinte à la personnalité

Les actions visées à l'art. 28*a* CC peuvent être dirigées, en vertu de la formulation de l'art. 28, al. 1, CC, contre toute personne qui participe à l'atteinte. Le lésé peut donc viser un participant secondaire s'il espère obtenir une meilleure protection par cette voie[68]:

> « Le législateur a précisément voulu permettre à la victime de s'en prendre à toute personne qui, par son comportement, joue objectivement un rôle quelconque dans la création ou le développement d'une atteinte, car c'est à cette seule condition que l'on garantira une protection complète de la personne [...]. Il suffit ainsi que la personne

---

61 Voir par ex. BSK ZGB I-*Schwaibold*, ad art. 28*g* n° 3 s.

62 Voir *Hausheer/Aebi-Müller* n° 12.40 ss; BSK ZGB I-*Meili*, ad art. 28 n° 16 ss; *Steinauer/Fountoulakis*, n° 513 ss.

63 *Hausheer/Aebi-Müller*, n° 12.08 s.; BSK ZGB I-*Meili*, ad art. 28 n° 55; *Steinauer/Fountoulakis*, n° 551.

64 Voir message du 5.5.1982 concernant la révision du code civil suisse (protection de la personnalité: art. 28 CC et 49 CO), FF 1982 II 661 ss, 682; *Hausheer/Aebi-Müller*, n° 12.12 ss.

65 *Fellmann/Kottmann*, Haftpflichtrecht I, n° 611.

66 *Fellmann/Kottmann*, Haftpflichtrecht I, n° 611; *Aebi-Müller*, n° 22, selon qui il est possible de déduire de l'art. 2 CC une obligation d'agir dans de rares cas d'atteinte à la personnalité par omission.

67 A ce sujet, voir le rapport du Conseil fédéral « Cadre juridique pour les médias sociaux » (note 1), 38 ss.

68 Arrêt du Tribunal fédéral 5P.308/2003 du 28.10.2003, consid. 2.5, avec un renvoi à *Tercier*, n° 845 et 847.

> recherchée contribue par son comportement à l'atteinte, même si elle ne joue dans celle-ci qu'un rôle secondaire […]. »

Le Tribunal fédéral a rendu plusieurs arrêts dans lesquels il a eu à examiner la légitimation passive en relation avec les médias. Il a notamment donné droit à des demandes dirigées contre le propriétaire d'un site Web privé qui y reproduisait des articles de journaux contenant des atteintes à la personnalité[69], un journal qui avait reproduit des courriers de lecteurs de ce type[70] et une imprimerie qui avait participé à la diffusion d'une série d'articles diffamatoires[71].

La légitimation passive ne peut cependant pas être d'une portée illimitée en matière de protection de la personnalité. Le cercle des personnes qui peuvent faire l'objet d'une action est restreint par deux clauses générales: la proportionnalité et, selon une partie de la doctrine, la causalité adéquate.

Le juge doit respecter le *principe de proportionnalité* lorsqu'il ordonne une mesure, que celle-ci vise la prévention de l'atteinte[72] ou la cessation de l'atteinte[73]. Il doit faire une pesée des intérêts, en tenant compte du fait que la mise en œuvre de sa décision risque de léser à son tour des intérêts du défendeur[74]. Une action contre un participant qui ne peut pas raisonnablement éviter ni faire cesser l'atteinte à la personnalité est en conséquence vouée à l'échec[75].

Par ailleurs, l'action (ou l'omission) contestée doit avoir un *lien de causalité adéquat* avec l'atteinte à la personnalité, selon une partie de la doctrine[76]. Selon la conception qu'a le Tribunal fédéral de la causalité adéquate, la cause doit être de nature, selon le cours naturel des choses et l'expérience générale de la vie, à entraîner un résultat tel que celui qui s'est produit (ou qui risque de se produire), c'est-à-dire que ce résultat doit sembler favorisé de manière générale par l'événement en question[77]. L'examen de ce point est particulièrement important dans le cas d'une action en prévention, car le demandeur doit prouver la probabilité de l'atteinte, et donc sa prévisibilité[78]. Les auteurs de doctrine évoqués à ce sujet estiment que la causalité adéquate doit aussi être prouvée dans le cas d'une action en cessation ou en constatation, même si un participant à l'acte tout à fait secondaire peut faire l'objet d'une action défensive fondée sur la protection de la personnalité[79]. Il serait donc envisageable de rejeter une telle action parce qu'elle ne respecte pas le principe de proportionnalité ou la causalité adéquate si le lien avec l'atteinte à la personnalité est ténu ou si le fournisseur ne peut raisonnablement pas prévenir ou faire cesser l'atteinte à la personnalité.

---

69 Arrêt du Tribunal fédéral 5P.308/2003 du 28.10.2003, consid. 2.5.
70 ATF 106 II 92.
71 ATF 126 III 161.
72 *Hausheer/Aebi-Müller*, n° 14.14; BSK ZGB I-*Meili*, ad art. 28*a* n° 2; sur les actions en prévention de l'atteinte, voir ch. 3.2.6.
73 *Aebi-Müller*, n° 285; BSK ZGB I-*Meili*, ad art. 28*a* n° 4; *Tercier*, n° 959.
74 *Aebi-Müller*, n° 285.
75 Voir aussi *Frech*, 274 ss, avec d'autres références à la note de bas de page 1381; sur le droit d'auteur, *Bühler Lukas*, 313 s.
76 *Aebi-Müller*, n° 140; *Geiser,* medialex 1996, 203 ss, 204; pour le droit de la propriété intellectuelle, *Hess-Blumer*, sic! 2003, 103.
77 Voir par ex. ATF 123 III 110, consid. 3.a.
78 Voir *Aebi-Müller*, n° 140; *Steinauer/Fountoulakis*, n° 579.
79 Pour des références, voir la note 76.

A notre connaissance, la doctrine reconnaît en général la légitimation passive des fournisseurs d'hébergement en cas d'atteinte à la personnalité par les utilisateurs de leurs services[80]. L'arrêt du Tribunal fédéral dans l'affaire Tribune de Genève[81] - que nous commenterons dans le chapitre qui suit – est également pertinent. Par contre, il ne semble pas qu'il faille considérer que les fournisseurs d'accès doivent répondre des atteintes, faute de lien de causalité adéquate entre celles-ci et leur participation[82].

c) Arrêt du Tribunal fédéral dans l'affaire Tribune de Genève

Dans le seul arrêt rendu à notre connaissance par le Tribunal fédéral sur la responsabilité d'un fournisseur (Tribune de Genève)[83], les juges ont conclu qu'une demande en cessation de l'atteinte pouvait être formée contre l'hébergeur d'un blog même si ce dernier ne sait rien du contenu de ce blog[84]. Il faut noter qu'un hébergeur de blogs n'est pas un fournisseur d'hébergement typique[85]. Dans ses considérants, le Tribunal fédéral se réfère à la formulation de l'art. 28, al. 1, CC, selon lequel il est possible d'agir en justice contre toute personne qui participe à une atteinte à la personnalité. Il considère que la différence avec un journal qui publie des lettres de lecteurs n'est pas pertinente car « la légitimation passive n'est pas liée à la maîtrise ou non du contenu des propos rapportés »[86]. Il rejette aussi dans les termes suivants les arguments de la Tribune de Genève:

> « La recourante se méprend aussi lorsqu'elle prétend que reconnaître la légitimation passive de l'hébergeur de blogs met en péril les fournisseurs d'accès qui se verront désormais actionnés en dommages-intérêts ou en réparation du tort moral. Ce faisant, elle se réfère ainsi aux actions réparatrices – qui ne sont pas en cause en l'espèce – réservées par l'art. [28*a*] al. 3 CC pour lesquelles les art. 41 ss CO prévoient des conditions particulières. En effet, si, dans ce cadre, le lésé peut également choisir contre qui il veut agir, ce choix sera toutefois limité par le fait qu'il ne peut s'adresser qu'à ceux dont il parvient à prouver la faute, exigence qui n'est pas posée pour les actions défensives. Pour le surplus, *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*. »[87]

Il faut noter que le tribunal de première instance avait condamné l'hébergeur de blogs à un quart des frais et l'auteur du blog aux trois quarts des frais.

La décision a été accueillie fraîchement par la doctrine. Certes, les auteurs ont approuvé la condamnation de la Tribune de Genève, mais ils ont reproché au Tribunal fédéral de ne pas avoir envisagé des restrictions possibles et d'avoir reconnu la légitimation passive de tous les

---

80 Voir *Rosenthal*, Aktuelle Anwaltspraxis 2013, 727 s. ; *Kernen*, Jusletter du 4.3.2013, n° 19 s. ; *Schoch/Schüepp*, Jusletter du 13.5.2012, n° 32.

81 Arrêt du Tribunal fédéral 5A_792/2011 du 14.1.2013.

82 *Schoch/Schüepp*, Jusletter du 13.5.2012, n° 32; sur la causalité adéquate en cas d'action réparatrice, *Rosenthal*, Internet-Provider-Haftung – ein Sonderfall?, n° 110 ss; *Weber*, E-Commerce, 509 s.; *auf der Maur/Steiner*, 423.

83 Arrêt du Tribunal fédéral 5A_792/2011 du 14.1.2013.

84 Arrêt du Tribunal fédéral 5A_792/2011 du 14.1.2013, consid. 6.2.

85 Voir ch. 2.4.

86 Arrêt du Tribunal fédéral 5A_792/2011 du 14.1.2013, consid. 6.3.

87 Arrêt du Tribunal fédéral 5A_792/2011 du 14.1.2013, consid. 6.3 (c'est nous qui mettons en évidence).

participants à une atteinte à la personnalité[88]. Ils ont aussi critiqué la décision de la condamner aux dépens sans lui avoir donné d'avertissement préalable ni lui avoir permis de satisfaire de son plein gré à la demande formée contre elle[89].

La portée de cet arrêt (qui n'est pas publié au recueil officiel des arrêts du Tribunal fédéral) et la possibilité de le transposer à d'autres domaines du droit ne sont pas certaines.

d) En particulier: légitimation passive des moteurs de recherche et des personnes qui mettent un lien sur leur page

Le Tribunal fédéral s'est tout récemment prononcé sur la légitimation passive des personnes qui mettent un lien sur leur page[90]. Il est parvenu à la conclusion qu'il ne suffisait pas, pour être considérée comme participant au sens de l'art. 28, al. 1, CC, qu'une entreprise mette sur son site Internet un lien général vers le site Internet d'un journal ou d'une station de radio qu'elle possède. Ce lien est trop peu spécifique pour causer, permettre ou favoriser une atteinte par une contribution du média en question. Le Tribunal fédéral n'a pas précisé si la situation juridique devait être appréciée autrement en cas de lien spécifique vers un article ou une émission particuliers.

A notre connaissance, il n'existe qu'une décision cantonale sur la légitimation passive des moteurs de recherche[91]. Dans l'arrêt Google suggest, le Tribunal cantonal du Jura est parvenu à la conclusion que les fonctionnalités de saisie automatique de Google, qui complétaient la raison de commerce d'une société suisse du mot « *scam* » (arnaque), ne pouvaient être considérées comme une atteinte à la personnalité de la part de Google. En effet, le moteur de recherche indique des suggestions sur la base des recherches les plus fréquentes des utilisateurs précédents de cet outil; l'internaute moyen comprend donc qu'il s'agit d'un renvoi à des sites qui contiennent des informations défavorables à la société et non d'une affirmation de Google. De plus, selon cet arrêt, les suggestions de recherche Google permettent l'accès au plus grand nombre d'informations possibles sur Internet, ce qui répond à un intérêt public[92]. Des tribunaux étrangers sont parvenus à des conclusions contraires dans des cas similaires, soulignant que Google pouvait influer sur les résultats de la recherche[93]. L'arrêt du Tribunal cantonal du Jura fait l'objet de critiques à ce sujet dans la doctrine[94].

Le processus de « saisie automatique » illustre la difficulté qu'il y a à tracer une ligne nette entre de simples actes de participation et une violation du droit par son propre comportement. La saisie automatique génère des propositions sans intervention humaine à partir des recherches des utilisateurs précédents. Il est cependant possible que ce processus automatique de renvoi à des informations données par des tiers entraîne une atteinte à la personnalité, s'il accole à un nom saisi dans le champ de recherche un vocable tel que « prostitué » ou « escroc ».

---

88 *Rosenthal*, Aktuelle Anwaltspraxis 2013, 727 s. ; *Kernen*, Jusletter du 4.3.2013, n° 19 s. ; *Schoch/Schüepp*, Jusletter du 13.5.2012, n° 36 s.

89 *Rosenthal*, Aktuelle Anwaltspraxis 2013, 728; *Schoch/Schüepp*, Jusletter du 13.5.2012, n° 36.

90 Arrêt du Tribunal fédéral 5A_658/2014 du 6.5.2015, consid. 4.2.

91 Arrêt du Tribunal cantonal du Jura du 12.2.2011 (CC117/2010), consultable à l'adresse www.jura.ch/Htdocs/Files/v/11625.pdf.

92 Arrêt du Tribunal cantonal du Jura du 12.2.2011 (note 91), consid. 4.2 ss.

93 Voir l'aperçu dans *Fanti*, Jusletter du 26.3.2012, n° 38 ss; arrêt de la Cour fédérale allemande du 14.5.2013, VI ZR 269/12 (Google Autocomplete).

94 *Fanti*, Jusletter du 26.3.2012, n° 31 ss; *Hürlimann*, 102 ss.

3.2.3 Protection des données

a) Remarques générales

La LPD a pour but de « *protéger la personnalité et les droits fondamentaux des personnes qui font l'objet d'un traitement de données* » (art. 1 LPD). On considère traditionnellement que la loi, dans sa partie consacrée au traitement de données personnelles par des personnes privées, concrétise et précise les règles générales du CC sur la protection de la personnalité[95]. Pour cette raison, le législateur a considéré que les règles sur la protection juridique en matière de protection des données devaient s'aligner sur celles prévues par le droit civil. Au lieu de créer un système d'actions spécifiques, il a ainsi choisi de renvoyer aux art. 28 ss CC, tout en insérant dans la LPD quelques règles particulières.

La personne concernée par un traitement de données dispose ainsi d'une part des actions prévues par les art. 28*a* et 28*l* du CC[96] (par renvoi de l'art. 15, al. 1, LPD), et d'autre part des actions spécifiques à la protection des données, telles l'action en mention du caractère litigieux (art. 15, al. 2, LPD), l'action en rectification (art. 5, al. 2, et 15, al. 2, LPD) et l'action en exécution du droit d'accès (art. 8 et 15, al. 4, LPD).

Ces actions sont subordonnées (à l'exception de l'action en exécution du droit d'accès, voire de l'action en rectification) à l'existence d'une atteinte illicite à la personnalité de la personne concernée (art. 12, al. 1, LPD).

L'art. 12, al. 2, LPD énumère de manière non exhaustive les principaux cas d'atteinte à la personnalité résultant d'un traitement de données personnelles. Il s'agit:

- du traitement des données personnelles en violation des principes généraux définis aux art. 4, 5, al. 1, et 7, al. 1, LPD;
- du traitement de données contre la volonté expresse de la personne;
- de la communication à des tiers des données sensibles ou des profils de la personnalité.

Précisons qu'il n'y a en règle générale pas d'atteinte à la personnalité lorsque la personne concernée a rendu les données accessibles à tout un chacun et ne s'est pas opposée formellement au traitement (art. 12, al. 3, LPD). L'illicéité de l'atteinte peut, suivant le régime normal prévu en matière de droits de la personnalité, être levée en présence d'un motif justificatif, soit la loi, le consentement de la victime, ou un intérêt prépondérant privé ou public (art. 13, al. 1, LPD, art. 28, al. 2, CC)[97]. L'art. 13, al. 2, LPD donne une liste exemplative des intérêts prépondérants de l'auteur du traitement susceptibles d'entrer en ligne de compte.

---

95 FF 1988 II 421 ss, 470 s.; ATF 138 II 346, consid. 8, et, entre autres, *Meier*, n° 332.

96 Ce renvoi concerne toutes les actions défensives de l'art. 28*a* CC, mais aussi l'action en exécution du droit de réponse (art. 28*l* CC) et les actions en réparation réservées par l'art. 28*a*, al. 3, CC.

97 Le Tribunal fédéral a jugé qu'un tel motif pouvait aussi justifier l'atteinte prévue à l'art. 12, al. 2, let. a, LPD, bien qu'il faille dans ce cas ne l'admettre qu'avec une extrême prudence (ATF 136 II 508, consid. 6.3.2/JT 2011 II 446).

b) La responsabilité des fournisseurs en particulier

Sous réserve de règlementations spéciales, les fournisseurs, dans la mesure où ils traitent des données personnelles, sont soumis à la LPD[98]. Cette loi ne prévoyant pas de disposition particulière les concernant, leur responsabilité est régie par ses règles générales. Compte tenu du renvoi de l'art. 15, al. 1, LPD à l'art. 28 CC, ce qui a été dit sur la légitimation passive en cas d'atteinte à la personnalité[99] s'applique aussi ici[100].

En lien avec la thématique de la responsabilité du fournisseur pour le comportement de tiers, on peut imaginer les cas suivants:

- Les utilisateurs d'un réseau social publient des données sensibles relatives à des tiers sans motif justificatif (photo relevant de la sphère intime, bilan médical, condamnation pénale; voir art. 3, let. c, LPD) et violent ainsi l'art. 12, al. 2, let. c, LPD;
- Les utilisateurs d'un réseau social, les participants à un blog ou plus largement les bénéficiaires d'un contrat d'hébergement publient des données personnelles fausses d'une personne, ou les publient contre sa volonté, violant ainsi l'art. 12, al. 2, let. a ou b, LPD.

c) Travaux de révision de la LPD

La LPD a fait l'objet d'une évaluation de 2010 à 2011. Il en est ressorti que les développements technologiques et sociétaux intervenus depuis l'entrée en vigueur de la loi avaient entraîné de nouvelles menaces pour la protection des données, et que l'efficacité de la loi pouvait être améliorée. Compte tenu des conclusions du rapport, le Conseil fédéral a donné le mandat au DFJP d'examiner quelles mesures seraient susceptibles d'améliorer l'efficacité de la loi et de lui faire des propositions sur la suite des travaux d'ici à fin 2014, en tenant compte des développements au plan de l'Union européenne et du Conseil de l'Europe.

Un groupe de travail a été mis sur pied par l'OFJ pour accompagner les travaux. Il a examiné une large palette de mesures, qui sont présentées dans le document « Esquisse d'acte normatif, Rapport du groupe d'accompagnement Révision LPD du 29 octobre 2014 »[101].

Par décision du 1er avril 2015, le Conseil fédéral a chargé le DFJP d'élaborer, en collaboration avec le Préposé fédéral à la protection des données (PFPDT), le Département fédéral de l'économie, de la formation et de la recherche, le Département fédéral des finances et le Département fédéral de l'intérieur, un projet pour la consultation externe d'ici fin août 2016 au plus tard. Ce calendrier devrait permettre de tenir compte des réformes en cours au plan européen, et qui pourraient aboutir fin 2015 ou début 2016. Le Conseil de l'Europe se penche en effet actuellement sur la modernisation de sa Convention du 28 janvier 1981 pour la protection des personnes à l'égard du traitement automatisé des données à caractère

98 Voir la contribution du Préposé fédéral à la protection des données « La protection des données et Internet » de l'été 2000, consultable à l'adresse www.edoeb.admin.ch/datenschutz/00628/00665/index.html?lang=fr&___fr___=.

99 Ch. 3.2.2.

100 Voir le message du Conseil fédéral du 23.3.1988 concernant la loi fédérale sur la protection des données (LPD), FF 1988 II 421 ss, 471.

101 Ce texte peut être consulté sous: www.ofj.admin.ch > Etat & Citoyen > Projets législatifs en cours > Renforcement de la protection des données > Rapports.

personnel (Convention STE 108)[102], et l'UE planche sur un projet de règlement général sur la protection des données (règlement UE) ainsi que sur un projet de directive concernant le domaine de la coopération judiciaire et policière (projet de directive UE). Ces deux derniers textes devraient remplacer respectivement la directive 95/46/CE[103] et la décision-cadre 2008/977/JAI[104]. Le projet de révision de la LPD devra notamment permettre à la Suisse, le moment venu, de ratifier la Convention STE 108 modernisée, de transposer la nouvelle directive UE et le nouveau règlement UE (pour autant qu'ils relèvent de l'acquis de Schengen/Dublin) et de mettre en œuvre les recommandations reçues dans le cadre de l'évaluation Schengen du printemps 2014[105].

Parmi les mesures examinées pour le secteur privé figurent[106]: la protection des données plus en amont et par défaut (« *privacy by design* » et « *privacy by default* »); le devoir de procéder à des analyses d'impact en cas de risque accru de violation de la personnalité; des mesures permettant d'accroître la transparence des traitements (par ex., dans le secteur privé, l'extension du devoir d'information, lors de la collecte des données, à tous les types de données personnelles) et des mesures qui assurent une meilleure maîtrise et un meilleur contrôle de leurs données personnelles par les personnes concernées (par ex. renforcement des pouvoirs du PFPDT). Il est également envisagé de mettre en place un mode alternatif de règlement des conflits (médiation/conciliation). Il est au surplus prévu d'examiner d'autres mesures, telles la promotion de l'autorégulation, l'allégement de la charge administrative pour les responsables du traitement et le renforcement des moyens dont disposent les particuliers pour faire valoir leurs droits.

Sous réserve de dispositions spéciales, les fournisseurs seront à l'avenir, comme ils le sont aujourd'hui, soumis aux obligations que leur impose la LPD.

3.2.4 Loi sur la concurrence déloyale

a) Bases juridiques

La LCD comporte un élément de droit de la personnalité[107]: elle vise à protéger la liberté économique, qui est l'une des facettes de ce droit[108]. A noter que la mention du dénigrement à l'art. 3, al. 1, let. a, LCD doit être comprise comme une concrétisation, sous l'angle de la concurrence, de la protection générale de la personnalité[109].

---

[102] Que la Suisse a ratifiée, ainsi que son protocole additionnel, respectivement le 2.10.1997 (RS 0.235.1) et le 20.12.2007 (RS 0.235.11).

[103] Directive 95/46/CE du Parlement européen et du Conseil du 24.10.1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, JO L 281 du 23.11.1995, p. 31.

[104] Décision-cadre 2008/977/JAI du Conseil du 27.11.2008 relative à la protection des données à caractère personnel traitées dans le cadre de la coopération policière et judiciaire en matière pénale, JO L 350 du 30.12.2008, p. 60.

[105] La Suisse fait l'objet d'évaluations périodiques dans le cadre de sa participation à la coopération Schengen. Lors de l'évaluation de 2014, les experts européens ont notamment recommandé à la Suisse de conférer des pouvoirs décisionnels au PFPDT.

[106] Pour des explications détaillées sur les différentes mesures, voir le rapport du groupe d'accompagnement (note de bas de page 101).

[107] *Jung*, Handkommentar UWG, Einleitung nº 18; *Baudenbacher*, ad art. 1 nº 76 ss. ; *von Büren*, Allgemeines, nº 8 ss.

[108] ATF 123 III 354, consid. 1b.

[109] ATF 123 III 354, consid. 1b.

En outre, l'art. 3, al. 1, let. b, LCD (indications fallacieuses en général) peut fonder une prétention contre un fournisseur, de même que l'art. 3, al. 1, let. d, LCD (fait de faire naître une confusion) et, bien entendu, l'art. 2 LCD (clause générale). La LCD vise, dans l'intérêt de toutes les parties concernées (les agents économiques comme les concurrents directs, les clients à tous les échelons, etc.), à protéger la concurrence loyale (art. 1 LCD). L'existence d'une relation de concurrence directe n'est pas nécessaire pour que la LCD s'applique[110].

Celui qui, par un acte de concurrence déloyale, subit une atteinte dans ses intérêts économiques en général ou celui qui en est menacé, peut intenter une action en interdiction, en cessation ou en constatation de l'atteinte contre l'auteur de celle-ci (art. 9, al. 1, LCD). Est réprouvé 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 (art. 2 LCD). L'acte incriminé doit être objectivement propre à influer sur le jeu normal de la concurrence; il n'y a pas besoin qu'un comportement fautif ait été constaté[111]. De même, les actions défensives fondées sur l'art. 9 LCD n'exigent rien d'autre que l'illicéité[112] (objective) de l'acte incriminé.

b) Légitimation passive dans le cas de violations de la LCD: principes formulés dans la jurisprudence du Tribunal fédéral

Les actions en interdiction et en cessation de l'atteinte visent des personnes qui influent sur le jeu normal de la concurrence, autrement dit qui « perturbent » la concurrence. La législation vise donc les « perturbateurs », lesquels peuvent aussi être des tiers qui ne sont pour rien dans la violation proprement dite.

> « *Bezüglich negatorischer Klagen ist passiv legitimiert, wer den Wettbewerb durch ein unlauteres Verhalten stört. Um den lauteren Wettbewerb wirksam schützen zu können, ist von einem weiten Begriff des Störers auszugehen. Dieser erfasst nicht nur den eigenverantwortlichen Verletzer, sondern auch Personen, welche einen Dritten zur Begehung eines Wettbewerbsverstosses anstiften, bei unlauterem Wettbewerbsverhalten Hilfestellung leisten oder solches Verhalten für sich ausnutzen, sofern sie den Wettbewerbsverstoss verhindern könnten.* »[113]

Il s'ensuit que le fabricant répond des pratiques anticoncurrentielles de ses distributeurs indépendants, s'il a permis ou favorisé ces pratiques d'une manière qui lui est imputable[114].

Dans l'arrêt Tiq of Switzerland du 22 février 2006, le Tribunal fédéral constate ce qui suit :

---

[110] Arrêt du Tribunal fédéral 4C.139/2003 du 4.9.2003 (CAP), consid. 5.1, in sic! 2004, 432.

[111] *Müller Jürg*, SIWR V/1, 53; cf. arrêt du Tribunal fédéral du 4.9.2003 CAP (note 110), consid. 5.1; ATF 136 III 23, consid. 9.1 avec des renvois à d'autres arrêts du Tribunal fédéral.

[112] En droit de la concurrence, le principe de la bonne foi pose la limite entre ce qui est permis et ce qui est illégal: tout acte de concurrence (objectivement) contraire aux règles de la bonne foi est déloyal et, partant, illicite (*Müller*, SIWR V/1, 52 s.).

[113] *Baudenbacher/Glöckner*, ad art. 11 LCD n° 5. « Des actions défensives peuvent être engagées contre quiconque perturbe la concurrence par un comportement déloyal. Afin de pouvoir protéger efficacement la concurrence loyale, la notion de « perturbateur » doit être comprise au sens large. Elle désigne non seulement la personne qui a commis la violation sous sa propre responsabilité, mais encore toute personne qui incite un tiers à commettre une infraction à la concurrence, qui prête son concours à un acte de concurrence déloyale ou qui tire profit d'un tel acte, alors qu'elle pourrait empêcher l'infraction à la concurrence. » (Traduction).

[114] *Baudenbacher/Glöckner*, ad art. 11 LCD n° 13.

> « *Im angefochtenen Urteil wird der Beklagten verboten, die definierten täuschenden Angaben durch Dritte verwenden zu lassen. Das 'Verwendenlassen' setzt voraus, dass die untersagte Verwendung durch Dritte von der Beklagten genehmigt bzw. zumindest toleriert wird und sie die Möglichkeit hätte, etwas dagegen zu unternehmen. Damit betrifft das Verbot nur Handlungen Dritter, welche der Beklagten zugerechnet werden bzw. als Störerin angelastet werden können, weshalb auch in diesem Punkt eine zu weite Formulierung des Verbots zu verneinen ist.* »[115]

Le cercle des personnes qui peuvent être visées par une action englobe également les instigateurs, les complices et les coauteurs. Une contribution à l'acte est suffisante; comme il est mentionné plus haut, il n'est pas nécessaire qu'une faute ait été commise[116].

c) Légitimation passive des médias dans le cas de violations de la LCD

Toute personne qui contribue ou a contribué directement à la propagation de propos déloyaux peut être visée par une action, soit le journaliste, l'auteur de l'article, l'éditeur, le rédacteur responsable et le diffuseur du produit de presse[117].

d) Légitimation passive des fournisseurs dans le cas de violations de la LCD

Selon la doctrine, le vaste principe du « perturbateur » (en droit de la concurrence) et la légitimation passive des médias qui en découle, également vaste, s'appliquent aussi aux fournisseurs[118]. Si l'on considère que l'illicéité (objective) suffit à fonder la légitimation passive[119], il est permis de douter qu'il s'agisse de déterminer, par exemple dans le cas d'offres déloyales sur des plateformes de vente aux enchères comme eBay ou Ricardo, si les exploitants de plateformes s'identifient ou non aux offres ou s'ils en ont connaissance ou non, comme le soutient une partie de la doctrine[120]. Il faut plutôt partir du principe que tout perturbateur (et donc tout exploitant de plateforme) qui participe à un acte de concurrence déloyale peut tomber sous le coup de la loi, par le biais d'une action défensive.

---

[115] Arrêt du Tribunal fédéral 4C.361/2005 du 22.2.2006 Tiq of Switzerland, consid. 3.8.3, in sic! 2006, 583 ss. « Dans l'arrêt attaqué, le défendeur a l'interdiction de laisser des tiers utiliser les indications trompeuses définies. 'Laisser utiliser' suppose que l'utilisation interdite par des tiers a été autorisée ou du moins tolérée par le défendeur et que celui-ci aurait eu la possibilité d'entreprendre quelque chose pour y remédier. En conséquence, l'interdiction ne touche que les actes de tiers qui peuvent être imputés au défendeur ou qui peuvent lui être reprochés en tant que perturbateur, c'est pourquoi une formulation trop large de l'interdiction doit être rejetée là aussi. » (Traduction).

[116] *Rauber*, SIWR V/1, 269 ; voir *von Büren*, ad art. 2 à 6 n° 58 ; *Schaltegger*, 96 avec d'autres références; voir aussi ch. 3.2.2.

[117] Arrêt du Tribunal fédéral 4C.224/2005 du 12.12.2005 Agefi/Edipresse, in sic! 2006, 280, 281, avec d'autres références ; BSK UWG-*Rüetschi*, ad art. 11 n° 5 ; *Schaltegger*, 96 : « *Passiv legitimiert sind deshalb neben dem Verfasser des Pressebeitrages vor allem der verantwortliche Redaktor und Verleger, aber auch der Drucker, Setzer, Vertreiber und Herausgeber eines Presseproduktes. Diese alle können unabhängig von einander je einzeln eingeklagt werden* » (« Par conséquent, ont qualité pour défendre, outre l'auteur du produit de presse, avant tout le rédacteur responsable et l'éditeur, mais aussi l'imprimeur, le typographe, le diffuseur et le directeur de publication du produit de presse. Toutes ces personnes peuvent être poursuivies individuellement, indépendamment les unes des autres. » [Traduction]).

[118] Voir *Baudenbacher/Glöckner*, ad art. 11 n° 30 ss.

[119] *Müller*, SIWR V/1, 52 s. ; voir aussi ch. 3.1.2 et 3.2.2.

[120] *Spitz*, Handkommentar UWG, ad art. 9 n° 53.

Dans l'affaire Tribune de Genève jugée par le Tribunal fédéral[121], il aurait aussi fallu admettre la légitimation passive sous l'angle du droit de la concurrence, si un cas de dénigrement au sens de l'art. 3, al. 1, let. a, LCD avait été invoqué.

Les *fournisseurs d'hébergement* peuvent être visés par une action lorsqu'ils diffusent sur Internet des contenus tiers aux fins de leur utilisation. Cela devrait aussi être le cas lorsqu'ils n'ont aucune connaissance de l'infraction à la concurrence[122].

Il reste à déterminer dans quelle mesure les *fournisseurs d'accès* peuvent faire l'objet d'actions défensives fondées sur le droit de la concurrence. Quoi qu'il en soit, en vertu du vaste principe du perturbateur, une légitimation passive ne saurait être totalement exclue[123]: toutefois, un fournisseur d'accès pourrait toujours, selon le cas de figure, faire valoir qu'il se contente de donner aux utilisateurs l'accès au web et qu'il n'entre dès lors pas dans la définition du perturbateur[124]. Il n'empêche que la situation juridique n'est pas claire.

La responsabilité du fait des *hyperliens* n'est pas claire non plus. Une partie de la doctrine est d'avis que la légitimation passive doit être admise en la matière lorsque l'auteur du lien hypertexte fait sien, à titre exceptionnel, le contenu en question ou lorsqu'il en a connaissance[125].

e) Légitimation passive des exploitants de moteurs de recherche en particulier

Etant donné que, en relation avec le droit de la concurrence, l'ensemble des circonstances sont déterminantes, l'utilisation de métabalises et de mots clés, servant à optimiser le référencement, peut être anticoncurrentielle[126]. Les *métabalises* sont des termes, figurant dans le code source d'une page web, qui permettent aux moteurs de recherche de trouver la page en question, mais qui ne sont pas visibles sur celle-ci. Des termes faisant référence à un concurrent peuvent aussi servir de métabalises. Selon une décision cantonale, l'apparence de la page web affichée grâce aux métabalises utilisées est déterminante. Si elle éveille l'impression trompeuse que l'exploitant du site est une entreprise liée au concurrent (en affaires avec lui), il faudrait conclure qu'il existe un risque de confusion au sens du droit de la concurrence[127]. En présence de circonstances qualifiées, une pratique commerciale pourrait aussi tomber sous le coup de la clause générale du droit de la concurrence, énoncée à l'art. 2 LCD. La *publicité par mots clés* (Google AdWords, par ex.) consiste à afficher, parmi les résultats du moteur de recherche, la publicité correspondant au terme recherché par l'utilisateur. Là aussi, des marques de concurrents, par exemple, peuvent être utilisées comme mots clés pour faire figurer sa propre publicité[128]. Un juge cantonal a considéré qu'il n'y avait pas infraction à la LCD vu que les internautes peuvent clairement distinguer les annonces publicitaires des résultats de leur recherche[129]. Cependant, si des mots clés et des métabalises étaient utilisés d'une façon contraire au droit de la concurrence, une légitimation passive des exploitants de moteurs de recherche serait envisageable. La doctrine estime que ces derniers

[121] Arrêt du Tribunal fédéral 5A_792/2011 du 14.1.2013.
[122] Autre opinion: *Spitz*, Handkommentar UWG, art. 9 nº 54.
[123] Voir note 117.
[124] Concernant l'exigence de la causalité adéquate: voir ch. 3.2.2 b).
[125] *Spitz*, Handkommentar UWG, ad art. 9 nº 53.
[126] Voir cas d'application présentés dans *Bühler Gregor*, 60 ss.
[127] Arrêt du Tribunal de commerce du canton d'Argovie du 10.4.2001 Soda Stream, in sic! 2001, 532 ss., 538 (consid. 3a/IV).
[128] Voir l'exposé des faits dans l'arrêt du Tribunal supérieur du canton de Thurgovie du 7.9.2011 Ifolor, in sic! 2012, 387 ss.
[129] Arrêt du Tribunal supérieur du canton de Thurgovie du 7.9.2011 Ifolor, in sic! 2012, 387 ss., consid. 7.

peuvent faire l'objet d'une action en tant que « perturbateurs par situation », s'ils pourraient raisonnablement identifier l'aspect anticoncurrentiel et y remédier[130].

3.2.5 Droit de la propriété intellectuelle

a) Légitimation passive en droit de la propriété intellectuelle

A l'art. 62, al. 1, let. a et b, LDA, il est défini que la personne qui subit ou risque de subir une violation de son droit d'auteur peut demander au juge de l'interdire, si elle est imminente, ou de la faire cesser. D'autres actes législatifs régissant la propriété intellectuelle comprennent des dispositions identiques ou similaires (art. 55, al. 1, let. a et b, LPM; art. 35, al. 1, let. a et b, de la loi du 5 octobre 2001 sur les designs [LDes][131]; art. 72 LBI). A la différence de l'art. 28 CC qui régit le droit de la personnalité[132], seules quelques lois spéciales réglementent la question de la légitimation passive, par exemple à l'art. 66, let. d, LBI. En vertu de celui-ci, la personne qui incite à commettre l'un des actes au sens des let. a à c, qui y collabore, en favorise ou facilite l'exécution est passible de poursuites civiles. La LDes contient une disposition similaire à son art. 9, al. 2: le titulaire peut interdire à des tiers de « participer à une utilisation illicite, de la favoriser ou de la faciliter ». Dans une version précédente, la loi sur la protection des marques incluait également une disposition sur les actes de participation, laquelle n'a pas été maintenue dans la version révisée qui est entrée en vigueur le 1er avril 1993. Les travaux préparatoires ne permettent pas de conclure que l'objectif visé était de limiter la légitimation passive.

Dans le droit de la propriété intellectuelle, répondre à la question de savoir contre qui une action défensive (question de la qualité pour défendre[133]) peut être intentée n'est pas aisé. La *doctrine* dominante part du principe que la légitimation passive dans les cas d'actions défensives et en particulier la responsabilité du simple participant sont appréciées en application des art. 50 s. CO[134]. S'agissant des *prétentions en réparation*, les lois spéciales régissant la propriété intellectuelle se réfèrent unanimement aux règles du CO[135]. En vertu de l'art. 50, al. 1, CO, lorsque plusieurs ont causé ensemble un dommage, ils sont tenus solidairement de le réparer, sans qu'il y ait lieu de distinguer entre l'instigateur, l'auteur principal et le complice. Dans ce cas, aucune concertation n'est nécessaire, la connaissance réciproque de la contribution suffit[136]. La doctrine estime que cette règlementation de la participation doit dès lors aussi s'appliquer aux actions défensives en droit de la propriété intellectuelle[137]. Il n'est pas concevable qu'une personne soit tenue pour responsable d'un contenu illicite, mais qu'on ne puisse pas lui réclamer de le supprimer.

---

130 *Spitz*, Handkommentar UWG, ad art. 9 nº 34 ss.; *Hürlimann*, 62 s.
131 RS 232.12.
132 Voir ch. 3.2.2.
133 Voir ch. 3.2.1.
134 Voir liste des principaux ouvrages de référence, *Hess-Blumer*, sic! 2003, 99 ss.; *Schoch/Schüepp*, Jusletter du 13.5.2012, nº 28 avec de nombreuses autres références des différents domaines juridiques; *Frech*, 275; concernant la LDA : *Barrelet/Egloff*, ad art. 62 LDA nº 5; *Wullschleger*, nº 174 ss.; *Rehbinder/Viganò*, ad art. 62 LDA nº 9; *Schlosser*, CR PI, ad art. 62 LDA nº 5 s.; concernant la LPM : *Staub*, Handkommentar MSchG, ad art. 55 nº 24; *Schlosser*, CR PI, ad art. 5 LPM nº 4.
135 Voir art. 62, al. 2, LDA; art. 55, al. 2, LPM; art. 35, al. 2, LDes; art. 73, al. 1, LBI et infra : ch. 4.
136 Voir BSK OR I-*Graber*, ad art. 50 CO nº 6 ss.
137 Voir références dans la note 134.

La *jurisprudence* aussi fournit des exemples justifiant une telle interprétation. Dans l'ATF 107 II 82 (PTT)[138], le Tribunal fédéral a reconnu une demande en cessation de l'atteinte à l'égard des PTT en tant que constructrice d'un appareillage électronique d'ondes dirigées, du fait de sa complicité dans une violation du droit d'auteur, en se référant aux principes généraux de l'art. 50, al. 1, CO. *Hess-Blumer* reprend un arrêt du Tribunal de commerce du canton de Zurich en droit des marques qui admet la légitimation passive d'une fabricante d'enseignes lumineuses dont l'utilisation aurait porté atteinte à la marque[139].

Bien que la LBI et la LDes contiennent leurs propres dispositions sur la participation, une partie de la doctrine plaide en faveur du maintien de l'application de l'art. 50 CO[140], arguant que le souci du législateur était de créer une *règlementation* aussi *uniforme* que possible de la *protection juridique* dans les actes législatifs régissant la propriété intellectuelle et qu'il n'existait aucune raison objective d'apprécier différemment la question de la participation dans les dispositions du droit de la propriété intellectuelle. Aussi, l'acte du participant doit être considéré objectivement comme tout autant répréhensible (ou non) qu'il s'agisse d'une contribution à une violation du droit d'auteur ou à une violation du droit des marques. Une appréciation différenciée en fonction du domaine juridique doit être fondée sur l'acte principal et non sur la participation[141]. Dans son ATF 129 III 588 (machine à broder à navettes), le Tribunal fédéral a également souligné 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[142].

Pour admettre la légitimation passive d'un *fournisseur*, l'existence préalable d'un lien avec un acte illicite principal est par conséquent nécessaire. Ce dernier doit, de plus, être objectivement imminent[143]. La faute n'est pas requise. Enfin, la participation doit favoriser l'acte illicite principal. La notion de participation recouvre la contribution, l'instigation, la favorisation ou la facilitation de la violation d'un droit de propriété intellectuelle[144]. Il n'est cependant pas clair si la légitimation passive est comprise de façon identique ou moins large que dans le droit de la personnalité[145] où toute personne qui participe à une violation est habilitée, conformément à l'art. 28, al. 1, CC, à se défendre en justice. Jusqu'à présent, ni la doctrine ni la jurisprudence n'ont donné de réponse univoque à cette question[146]. Selon *Schoch/Schüepp*, la qualité pour défendre de participants à une violation d'un droit de propriété immatérielle peut être aussi étendue que celle que le Tribunal fédéral a reconnue dans l'affaire Tribune de Genève pour le droit de la personnalité[147].

b) Droit d'auteur

Malgré l'absence de règlementation de la participation dans la LDA, la doctrine et la jurisprudence approuvent majoritairement la possibilité d'intenter des actions défensives

---

[138] ATF 107 II 82, consid. 9.a.
[139] Tribunal de commerce de Zurich du 29.3.2001 (HG980397), rapporté par *Hess-Blumer*, sic! 2003, 99.
[140] *Hess-Blumer*, sic! 2003, 100 s.; *Schoch/Schüepp*, Jusletter du 13.5.2012, nº 27 ss.
[141] *Schoch/Schüepp*, Jusletter du 13.5.2012, nº 27.
[142] ATF 129 III 588, consid. 4.1.
[143] *Hess-Blumer*, sic! 2003, 101 avec d'autres références dans la note de bas de page 29.
[144] Voir les références dans la note 134.
[145] Voir ch. 3.2.2.
[146] Pour l'application des principes du droit de la personnalité: *Frech*, 275 avec d'autres références; autre opinion : *Wullschleger*, nº 212 ss.
[147] *Schoch/Schüepp*, Jusletter 13.5.2012, nº 34.

contre un participant[148]. En tant que participants à la violation de droits d'auteur commise par leurs utilisateurs, les fournisseurs engagent dès lors leur responsabilité selon les règles susmentionnées.

Le fournisseur peut aussi être poursuivi quand il se rend lui-même coupable de violations du droit d'auteur, par exemple si des contenus externes lui sont imputables. Dans la doctrine, d'aucuns sont d'avis qu'un fournisseur d'hébergement sur le site duquel sont chargés des contenus portant atteinte à des droits d'auteur commet lui-même une violation du droit d'auteur puisqu'il met à disposition, fait voir ou entendre les contenus en question (art. 10, al. 2, let. c, LDA)[149]. Concernant la responsabilité des fournisseurs de services (hébergeurs), l'assimilation entre contenus propres et contenus tiers est exceptionnellement confirmée lorsque, du point de vue d'un tiers, l'information se présente comme l'information propre de l'exploitant. En Allemagne, par exemple, YouTube a été rendue responsable de violations du droit d'auteur pour appropriation de contenus tiers[150]. En vertu de l'art. 8 du Traité de l'Organisation mondiale de la propriété intellectuelle sur le droit d'auteur (WCT)[151], la mise à la disposition du public d'une œuvre est réservée au titulaire du droit:

> « […] les auteurs d'œuvres littéraires et artistiques jouissent du droit exclusif d'autoriser toute communication au public de leurs œuvres par fil ou sans fil, y compris la mise à la disposition du public de leurs œuvres de manière que chacun puisse y avoir accès de l'endroit et au moment qu'il choisit de manière individualisée. »

En vertu des déclarations communes concernant l'art. 8 WCT, la « mise à disposition des conditions matérielles » ou la « simple fourniture d'installations destinées à permettre ou à réaliser une communication » ne constituent pas une communication au public.

> « Déclarations communes concernant l'article 8: Il est entendu que la simple fourniture d'installations destinées à permettre ou à réaliser une communication ne constitue pas une communication au public au sens du présent traité ou de la Convention de Berne […].»

Acceptées sous la pression des fournisseurs et des sociétés de télécommunications, les déclarations communes excluent uniquement leur responsabilité en tant qu'auteur principal (mais pas en tant que participant). Leur revendication de voir leur responsabilité limitée lorsque leur clientèle viole le droit d'auteur n'a donc pas abouti[152].

La LDA prévoit également une exception pour les reproductions provisoires de nature purement technique dont l'unique finalité est de permettre une transmission dans un réseau entre tiers par un intermédiaire et qui n'ont pas de signification économique indépendante (art. 24*a*, let. c, LDA).

c) Droit des marques

aa) Légitimation passive des fournisseurs d'accès et des fournisseurs d'hébergement

Une action défensive peut être dirigée contre toute personne qui intervient dans le domaine d'exclusivité protégé par le droit des marques, ce qui comprend aussi bien l'auteur primaire

---

[148] Voir les références dans la note 134.
[149] *Weber*, E-Commerce, 518.
[150] Arrêt du tribunal du land de Hambourg du 3.9.2010, Az. 308 O 27-09.
[151] RS 0.231.151, entrée en vigueur pour la Suisse le 1.7.2008.
[152] *Ficsor*, ad art. 8 n° C8.24.

que l'auteur secondaire[153]. Comme la légitimation passive des fournisseurs est régie par les dispositions sur la responsabilité des participants, on peut renvoyer aux explications ci-dessus[154]. Concernant les fournisseurs d'hébergement, la mise à disposition d'espace sur un serveur pouvant accueillir des sites Web peut être considérée, d'après le cours ordinaire des choses et l'expérience générale de la vie, comme propre à favoriser la violation de droits. C'est pourquoi la légitimation passive des fournisseurs d'hébergement est majoritairement confirmée aussi dans le droit des marques[155]. Concernant les fournisseurs d'accès, la situation juridique n'est pas claire, mais il n'est pas exclu non plus, selon un avis de doctrine, que les tribunaux accordent la légitimation passive aussi aux fournisseurs d'accès[156].

bb) Responsabilité du moteur de recherche (mots clés et métabalises)

En remarque liminaire, il faut relever que la doctrine dominante en Suisse estime que l'utilisation d'une marque d'un tiers dans la publicité par mots clés et dans les métabalises[157] ne constitue pas une violation de son *droit à la marque* parce que ces mots clés sont invisibles[158]. Elle considère que cela ne constitue pas un usage distinctif de la marque[159].

La question de la responsabilité des exploitants de moteurs de recherche se pose néanmoins dans ce contexte. A l'heure actuelle, une responsabilité *directe* du moteur de recherche pour une violation du droit des marques imputable à la simple mise à disposition d'une publicité par mots-clés semble exclue par la doctrine suisse. En effet, le moteur de recherche ne fait pas un usage « distinctif » de la marque[160]. En revanche, la responsabilité *indirecte* du moteur de recherche pour les violations causées par des tiers à l'aide de ce modèle d'affaires a fait couler davantage d'encre[161].

d) Droit des brevets

En vertu de l'art. 8 LBI, le détenteur du brevet peut interdire à des tiers d'utiliser l'invention professionnellement, l'offre et la mise en circulation faisant explicitement partie des actes d'utilisation. L'auteur de l'infraction, mais aussi le participant peuvent être poursuivis civilement et pénalement (art. 66, let. d, LBI)[162]. La participation peut notamment consister en l'intermédiation d'affaires qui enfreignent un brevet, en la facilitation de vente de produits portant atteinte à un brevet et en la mise à disposition de l'infrastructure permettant de commettre une violation de brevet. Dans son ATF 129 III 588 (machine à broder à navettes), le Tribunal fédéral a constaté que l'acte de participation doit présenter un lien de causalité adéquat avec la violation de brevet. Selon lui, lorsque l'offre et la mise en circulation portent sur des produits communément disponibles sur le marché, la question de l'acte de participation

---

153 *Marbach*, SIWR III/1, nº 1468.
154 Voir ch. 3.2.5 a).
155 *Staub*, Handkommentar MSchG, ad art. 55 nº 25; *Schoch/Schüepp*, Jusletter du 13.5.2012, nº 32.
156 *Schoch/Schüepp*, Jusletter du 13.5.2012, nº 32.
157 Voir à ce sujet ch. 3.2.4 e).
158 *Thouvenin/Dorigo*, Handkommentar MSchG, ad art. 13 nº 46 ss. (479 ss.) et la doctrine citée, voir aussi arrêt Ifolor, Tribunal cantonal de Thurgovie du 7.9.2011, in: sic! 2012, 387 ss.; autre opinion: *Reinle/Obrecht*, sic! 2009, 112.
159 Voir *Rivara*, AJP 2012, 1546 ss. pour une appréciation critique de cette question avec d'autres références.
160 Voir *Rivara*, AJP 2012, 1559 s., concernant les Google AdWords.
161 Voir *Rivara*, AJP 2012, 1562 ss.; concernant la publicité par mots clés dans le droit de la concurrence, voir ch. 3.2.4 e).
162 Voir ch. 3.2.5 a).

appelle généralement une réponse négative, sauf si les marchandises ont été expressément vendues pour une utilisation portant atteinte au brevet, ce qu'il faudrait qualifier d'instigation au sens de l'art. 66, let. d, LBI[163].

3.2.6 Différentes formes d'action: particularités des fournisseurs

a) Demande en prévention de l'atteinte ?

En vertu de l'art. 28*a*, al. 1, ch. 1, CC, le demandeur peut requérir le juge d'interdire une violation à son droit à la personnalité, si elle est imminente. Plusieurs lois spéciales comprennent des dispositions identiques ou similaires (art. 62, al. 1, let. a, LDA; art. 55, al. 1, let. a, LPM; art. 35, al. 1, let. a, LDes; art. 9, al. 1, let. a, LCD). Dans la pratique, le juge interdit dans la majorité des cas au défendeur d'accomplir l'acte incriminé sous menace de la peine prévue pour insoumission à une décision par l'art. 292 CP[164]. Par demande en prévention de l'atteinte, visant à empêcher une nouvelle mise en ligne (*stay down*), on entend ci-après une prétention à l'encontre d'un fournisseur sur l'infrastructure duquel un tiers a mis à disposition ou entend mettre à disposition une déclaration, une œuvre, etc. La finalité de cette prétention est d'empêcher la mise à disposition (réitérée) de ce contenu, typiquement après que celui-ci a été retiré (*take down*) dans le cadre d'une demande de retrait. Les prétentions à l'égard de l'auteur du dommage ne seront pas étudiées ici.

La demande en prévention de l'atteinte a une visée préventive et a, assortie de la menace de sanction, des conséquences lourdes. Selon la doctrine, il convient d'y accéder avec grande retenue et dans le respect du principe de la proportionnalité[165]. Un danger concret et imminent ou le fait de craindre sérieusement un comportement futur constituent la condition préalable pour formuler une requête en prévention de l'atteinte[166]. Le caractère hypothétique du risque d'une violation ne suffit pas. Un danger suffisamment concret peut résulter de deux situations. Premièrement, lorsqu'un utilisateur déterminé a déjà commis une violation et qu'il faut sérieusement craindre qu'il la répète. Deuxièmement, lorsque des circonstances très concrètes laissent supposer qu'une personne va commettre pour la première fois une violation[167]. Les exigences en matière de preuve liées à un *risque de réitération* sont moins strictes selon la jurisprudence du Tribunal fédéral[168]. Le risque de réitération est en effet présumé lorsqu'une violation a déjà eu lieu et que le défendeur continue de contester le caractère illicite de son comportement ou qu'il refuse de le modifier[169].

---

[163] ATF 129 III 588, consid. 4.1.
[164] BSK ZGB I-*Meili* ad art. 28a nº 2.
[165] BSK ZGB I-*Meili* ad art. 28*a* n° 2; *Hausheer/Aebi-Müller*, nº 14.13 ss.
[166] Voir ATF 95 II 481 consid. 11; BSK ZGB I-*Meili*, ad art. 28*a* nº 2; *Hausheer/Aebi-Müller*, nº 14.14; BSK UWG-*Rüetschi/Roth*, ad art. 9 nº 16; *Schlosser*, CR PI, ad art. 62 LDA nº 10.
[167] BSK UWG-*Rüetschi/Roth*, ad art. 9 nº 17 ss. ; *Schlosser*, CR PI, ad art. 62 LDA nº 12 ss. ; concernant l'action en prévention de l'atteinte et l'exigence d'un désistement formel de la partie défenderesse afin d'exclure le risque de réitération des actes présumés dans le droit de la concurrence, voir l'arrêt du Tribunal de commerce de St-Gall du 29.8.2006 Staubsauger, sic! 2007, 122 ss. avec d'autres références à la jurisprudence du Tribunal fédéral; voir aussi *Spitz*, Handkommentar UWG, ad art. 9 nº 63 ss.
[168] Voir références chez BSK UWG-*Rüetschi/Roth*, ad art. 9 nº 19 ss.
[169] Voir ATF 128 III 96 consid. 2.e (concernant la LPM) ; ATF 124 III 72 consid. 2.a (concernant la LCD) ; l'arrêt du Tribunal fédéral 5A_228/2009 du 8.7.2009 consid. 4.2 (concernant la protection de la personnalité) arrive à des conclusions différentes.

Une requête en prévention de l'atteinte doit en outre viser un acte concret et imminent et être formulée de façon suffisamment précise pour que l'acte incriminé soit identifiable sans autres pour le défendeur[170]. Le tribunal doit pouvoir exécuter l'interdiction requise sans avoir à rejuger le comportement en question[171].

En Suisse, aucune décision acceptant une action en prévention de l'atteinte n'a apparemment été rendue contre un fournisseur. Une *obligation générale de « stay down »* au sens où le fournisseur doit garantir qu'aucun contenu illicite ne soit plus mis en ligne sur son infrastructure semble exclue. Pour se conformer à une telle demande, le fournisseur devrait en effet soumettre toutes les données que ses clients souhaitent charger sur une plateforme centralisée à un contrôle (préalable). Une telle action présupposerait une obligation de surveillance étendue de la part du fournisseur[172] et serait, du moins en règle générale, en porte-à-faux avec les dispositions en vigueur qui limitent l'obligation aux actes concrets[173]. Une obligation de surveillance générale empièterait par ailleurs sur divers droits fondamentaux (par ex. la liberté d'opinion et d'information, la liberté des médias et la protection de la sphère privée des internautes). Toute atteinte aux droits fondamentaux doit être fondée sur une base légale suffisante, justifiée par un intérêt public et proportionnée (art. 36 Cst.). Lors de la pesée des intérêts, il faut tenir compte également de l'interdiction de la censure[174], qui est l'essence même de la liberté des médias (art. 17, al. 2, Cst.). Celle-ci est en contradiction avec un contrôle préventif général des contenus de communication. A la lumière de l'interdiction de la censure, la surveillance exercée par les autorités, mais aussi le fait de contraindre à un contrôle les fournisseurs de services techniques de transmission s'avèrent problématiques[175]. De plus, une surveillance globale de tous les contenus ne serait, dans la majorité des cas, guère réalisable ni raisonnable. C'est pourquoi la doctrine rejette majoritairement une obligation générale pour les fournisseurs de prévenir les violations futures de droits[176].

Même si la demande en prévention de l'atteinte vise seulement à prévenir la *réitération* d'une violation concrète, le juge ne pourra y donner suite que sous des conditions extrêmement strictes. D'un point de vue purement technique, il est impossible, pour un *fournisseur d'accès* qui procure un accès à l'ensemble de la Toile, de surveiller certains contenus à moins d'engager des moyens considérables. Pour répondre à la question de savoir si les *fournisseurs d'hébergement* sont concernés par l'obligation de surveillance, on cite souvent l'ATF 126 III 161[177]. La Cour suprême avait en effet rejeté, en l'espèce, l'argument d'une imprimerie qui avait imprimé de manière répétée des articles portant atteinte à l'honneur et qui se prévalait du fait de ne pas pouvoir contrôler les contenus qu'elle imprime. L'argument invoqué du manque de moyens pour exercer un contrôle n'a pas été admis pour deux raisons:

---

[170] Concernant la LDA: *Müller Barbara K.*, Handkommentar URG, ad art. 62 n° 3; concernant la LCD: *Spitz*, Handkommentar UWG, ad art. 9 n° 65 avec d'autres références à la jurisprudence du Tribunal fédéral.

[171] BSK UWG-*Rüetschi/Roth*, ad art. 9 n° 25.

[172] Voir à ce propos *Frech*, 42.

[173] Voir aussi art. 15, al. 1, de la directive sur le commerce électronique (voir ch. 3.3.1, a), bb)) : les Etats membres n'imposent pas aux fournisseurs de services au sens des art. 12, 13 et 14 une obligation générale de surveiller les informations qu'ils transmettent ou stockent, ni même de rechercher activement des faits ou des circonstances révélant des activités illicites.

[174] Voir ch. 1.3.2 c).

[175] Voir *Krüsi*, 286 ss.; voir aussi ch. 1.3.2.

[176] *Rosenthal*, Internet- Provider-Haftung – ein Sonderfall?, n° 65 ss.; *Frech*, 278 s.; *Auf der Maur/Steiner*, FS Weber, 425; *Fountoulakis/Francey*, medialex 2014, 181 s. ; *Beranek Zanon*, Jusletter IT du 11.12.2013, n° 128 (pour les hébergeurs de fichiers).

[177] Traduit dans Journal des Tribunaux 2000 I 292.

premièrement, il ne pouvait pas être pris en considération concernant une action défensive puisqu'il relevait de la question de la faute[178]; deuxièmement, l'imprimerie aurait dû, après la parution des premiers articles, être consciente du fait qu'elle participait à une atteinte à la personnalité et qu'il aurait par conséquent fallu mieux surveiller les contenus imprimés[179]. 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. Dans l'affaire susmentionnée jugée par le Tribunal fédéral, l'imprimerie aurait eu, en théorie, la possibilité de contrôler les contenus avant leur publication, mais pour un fournisseur d'hébergement qui stocke, selon les circonstances, une énorme quantité de données, l'obligation de surveillance entraînerait un retard conséquent de la mise en ligne des contenus licites. Il serait cependant imaginable qu'une requête en prévention de l'atteinte correctement formulée ordonnant à un fournisseur d'hébergement de prévenir la réitération d'une atteinte concrète par un utilisateur déterminé aurait des chances de succès[180]. L'adéquation et partant la proportionnalité d'une telle injonction devra être évaluée différemment en fonction des moyens du fournisseur d'influencer et de contrôler les contenus[181].

La question de l'obligation de surveillance telle qu'elle a été décrite par le Tribunal fédéral dans l'ATF 126 III 161[182] est pertinente dans un autre contexte également. Il convient d'examiner ci-après, dans le cadre des prétentions en réparation, dans quelles circonstances un fournisseur doit faire preuve d'une diligence accrue parce qu'au vu de circonstances particulières, il devrait anticiper une violation[183].

b) Action en cessation de l'atteinte, notamment verrouillage des adresses IP et DNS

aa) Introduction

La discussion sur les actions défensives à l'égard des fournisseurs ne saurait être exhaustive si l'on ne rappelle pas les moyens dont ils disposent pour faire cesser les atteintes ou pour retirer les contenus illicites.

En règle générale, les *fournisseurs d'hébergement* disposent des moyens techniques pour supprimer les contenus qu'ils mettent à disposition[184].

Les *fournisseurs d'accès* offrent à leur clientèle l'accès à la globalité d'Internet. Si l'on reconnaît la légitimation passive de simples fournisseurs d'accès, un grand nombre d'entreprises tombe dans le champ d'application de la loi: par principe, tous les fournisseurs d'accès donnent accès à tous les contenus, donc aussi à ceux qui sont illicites. Rien qu'en Suisse, on compte une douzaine de fournisseurs d'accès, et le seul moyen dont ils disposent pour empêcher l'accès à des contenus illicites est a priori le verrouillage.

---

[178] Consid. 5.a/bb, 166.
[179] Consid. 5.b/cc, 170.
[180] *Rosenthal* est d'un autre avis : Internet- Provider-Haftung – ein Sonderfall?, n° 68. Selon lui, une mise en ligne d'un contenu identique par la même personne n'est pas couverte par une action en cessation de l'atteinte puisque celle-ci ne peut se référer qu'à des contenus déjà bloqués et que la violation ne peut avoir lieu qu'en cas de déblocage des contenus.
[181] Sur la différenciation en fonction de la proximité avec le contenu, voir ch. 2.4.
[182] Consid. 5.a/bb, 166.
[183] Voir ch. 4.1.1.
[184] Voir cependant la remarque dans la note 38.

Tant les fournisseurs d'hébergement que les fournisseurs d'accès automatisent quantité de processus. Sans ces automatisations d'ailleurs, Internet ne serait pas devenu ce qu'il est aujourd'hui. Le revers de la médaille est que les premiers ne connaissent souvent pas les contenus qu'ils mettent à disposition. Quant aux seconds, ils sont encore moins en mesure de prendre connaissance des contenus diffusés à moins d'engager des moyens considérables.

Le *verrouillage des adresses IP* permet de bloquer l'accès à un serveur déterminé. Pour ce faire, le fournisseur supprime l'accès de ses clients à l'adresse IP attribuée à ce serveur. Par le biais d'un *verrouillage des adresses DNS*, le fournisseur d'accès bloque le processus qui consiste à « traduire » l'adresse Internet, sous sa forme parlante - le nom de domaine -, en une adresse IP, comme s'il effaçait dans son exemplaire de l'annuaire le numéro de téléphone d'une personne. Cette procédure ne fonctionne qu'en partie, à savoir que lorsqu'un nom de domaine est nécessaire pour la connexion.

Ces mesures ne sont que partiellement efficaces car leur contournement est relativement aisé. Dans le cas d'un verrouillage de l'adresse DNS, il suffit de connaître l'adresse IP ou d'appeler un autre serveur DNS (en quelque sorte avec un autre « exemplaire de l'annuaire »)[185]. Dans celui du verrouillage de l'adresse IP, l'internaute peut se connecter au serveur de destination via un serveur intermédiaire (serveur proxy). Le fournisseur a la possibilité de changer l'adresse IP sous laquelle il sauvegarde ses contenus pour être à nouveau atteignable sous le même nom. Le contournement, quant à lui, requiert davantage d'efforts dans la recherche d'offres. Les utilisateurs moins avisés sont dès lors moins enclins, pour des raisons de confort, à consommer des offres illégales[186]. Dans le cas du verrouillage des adresses IP surtout, mais aussi avec les autres mesures, le risque d'effets secondaires indésirables ne peut être exclu.

Il y a en effet 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 tous les autres contenus (licites) consultables sous la même adresse IP. De plus, certaines mesures de contournement (par ex. l'utilisation de serveurs proxy ou la commutation vers un autre serveur DNS) sont susceptibles de réduire la stabilité d'Internet. Enfin et surtout, des listes de blocage de plusieurs Etats ont déjà été publiées sur Wikileaks, ce qui attire justement l'attention de certains internautes sur les contenus bloqués.

bb) Verrouillage des adresses IP et DNS en droit civil

Aujourd'hui, il n'existe pas de base juridique explicite en droit civil autorisant le verrouillage des adresses IP et DNS. Un tribunal pourrait néanmoins ordonner un tel verrouillage. Il est cependant rare qu'un juge prescrive à un défendeur comment mettre en œuvre une mesure. Un tribunal pourrait simplement ordonner à un fournisseur d'accès de retirer les contenus illicites (ou d'éliminer toute possibilité d'accéder à ces contenus) sans nécessairement qualifier cette injonction de blocage ou de verrouillage. Il doit toutefois examiner au préalable la proportionnalité et l'adéquation de la mise en œuvre technique d'une telle mesure[187]. Un fournisseur d'accès pourrait dès lors invoquer, dans un cas concret, le fait qu'il ne lui est raisonnablement pas possible, d'un point de vue technique, de retirer les contenus illicites et que la mesure doit donc être considérée comme disproportionnée. Par exemple, si un tribunal ordonnait de mettre en œuvre des mesures non automatisables dans le cas de processus

[185] Appeler un autre serveur DNS n'est possible que si le verrouillage n'est pas opéré par le registre du nom de domaine; voir à ce propos art. 15 de l'ordonnance du 20.9.2002 sur les domaines Internet (ODI; RS 784.104.2).

[186] Voir aussi le rapport du groupe AGUR12 (note 19), recommandation 9.3.4.

[187] Voir ch. 3.2.2 et notamment les références dans les notes 72 ss.

automatisés, son injonction ne serait pas proportionnée si elle avait pour conséquence la cessation complète des activités du fournisseur.

cc) Digression: décisions de blocage d'accès en droit pénal et administratif

i) Droit pénal

Le retrait (*take down*) de pages Internet peut aussi être envisagé dans la procédure pénale. Il s'agit d'effacer des données illicites (par ex. en raison de leur contenu pornographique ou raciste, ou d'une atteinte à l'honneur). En droit pénal, on utilise pour ce faire les règles sur la *confiscation*.

La base légale varie: alors que la pornographie dite dure (art. 197, al. 4 et 5, CP) et les représentations de la violence (art. 135 CP) peuvent spécifiquement donner lieu à une confiscation (art. 197, al. 6, et 135, al. 2, CP), dans le cas de la pornographie douce (art. 197, al. 1 et 2, CP), de la discrimination raciale (art. 261bis CP) et des infractions contre l'honneur (art. 173 ss. CP), il faut recourir à la norme générale de l'art. 69 CP. L'application de cette norme pose cependant de nombreuses difficultés: la notion de données peut susciter la discussion en droit pénal, ainsi que l'interdiction de l'interprétation par analogie (art. 1 CP)[188].

La suppression des données est difficile, voir impossible, lorsque le fournisseur d'hébergement a son siège à l'étranger. On envisage alors parfois d'ordonner aux *fournisseurs d'accès de bloquer l'accès* en Suisse. On a aussi essayé d'empêcher l'accès à des pages Internet en interprétant de manière extensive les dispositions de procédure pénale (mesures de contrainte)[189]. Toutefois, comme les mesures de procédure pénale visent uniquement à assurer le bon déroulement de la procédure et sont toujours provisoires, cette base légale cesse de s'appliquer au plus tard à la fin de la procédure. Les autres bases légales évoquées par les ouvrages de doctrine (par ex. les clauses générales de police) sont aussi plus que douteuses[190]. A côté de cette question de principe, de nombreux autres problèmes se posent, notamment la pertinence de la mesure – qui peut être très facilement contournée – et sa proportionnalité (*overblocking*)[191].

ii) Droit administratif

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

---

[188] Analyse détaillée dans *Bommer*, 172 s., 178 s. Voir aussi l'arrêt 2014/250 du Tribunal cantonal de Vaud, Chambre des recours pénale, du 18.6.2014 (extraits publiés dans: Journal des Tribunaux 2014 III, 168, consid. 4d). L'arrêt concerne Google en tant qu'exploitant d'une plateforme informatique (blogspot.ch). Sur l'analogie en droit pénal suisse, voir BSK Strafrecht I-*Popp/Berkemeier*, ad art. 1 n° 31 ss, en particulier n° 42.

[189] Par ex. dans l'affaire Appel au peuple (voir l'arrêt du Tribunal fédéral 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 au sens des dispositions sur la confiscation et que le séquestre était donc aussi inenvisageable. Toutefois, il a demandé que les fournisseurs d'accès soient informés du fait qu'ils pouvaient se rendre coupables de complicité de l'acte principal s'ils ne procédaient pas au blocage. Voir aussi l'arrêt du Tribunal fédéral 1B_294/2014 du 19.3.2015 concernant une décision de blocage d'un ministère public sur la base de l'art. 69, al. 2, CP (« destruction ») adressée à un fournisseur de domaine Internet (« registraire ») en raison de contenus présumés punissables.

[190] Voir *Bommer*, 200; *Schwarzenegger*, 267 s.

[191] Voir ch. 3.2.6 a et ch. 7.1.2, ainsi que l'arrêt du Tribunal fédéral 1B_294/2014 du 19.3.2015, consid. 4.5.

Ainsi, en vertu de l'art. 15, al. 1 et 2, ODI, les registres doivent bloquer un *nom de domaine* s'il existe un soupçon fondé de présumer que le nom de domaine en question est utilisé pour accéder par des méthodes illicites à des données critiques ou pour diffuser des logiciels malveillants, et si un service de lutte contre la cybercriminalité reconnu par l'OFCOM a présenté une demande de blocage. En l'absence de demande, le registre peut bloquer un nom de domaine durant cinq jours ouvrables au maximum. La mesure peut être maintenue au-delà des cinq jours en cas de demande de blocage subséquente. Ces dispositions ne sont cependant guère pertinentes au regard de la problématique que nous examinons ici, car elles reposent sur un examen des noms de domaine par des procédés automatiques, en fonction de leurs caractéristiques techniques.

La loi fédérale du 21 mars 1997 instituant des mesures visant au maintien de la sûreté intérieure (LMSI)[192] prévoit également une possibilité de blocage. Lorsque du matériel est susceptible de servir à des fins de propagande et que son contenu incite, d'une manière concrète et sérieuse, à faire usage de la violence contre des personnes ou des objets, l'Office fédéral de la police (fedpol) peut, après avoir consulté le Service de renseignement de la Confédération, soit ordonner la suppression du site concerné si le matériel de propagande se trouve sur un serveur suisse, soit recommander aux fournisseurs d'accès suisses de bloquer le site concerné si le matériel de propagande ne se trouve pas sur un serveur suisse (art. 13*e*, ch. 5, LMSI).

Le Service de coordination de la lutte contre la criminalité sur Internet (SCOCI)[193] rattaché à fedpol est le point de contact central pour les personnes souhaitant signaler l'existence de sites ou contenus Internet suspects[194]. Les contenus signalés font l'objet d'un premier examen et sont sauvegardés, puis les signalements sont transmis aux autorités de poursuite pénale en Suisse ou à l'étranger. Le SCOCI parcourt en outre la Toile à la recherche de contenus illicites. Ce service a été créé fin 2001 sur la base d'un arrangement administratif du DFJP et de la Conférence des directrices et directeurs des départements cantonaux de justice et police et est rattaché à la Police judiciaire fédérale – l'une des divisions principales de fedpol. Le SCOCI soutient les fournisseurs d'accès à Internet dans leur effort pour bloquer l'accès aux sites contenant ou soupçonnés de contenir de la pédopornographie, en leur transmettant une liste des sites Internet étrangers offrant ce type de pornographie malgré une demande de suppression des contenus illicites. Depuis juillet 2014, il dresse également une liste des sites de pornographie qui ont pour contenu des actes sexuels avec des animaux ou comprenant des actes de violence. L'initiative sectorielle de l'Association suisse des télécommunications (Asut)[195] contient la disposition suivante: « *Les signataires intègrent cette liste dans leurs systèmes, bloquent les adresses en question et empêchent ainsi l'accès de leurs clients aux sites internationaux de pornographie pédophile depuis la Suisse. La liste est régulièrement complétée par le SCOCI et prise en considération par les signataires sous sa forme actualisée* »[196]. Les principaux fournisseurs d'accès à Internet de Suisse ont adhéré à cette initiative.

---

[192] RS 120.

[193] www.cybercrime.admin.ch.

[194] Voir aussi le rapport du Conseil fédéral « Jeunes et médias » du 13.5.2015, p. 30 s., sur le site : www.ofas.admin.ch > Thèmes > Questions de l'enfance et de la jeunesse > Protection des jeunes.

[195] Initiative sectorielle de l'Association suisse des télécommunications (Asut) de juin 2008 pour une meilleure protection de la jeunesse dans les nouveaux médias et pour la promotion de la compétence en matière de médias dans la société, consultable sous www.asut.ch > Publications > Initiative sectorielle.

[196] Asut 2008 (note 195), p. 4.

Le projet de *loi sur les jeux d'argent* prévoit à l'art. 84 la possibilité de bloquer l'accès à des jeux d'argent en ligne non autorisés dont l'exploitant a son siège à l'étranger et qui sont accessibles en Suisse[197]. L'AGUR12 a recommandé que dans les cas graves, les fournisseurs d'accès établis en Suisse soient tenus, sur ordre de l'autorité compétente, de bloquer l'accès aux portails proposant des sources manifestement illégales par le biais du verrouillage des adresses IP et DNS[198]. La mise en œuvre de cette recommandation passera sans doute par une mesure de droit administratif, même si elle est inscrite dans la LDA, soit un acte de droit civil.

dd) Jurisprudence de la CEDH

Les mesures de verrouillage des adresses IP et DNS peuvent entrer en conflit avec des droits de l'homme, notamment la liberté d'opinion (art. 16 Cst. et art. 10 CEDH)[199]. Dans l'affaire Ahmet Yildirim contre la Turquie[200], la Cour européenne des droits de l'homme a déclaré que la CEDH n'excluait pas a priori les décisions de blocage de sites par les autorités, mais que celles-ci devaient reposer sur une base légale suffisamment précise et être faites de manière à éviter que des contenus légaux soient bloqués en même temps que les contenus illégaux.

Dans cet arrêt, la Cour européenne a déclaré contraires à la Convention les mesures prises par les autorités turques. Celles-ci, pour lutter contre un site portant atteinte à la mémoire d'Atatürk, avaient provisoirement bloqué l'accès à sites.google.com. Aux yeux de la Cour, de telles restrictions appellent de la part des tribunaux un examen des plus scrupuleux, afin d'éviter des risques d'arbitraire. Elle a notamment reproché aux autorités turques de ne pas même avoir considéré des mesures ayant moins d'effets collatéraux avant d'ordonner le blocage total de l'accès à Google sites.

Dans l'affaire Yaman Akdeniz contre la Turquie[201], la Cour européenne a dénié à un utilisateur de services Internet de diffusion de musique, bloqués pour des raisons de protection des droits d'auteur, la qualité de victime et donc la qualité pour présenter une requête. Dans ses considérants, elle a souligné que les Etats membres avaient une grande marge d'appréciation quant à la restriction de la liberté d'expression dans le domaine purement commercial – contrairement au domaine politique[202].

3.3 Droit étranger

3.3.1 Union européenne

a) Directives

aa) Directives 95/46/CE (directive sur la protection des données) et 2002/58/CE (directive vie privée et communications électroniques)

La protection des données en droit privé est régie dans l'Union européenne principalement par la directive 95/46/CE relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (directive sur la

[197] A consulter sur le site: www.ofj.admin.ch > Economie > Projets législatifs en cours > Jeux d'argent.
[198] Rapport final AGUR12 (note 19), recommandation 9.3.4.
[199] Sur la portée (largement identique) de ces deux dispositions, voir le ch. 1.3.2 c).
[200] Cour EDH, 18.12.2012, n° 3111/10, Ahmet Yildirim c. Turquie.
[201] Cour EDH, 11.3.2014, n° 20877/10, Yaman Akdeniz c. Turquie.
[202] Cour EDH, 11.3.2014, n° 20877/10, Yaman Akdeniz c. Turquie, ch. 28. Sur l'arrêt, voir aussi *Zeller*, medialex 2014, 209 ss.

protection des données)[203]. Elle est complétée par la directive 2002/58/CE concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques (directive vie privée et communications électroniques)[204].

La directive sur la protection des données ne contient pas de règles particulières concernant les fournisseurs. Elle s'applique principalement aux « responsables du traitement », au sens de son art. 2, let. d.

L'art. 6 de la directive donne mandat aux États membres de prévoir que les données à caractère personnel ne doivent être traitées que moyennant le respect de certains principes, notamment ceux de licéité, de proportionnalité, de finalité et d'exactitude. Il mentionne qu'il incombe au responsable du traitement d'assurer le respect de ces principes. L'art. 7 précise à quelles conditions un traitement est licite.

Lorsqu'un traitement ne satisfait pas aux dispositions de cette directive, notamment en raison du caractère incomplet ou inexact des données, les États membres doivent garantir le droit d'obtenir du responsable du traitement, selon les cas, la rectification, l'effacement ou le verrouillage des données (art. 12, let. b). La directive reconnaît au surplus à une personne concernée le droit de s'opposer à tout moment à un traitement pour des raisons prépondérantes et légitimes, sauf en cas de disposition contraire du droit national. La directive prévoit également un droit d'accès (art. 12, let. a). Comme on l'a mentionné au ch. 3.2.3, let. c, un projet de règlement est actuellement en voie d'élaboration au sein de l'UE. Il remplacera l'actuelle directive sur la protection des données. Selon les indications dont nous disposons, le projet devrait aboutir fin 2015 ou début 2016.

Le projet de règlement UE, selon l'orientation générale adoptée par le Conseil JAI le 15 juin 2015[205], reprend la liste des principes de l'actuel art. 6 de la directive sur la protection des données, ainsi que les conditions auxquelles un traitement est licite. Il reprend aussi le droit d'opposition (art. 19) et de rectification (art. 16). Il introduit notamment un droit à l'oubli numérique et à l'effacement (art. 17), des mesures sur le profilage (art. 20) et un droit à la portabilité des données (art. 18). Le projet ne prévoit pas de règles spéciales pour les fournisseurs. Il élargit la responsabilité aux sous-traitants (art. 77).

La Suisse ne sera pas liée par le règlement UE dans le domaine privé. Toutefois, si elle souhaite que l'UE reconnaisse à sa législation en matière de protection des données un niveau de protection adéquat (ce qui permet de faciliter les échanges de données entre la Suisse, considérée comme Etat tiers, et les Etats membres de l'UE), elle a tout intérêt à renforcer elle aussi ses textes législatifs en se rapprochant de la législation européenne, même si elle n'est pas tenue de coller au texte européen.

bb) Directive 2000/31/CE (directive sur le commerce électronique)

Dans l'UE, la responsabilité des fournisseurs est définie par les règles spécifiques de la directive sur le commerce électronique[206].

---

[203] Voir note 103.

[204] Directive 2002/58/CE du Parlement européen et du Conseil du 12.7.2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques, JO L 201 du 31.7.2002, p. 37.

[205] A consulter sous: http://www.consilium.europa.eu/fr/press/press-releases/2015/06/15-jha-data-protection/.

[206] Voir note 43.

Cette directive exempte les fournisseurs d'accès et d'hébergement (prestataires)[207] établis dans l'UE de la responsabilité des informations transmises s'ils remplissent certaines conditions. Cette exemption couvre tous les domaines du droit et vise tant la responsabilité civile que pénale[208].

Un fournisseur d'accès ne peut pas être rendu responsable s'il n'est pas à l'origine de la transmission, qu'il ne sélectionne pas le destinataire de la transmission et qu'il ne sélectionne et ne modifie pas les informations faisant l'objet de la transmission (art. 12).

Selon l'art. 14 de la directive, les prestataires qui stockent des informations sur leurs serveurs (fournisseurs d'hébergement) n'ont pas non plus à répondre des informations transmises, du moins tant qu'ils n'ont pas connaissance de l'activité illicite; une fois qu'ils en ont connaissance, ils doivent agir promptement pour retirer les informations ou rendre l'accès à celles-ci impossible.

L'art. 15 de la directive prévoit que les États membres ne doivent pas imposer aux prestataires une obligation générale de surveiller les informations qu'ils transmettent ou stockent, ou une obligation générale de rechercher activement des faits ou des circonstances révélant des activités illicites. Pourtant, le dernier paragraphe des art. 12 à 14 prévoit que les prestataires peuvent être obligés, conformément aux systèmes juridiques nationaux, de mettre fin à une violation *ou de la prévenir*. Plusieurs auteurs de doctrine pensent que le privilège – l'exonération de responsabilité – accordé par la directive devrait s'appliquer non seulement aux actions réparatrices, mais aussi aux actions en prévention ou en cessation de l'atteinte[209]. Ils estiment que l'art. 15, al. 1, de la directive devrait être appliqué dans tous les cas en relation avec les actions défensives. Dans la pratique, il existe donc une certaine incertitude juridique.

cc) Directive 2001/29/CE (directive sur l'harmonisation de certains aspects du droit d'auteur et des droits voisins dans la société de l'information)

L'art. 8, al. 3, de la directive 2001/29/CE sur l'harmonisation de certains aspects du droit d'auteur et des droits voisins dans la société de l'information (directive sur le droit d'auteur)[210] prévoit que les titulaires de droits puissent demander qu'*une ordonnance sur requête soit rendue à l'encontre des intermédiaires* dont les services sont utilisés par un tiers pour porter atteinte à un droit d'auteur ou à un droit voisin. De nombreux Etats membres[211] de l'UE ont mis en œuvre cette disposition par le biais d'un blocage d'accès aux adresses IP ou DNS[212].

De plus, l'art. 5, al. 1, de la directive sur le droit d'auteur prévoit une *exception au droit d'auteur* qui peut être revendiquée aussi par les fournisseurs:

> « Article 5 - Exceptions et limitations

[207] Pour la terminologie, nous renvoyons au ch. 2.3.1.
[208] *Verbiest/Spindler/Riccio Giovanni/van der Perré*, 4.
[209] Voir l'aperçu donné par *Härting*, n° 2136 s. avec des renvois dans la note de bas de page 4; voir aussi *Frech*, 253 ss; *Smith*, n° 2 à 162, note de bas de page 34: au moins tenir compte de l'art. 15 de la directive sur le commerce électronique par des injonctions.
[210] Directive 2001/29/CE du Parlement européen et du Conseil du 22.5.2001 sur l'harmonisation de certains aspects du droit de la propriété intellectuelle et des droits voisins dans la société de l'information, JO L 167 du 22.6.2001, 10.
[211] Voir la liste figurant dans le rapport final AGUR12 (note 19), 68.
[212] Concernant le verrouillage des adresses IP et DNS dans le droit suisse, voir ch. 3.2.6 b).

> (1) Les actes de reproduction provisoires visés à l'article 2, qui sont transitoires ou accessoires et constituent une partie intégrante et essentielle d'un procédé technique et dont l'unique finalité est de permettre:
>
> a) une transmission dans un réseau entre tiers par un intermédiaire, ou
>
> b) une utilisation licite
>
> d'une œuvre ou d'un objet protégé, et qui n'ont pas de signification économique indépendante, sont exemptés du droit de reproduction prévu à l'article 2. »

La directive sur le droit d'auteur ne définit donc pas l'auteur, mais plutôt l'*acte*. Toute personne qui accomplit l'acte en question peut par conséquent invoquer cette disposition.

dd) Directive 2004/48/CE (directive sur les droits de propriété intellectuelle)

La directive 2004/48/CE relative au respect des droits de propriété intellectuelle (directive sur les droits de propriété intellectuelle)[213] dispose en son art. 11 que les Etats membres veillent à ce que, lorsqu'une décision judiciaire a été prise constatant une atteinte à un droit de propriété intellectuelle, les autorités judiciaires compétentes puissent *rendre à l'encontre du contrevenant une injonction* visant à interdire la poursuite de cette atteinte. Les Etats membres doivent veiller également à ce que les titulaires de droits puissent demander une injonction à l'encontre des *intermédiaires* dont les services sont utilisés par un tiers pour porter atteinte à un droit de propriété intellectuelle. L'application de l'art. 8, al. 3, de la directive sur le droit d'auteur[214] est par conséquent étendue, au-delà des droits d'auteur et des droits voisins, aux autres droits de la propriété immatérielle[215].

A son art. 9, al. 1, let. a, la directive sur les droits de propriété intellectuelle demande en outre aux Etats membres de garantir aux tribunaux compétents la possibilité de rendre une ordonnance de référé à l'encontre d'un intermédiaire dont les services sont utilisés par un tiers pour porter atteinte à un droit de propriété intellectuelle[216].

b) Jurisprudence de la CJUE

Un grand nombre d'arrêts rendus par la Cour de justice de l'Union européenne (CJUE) permettent d'interpréter les directives pertinentes relatives à la responsabilité civile des fournisseurs.

aa) Système de filtrage: Scarlet contre SABAM et SABAM contre Netlog

En 2011, la CJUE a eu pour la première fois à trancher s'il est admissible ou non de soumettre un fournisseur d'accès à l'obligation d'introduire un système de filtrage en vue d'identifier l'échange de données portant atteinte au droit d'auteur dans son réseau et, le cas échéant, de bloquer la transmission des œuvres[217]. Une question similaire s'était posée pour l'exploitant d'une plateforme de réseau social que la CJUE avait considéré comme un fournisseur d'hébergement[218]. Dans les deux cas, la Cour est arrivée à la conclusion que les fournisseurs

[213] Directive 2004/48/CE du Parlement européen et du Conseil du 29.4.2004 relative au respect des droits de propriété intellectuelle, JO L 157 du 30.4.2004, 45.
[214] Voir ch. 3.3.1 a) cc).
[215] Voir *Neumann*, 228 ss.
[216] Concernant les mesures provisionnelles selon le droit suisse, voir ch. 6.1.2.
[217] Arrêt de la CJUE C-70/10 du 24.11.2011 (Scarlet c. SABAM).
[218] Arrêt de la CJUE C-360/10 du 16.2.2012 (SABAM c. Netlog).

ne pouvaient être tenus de mettre en place un système de filtrage global et sans limitation dans le temps même si, en vertu de l'art. 8, al. 3, de la directive sur le droit d'auteur et de l'art. 11, 3e phrase, de la directive sur les droits de propriété intellectuelle, les titulaires de droits peuvent demander une injonction judiciaire à l'encontre des fournisseurs pour que ces derniers prennent des mesures destinées à prévenir de nouvelles violations du droit d'auteur. Or un tribunal qui ordonnerait la mise en place d'un système de filtrage global et sans limitation dans le temps se placerait en contradiction avec l'exigence de garantir un juste équilibre entre le droit de propriété intellectuelle, d'une part, et la liberté d'entreprise, le droit à la protection des données à caractère personnel et la liberté de recevoir ou de communiquer des informations, d'autre part[219]. Dans ses considérants, la CJUE s'est notamment basée sur l'art. 15, al. 1, de la directive sur le commerce électronique, en vertu duquel les Etats membres ne doivent pas imposer aux fournisseurs de services une obligation générale de surveiller les informations qu'ils transmettent ou stockent[220], et sur l'art. 3 de la directive sur les droits de propriété intellectuelle, qui énonce que les mesures visées par cette dernière doivent être équitables et proportionnées sans être excessivement coûteuses[221].

bb) Blocage d'accès: UPC Telekabel Wien

La CJUE a décidé en 2014 qu'il était admissible, en droit européen, d'interdire par injonction du juge à un fournisseur d'accès de donner accès à ses clients à un site Web sur lequel des objets protégés sont mis à la disposition du public sans l'autorisation du titulaire de droits[222]. Elle a toutefois souligné la nécessité de prendre en compte les droits fondamentaux reconnus par le droit de l'Union (notamment la liberté d'entreprise du fournisseur d'accès à Internet et la liberté d'information des utilisateurs d'Internet). Le destinataire de l'injonction n'est pas tenu, selon la CJUE, de faire des sacrifices insupportables, notamment du fait qu'il n'est pas au premier chef l'auteur de l'atteinte au droit de propriété intellectuelle. L'injonction est compatible avec le droit de l'Union si elle ne prescrit pas quelles mesures concrètes le fournisseur d'accès doit prendre et qu'il puisse choisir celles qui conviennent à ses ressources et à ses possibilités. Avant d'être sanctionné, il doit avoir la possibilité de faire valoir « que les mesures prises étaient bien celles qui pouvaient être attendues de lui afin d'empêcher le résultat proscrit ». Il peut échapper aux astreintes visant à réprimer la violation de l'injonction en prouvant qu'il a pris toutes les mesures raisonnables, à condition cependant que les mesures prises ne privent pas inutilement les utilisateurs d'Internet de la possibilité d'accéder de façon licite aux (autres) informations disponibles. Ce point doit pouvoir être vérifié par un tribunal. Les législations de procédure nationales doivent donc offrir aux utilisateurs d'Internet de faire valoir leurs droits par la voie judiciaire[223]. La CJUE concède que les mesures mises en œuvre par le fournisseur d'accès n'ont peut-être pas totalement mis fin à la violation du droit de la propriété intellectuelle, éventuellement parce qu'elles peuvent être contournées. Le droit de propriété

[219] Arrêt de la CJUE C-70/10 du 24.11.2011 (Scarlet c. SABAM), nº 53; arrêt de la CJUE C-360/10 du 16.2.2012 (SABAM c. Netlog), nº 51.
[220] Arrêt de la CJUE C-70/10 du 24.11.2011 (Scarlet c. SABAM), nº 35; arrêt de la CJUE C-360/10 du 16.2.2012 (SABAM c. Netlog), nº 33.
[221] Arrêt de la CJUE C-70/10 du 24.11.2011 (Scarlet c. SABAM), nº 36; arrêt de la CJUE C-360/10 du 16.2.2012 (SABAM c. Netlog), nº 34.
[222] Arrêt de la CJUE C-314/12 du 27.3.2014 (UPC Telekabel Wien c. Constantin Film Verleih, Wega Filmproduktionsgesellschaft [kino.to]).
[223] Sur la mise en œuvre de l'arrêt de la CJUE C-314/12 en droit autrichien et sur les décisions de blocage dans d'autres Etats de l'UE, voir par ex. *Kraft*, Medien und Recht 2014, 171 ss.

intellectuelle n'étant cependant pas intangible, elle estime que sa protection ne doit pas nécessairement être assurée de manière absolue[224].

cc) Responsabilité de moteurs de recherche en matière de protection des données: Google Spain

Dans un arrêt du 13 mai 2014[225], la CJUE a clarifié la question de la responsabilité des moteurs de recherche. Ces derniers sont soumis à la directive sur la protection des données[226] et peuvent être tenus de supprimer d'une liste de résultats affichée à la suite d'une recherche effectuée à partir du nom d'une personne, des liens vers des pages Web publiées par des tiers et contenant des informations relatives à cette personne. La Cour a précisé qu'une telle obligation peut aussi exister lorsque les informations ne sont pas effacées de ces pages Web et, le cas échéant, même si leur publication sur lesdites pages est licite.

dd) Application de la directive sur le commerce électronique à des moteurs de recherche: Google France

Dans un arrêt[227] dans lequel elle avait à juger de l'usage de la marque d'un concurrent en tant que mot-clé pour faire afficher une publicité pour des produits ou des services identiques, dans le cadre de Google-AdWords, la CJUE s'est penchée sur la question de savoir si le privilège prévu par la directive sur le commerce électronique s'appliquait aux opérateurs de moteurs de recherche. Elle a conclu que l'art. 14 de la directive, qui exclut la responsabilité des fournisseurs d'hébergement, « *doit être interprété en ce sens que la règle y énoncée s'applique au prestataire d'un service de référencement sur Internet lorsque ce prestataire n'a pas joué un rôle actif de nature à lui confier une connaissance ou un contrôle des données stockées. S'il n'a pas joué un tel rôle, ledit prestataire ne peut être tenu responsable pour les données qu'il a stockées à la demande d'un annonceur à moins que, ayant pris connaissance du caractère illicite de ces données ou d'activités de cet annonceur, il n'ait pas promptement retiré ou rendu inaccessibles lesdites données.* » La CJUE applique donc les mêmes critères aux opérateurs de moteurs de recherche qu'aux fournisseurs d'hébergement.

ee) Hyperliens et *framing:* Svensson et BestWater

Dans l'arrêt Svensson contre Retriever Sverige AB[228], la CJUE a jugé légal le fait d'établir un lien vers une œuvre protégée par le droit d'auteur. Plusieurs journalistes suédois avaient saisi les juridictions contre l'exploitant d'une collection de liens. Selon la Cour, l'art. 3, al. 1, de la directive sur le droit d'auteur doit être interprété en ce sens que la mise à disposition, sur un site Internet, de liens cliquables renvoyant à des œuvres disponibles en accès libre sur un autre site Internet ne constitue pas un acte de communication au public, tel que visé par cette disposition. Les Etats membres ne doivent dès lors pas sanctionner les liens directs vers des œuvres protégées par le droit d'auteur en accès libre comme une violation du droit d'auteur.

---

[224] Arrêt de la CJUE C-314/12 du 27.3.2014 (UPC Telekabel Wien c. Constantin Film Verleih, Wega Filmproduktionsgesellschaft [kino.to]), n° 61.

[225] Arrêt de la CJUE C-131/12 du 13.5.2014 (Google Spain SL et Google Inc./Agencia Española de Protección de Datos (AEPD) et Mario Costeja González).

[226] Voir note 103.

[227] Arrêt de la CJUE C-236/08 à C-238/08 du 23.3.2010 Google France SARL et Google Inc. c. Louis Vuitton Malletier SA, Google France SARL c. Viaticum SA et Luteciel SARL, Google France SARL c. Centre national de recherche en relations humaines (CNRRH) SARL, Pierre-Alexis Thonet, Bruno Raboin et Tiger SARL.

[228] Arrêt de la CJUE C-466/12 du 13.2.2014.

Cet arrêt a été confirmé également pour la technique de la « transclusion » (*framing*) dans la décision BestWater International GmbH contre Michael Mebes et Stefan Potsch[229] . L'inclusion sur un site Internet, au moyen d'un lien, d'une œuvre protégée ayant été librement communiquée au public sur un autre site Internet ne peut pas être qualifiée de communication au public au sens de l'art. 3, al. 1, de la directive sur le droit d'auteur puisque cet acte n'est effectué ni auprès d'un public nouveau, ni selon un mode technique spécifique, différent de celui utilisé lors de la communication initiale.

ff) Responsabilité des exploitants de place de marché en ligne en cas de violation du droit des marques commise par leurs clients: L'Oréal contre eBay

Dans l'arrêt L'Oréal contre eBay[230], la CJUE a déclaré que l'exonération de responsabilité de l'art. 14 de la directive sur le commerce électronique ne s'applique à l'exploitant d'une place de marché en ligne que lorsque celui-ci n'a pas joué un rôle actif qui lui permette d'avoir une connaissance ou un contrôle des données stockées, en prêtant une assistance consistant notamment à optimiser la présentation des offres à la vente en cause ou à promouvoir ces offres. Elle a précisé que l'exonération de responsabilité ne s'applique cependant pas si l'exploitant, bien que n'ayant pas joué un rôle actif, a eu connaissance de faits ou de circonstances sur la base desquels un opérateur économique diligent aurait dû constater l'illicéité des offres en cause et, dans l'hypothèse d'une telle connaissance, n'a pas promptement agi pour retirer les informations ou rendre l'accès à celles-ci impossible (art. 14, al. 1, let. b, de la directive).

gg) Conclusion

L'argumentation de la CJUE montre que celle-ci n'hésite pas à reconnaître des devoirs aux fournisseurs. Les Etats de l'UE doivent cependant garantir un équilibre approprié entre les droits fondamentaux de tous les intéressés et notamment respecter le principe de proportionnalité. Ainsi, ordonner une surveillance absolue n'est pas compatible avec le droit de l'Union. Les fournisseurs peuvent néanmoins être tenus de prendre des mesures raisonnablement exigibles pour mettre fin à la violation du droit et prévenir des violations futures. Les opérateurs de moteurs de recherche peuvent en outre être contraints de prendre des mesures de protection des données personnelles.

c) Allemagne

En Allemagne, la directive sur le commerce électronique a été concrétisée dans la *Telemediengesetz* (*TMG*). Comme la directive, les articles qui définissent le champ d'application du privilège (§§ 8 à 10 TMG) parlent de « responsabilité », sans que la formulation permette de conclure si les actions défensives sont incluses, ou bien si seules les actions réparatrices sont possibles. La Cour fédérale suprême allemande ne les applique qu'aux actions réparatrices, ce qui suscite les critiques de la doctrine[231]. La notion allemande de la « *Störerhaftung* » (responsabilité « du perturbateur ») donne une très vaste portée à la légitimation passive. Selon les principes de la *Störerhaftung* - que la Cour fédérale applique en cas de violation des droits de propriété intellectuelle, en tant que droits bénéficiant d'une protection absolue – toute personne qui, de quelque manière que ce soit, contribue à porter atteinte à un bien protégé, volontairement et selon un lien de causalité adéquate, peut avoir à

[229] Arrêt de la CJUE C-348/13 du 21.10.2014.
[230] Arrêt de la CJUE C-324/09 du 12.7.2011.
[231] Voir *Härting*, n° 2136 s., avec d'autres références.

en répondre en tant que « perturbateur ». Elle ne doit pas nécessairement être auteur principal ou participant de l'acte commis[232]. Dans plusieurs arrêts, la Cour fédérale a accepté des demandes de prévention et de cessation de l'atteinte contre des fournisseurs d'hébergement[233] et d'accès[234]. Dans des arrêts plus récents, elle a cependant eu tendance à restreindre la *Störerhaftung* dans le domaine d'Internet, en exigeant que le fournisseur ait violé un devoir de contrôle qu'il aurait raisonnablement pu respecter[235].

A noter que la jurisprudence allemande estime qu'un hébergeur de fichiers doit, dans certains cas, éviter qu'une violation avérée ne se répète à l'avenir, en déployant les moyens techniques à sa disposition (par ex. filtre par mots clés)[236].

d) Autriche

En Autriche, la directive sur le commerce électronique a été concrétisée dans une nouvelle loi d'application générale[237], entrée en vigueur le 1er janvier 2002. Le législateur autrichien est allé au-delà des dispositions de la directive et a prévu des exonérations de la responsabilité pour d'autres « fournisseurs de services » tels que des moteurs de recherche et des personnes qui mettent un lien sur une page. Le privilège en matière de responsabilité des moteurs de recherche s'inspire du privilège des fournisseurs d'hébergement (§§ 13 et 14 ECG), celui des auteurs de liens s'inspire du privilège des fournisseurs d'accès (§§ 16 et 17 ECG). Les règles sur la responsabilité des fournisseurs de services (§§ 13 à 18) s'étendent aux services non payants selon le § 19, al. 2, ECG.

Selon le § 19, al. 1, ECG, ces dispositions (§§ 13 à 18 ECG) ne concernent pas les actions en prévention ou en cessation de l'atteinte. Le § 81, al. 1*a*, de la loi sur le droit d'auteur[238] dispose pourtant que les actions en prévention de l'atteinte contre l'intermédiaire ne peuvent être engagées qu'après un avis formel si les conditions d'une exonération de la responsabilité sont réunies selon les §§ 13 à 17 ECG. Cette disposition s'applique par analogie aux actions en cessation de l'atteinte (§ 82, al. 1, UrhG).

3.3.2 Etats-Unis

Contrairement à l'UE[239], les Etats-Unis ont opté pour une approche verticale et ne connaissent des règles en matière de responsabilité applicables aux fournisseurs que dans trois domaines juridiques différents pour des états de fait très précis. Il s'agit de la responsabilité en raison de la présence d'« *offensive material* » (à l'exclusion expresse des violations de droits de propriété

[232] *Härting*, n° 2144.
[233] Aperçu dans *Härting*, n° 2182 ss.
[234] Aperçu dans *Härting*, n° 2176 ss.
[235] Divers renvois dans *Härting*, n° 2145, note de bas de page 3.
[236] Arrêt Rapidshare (Alone in the dark) de la Cour fédérale allemande (BGH I ZR 18/11, 12.07.2012), consid. 31 ss.
[237] *Bundesgesetz, mit dem bestimmte rechtliche Aspekte des elektronischen Geschäfts- und Rechtsverkehrs geregelt werden* (*E-Commerce-Gesetz – ECG*).
[238] *Bundesgesetz über das Urheberrecht an Werken der Literatur und der Kunst und über verwandte Schutzrechte* (*Urheberrechtsgesetz - UrhG*).
[239] Concernant la directive sur le commerce électronique, voir ch. 3.3.1 a) bb.

intellectuelle)[240], de violations de droits d'auteur[241] et de violations de droits de marque[242]. Les règles générales en matière de responsabilité à l'égard des fournisseurs s'appliquent dans les autres domaines.

Les trois règlementations en matière de responsabilité ne sont pas harmonisées. D'où des obligations différentes pour les fournisseurs[243]. Les régimes d'exception s'étendent toutefois tous aux actions en prévention de l'atteinte, certains même aux actions en cessation de l'atteinte[244].

Le *Communications Decency Act* a été édicté pour réglementer l'« *offensive material* » (par ex. contenus pornographiques, discriminatoires ou diffamatoires)[245]. A son § 230(c), il contient toutefois une exonération étendue de la responsabilité des fournisseurs, non liée à certains biens juridiques. Selon le § 230(c)(1) CDA, un fournisseur ne doit jamais être assimilé à l'éditeur ou l'auteur d'informations provenant d'un autre fournisseur de contenu. Le privilège en matière de responsabilité s'applique dès lors indépendamment de la proximité avec le contenu ou de la connaissance des contenus et permet aux fournisseurs de prendre également en charge des tâches rédactionnelles sans que cela implique une responsabilité pour les contenus[246]. La disposition assure en parallèle que les fournisseurs qui, de bonne foi, prennent *sur une base volontaire* des mesures comme le verrouillage afin de prévenir l'accès à du « matériel offensif » ne puissent pas être poursuivis[247]. Le droit de la propriété intellectuelle est expressément exclu du domaine d'application du CDA (§230[e][2] CDA).

Le § 32(2) du *Lanham Act* concerne le droit des marques[248] et prévoit un privilège de responsabilité et une restriction de ce qu'on appelle les « *injunctions* » (demandes en prévention et en cessation de l'atteinte) pour les éditeurs de certains médias (communication électronique incluse). La condition est qu'il n'y ait aucune faute dans la violation du droit de la marque (« *innocent infringer* », §32[2][A])[249].

Le *Digital Millennium Copyright Act* réglemente l'activité des fournisseurs dans le *droit d'auteur* et prévoit même des exonérations de la responsabilité sous certaines conditions[250]. Il contient en premier lieu une limitation de la responsabilité pour les simples transmissions, le routage et les reproductions provisoires qui en résultent (§ 512[a]) et pour la mise en cache (§ 512[b]). Il inclut en outre une limitation de la responsabilité des fournisseurs d'hébergement, à condition qu'ils n'aient pas connaissance d'activités illicites, qu'ils ne soient pas supposés en avoir au vu des circonstances et qu'ils suppriment ou bloquent l'accès aux contenus illicites dès que ceux-ci sont portés à leur connaissance ou qu'ils en sont informés (§ 512[c])[251]. Pour que l'exonération de la responsabilité déploie effet, il faut que le fournisseur nomme un

---

[240] 47 U.S.C. § 230 (*Communications Decency Act ; CDA*).
[241] 17 U.S.C. § 512 (*Digital Millennium Copyright Act; DMCA)* ; pour ce qui est des définitions qu'il contient voir ch. 2.3.2.
[242] 15 U.S.C. § 1114(2), connu comme § 32(2) *Lanham Act*.
[243] *Frech*, 125.
[244] Présentation par *Frech*, 235 ss., résumé à la p. 250.
[245] Concernant la genèse de la loi, voir *Frech*, 76 ss.
[246] Voir *Gilliéron*, RDS 2002, 394 ss.
[247] Protection du « *'Good Samaritan' blocking* » et du « *screening of offensive material* », § 230(c)(2) CDA.
[248] Voir *Frech*, 97 ss.
[249] Voir *Frech*, 245 ss. concernant l'interprétation de cette disposition.
[250] 17 U.S.C. § 512.
[251] La procédure est réglée en détail dans la section 512(c)(3) DMCA, qui va jusqu'à définir le contenu nécessaire de la demande à l'encontre du fournisseur d'hébergement.

représentant (« *agent* ») auprès du *United States Copyright Office* et sur son site, qu'il charge de la notification des plaintes contre les contenus illicites (« *notices* »). De plus, il ne doit tirer aucun avantage financier direct des violations dans la mesure où il a le droit et la possibilité d'exercer un contrôle. Il est tenu d'édicter des règles prévoyant la cessation des relations avec la clientèle en cas de violations répétées de droits. Il n'est pas autorisé à empêcher les mesures techniques usuelles (« *standard technical measures* »); celles-ci se réfèrent à des mesures que les titulaires de droits ont développées pour repérer les contenus illicites[252]. Enfin, le § 512(d) DMCA comprend aussi des exonérations de la responsabilité pour les services de recherche d'informations (par ex. les moteurs de recherche et les collections de liens). Ces exonérations correspondent à celles applicables aux fournisseurs d'hébergement[253].

Le DMCA ne prévoit aucune mesure de verrouillage des adresses IP et DNS. Il était prévu à l'origine d'introduire des mesures de verrouillage des adresses DNS dans le *Stop Online Piracy Act* (SOPA). Elles devaient toutefois être biffées du projet en raison des conséquences incertaines qu'elles auraient pu avoir[254]. Des campagnes de communication massive des fournisseurs de services (par ex. *blackout* de Wikipédia) ont cependant suscité une telle résistance de la part des citoyens, des entreprises et de la société civile que le projet de loi n'a jamais été adopté par le parlement américain[255].

Les discussions menées aux Etats-Unis sur les *conséquences d'une règlementation* sont intéressantes. En effet, le risque de voir la nouvelle règlementation entraver le progrès technique, dans le sens où elle est susceptible d'affaiblir les incitations pour les fournisseurs à prévenir, de leur propre initiative, les violations de droits, avait déjà été pointé au moment de la promulgation du DMCA[256]. Dans une étude juridique transversale publiée récemment[257], les auteurs font cependant remarquer que ce risque est atténué par d'autres facteurs, notamment, dans le droit d'auteur, par le fait que l'industrie des fournisseurs s'efforce de maintenir de bonnes relations avec les titulaires de droits. Mais force est de constater que, dans le droit de la personnalité, l'immunité va aux dépens de la personne dont les droits ont été enfreints et permet l'émergence d'un Internet dans lequel les fournisseurs qui agissent très peu sur les contenus de leurs utilisateurs sont favorisés[258].

---

[252] Voir *The Digital Millennium Copyright Act* de 1998, *U.S. Office of Copyright Summary* de décembre 1998, 9 s., consultable à l'adresse: www.copyright.gov/legislation/dmca.pdf.
[253] Voir *The Digital Millennium Copyright Act* de 1998, *U.S. Office of Copyright Summary* de décembre 1998 (note 252), 12 s.
[254] Voir judiciary.house.gov/index.cfm/2012/1/smithtoremovednsblockingfromsopa.
[255] Voir par ex. l'article du *Wall Street Journal* intitulé « Congress Tosses Antipiracy Bills» du 21.1.2012, consultable à l'adresse: on.wsj.com/1x3sUlB.
[256] Voir le résumé de *Mehra/Trimble*, AMJCL 2014, 691.
[257] *Mehra/Trimble*, AMJCL 2014, 691 ss.
[258] Voir *Mehra/Trimble*, AMJCL 2014, 702.

4 Actions réparatrices (dommages-intérêts, réparation du tort moral, remise du gain, etc.)

4.1 Droit suisse

4.1.1 Action en dommages-intérêts

En vertu de l'art. 41, al. 1, CO, celui qui cause un dommage à autrui d'une manière illicite, soit intentionnellement, soit par négligence ou imprudence, est tenu de le réparer. Les conditions de base de la responsabilité sont donc l'existence du dommage[259], d'un acte illicite, d'un lien de causalité et d'une faute.

Ici non plus, nous n'approfondirons pas les actions possibles contre le fournisseur qui (en qualité de fournisseur de contenus, par ex.) porte lui-même directement atteinte aux droits d'autrui ou les lèse de toute autre manière, car l'examen des prétentions ne pose a priori pas de problèmes[260]. Un examen plus approfondi de la question s'impose pour les cas dans lesquels le dommage subi par le tiers découle du comportement des utilisateurs des services du fournisseur. La question qui se pose est notamment de savoir si cela pourrait (aussi) fonder une action réparatrice *contre le fournisseur*.

Au sens de l'art. 50, al. 1, CO, celui qui a concouru au dommage causé de manière illicite, que ce soit en qualité d'instigateur ou de complice (ou de receleur), répond solidairement du dommage avec l'auteur principal. Cette norme ne fonde cependant pas directement une responsabilité des participants, celle-ci n'entrant en considération que si les conditions de base de la responsabilité sont remplies[261]. Voyons donc ce qu'il en est de ces conditions dans le détail.

a) Dommage

Pour obtenir des dommages-intérêts, la partie lésée, soit le demandeur, doit établir l'existence d'un dommage financier grevant son patrimoine[262]. Ce type de dommage est possible en cas de violation des droits d'auteur, bien que des questions de délimitation complexes se posent en pratique[263]. L'atteinte illicite aux droits de la personnalité viole certes un bien juridique qui n'a pas de valeur pécuniaire en soi[264], mais on peut tout de même admettre l'existence d'un dommage au sens juridique du terme si quelqu'un subit une baisse de son volume d'affaires à la suite de calomnies diffusées sur Internet[265].

---

[259] L'existence d'un dommage est toujours une condition de base de l'action réparatrice, même si une partie de la doctrine ne la qualifie pas de condition mais plutôt de conséquence de la responsabilité, voir *Roberto*, Haftpflichtrecht, n° 03.12 s.

[260] Voir ch. 3.1.1.

[261] BK-*Brehm*, ad art. 50 CO n° 33 ; *Fellmann/Kottmann*, Haftpflichtrecht I, n° 2760 s. ; *Briner*, sic! 2006, 383 ss., 387.

[262] Voir notamment BSK OR I-*Kessler*, ad art. 41 n° 3.

[263] Voir par ex. *Müller Barbara K.*, Handkommentar URG, ad art. 62 n° 10 ss.

[264] Voir *Hausheer/Aebi-Müller*, n° 14.47 ; *Steinauer/Fountoulakis*, n° 501 s.

[265] Voir l'arrêt du Tribunal fédéral 5C.57/2004 du 2.9.2004 concernant une baisse de revenus à la suite d'une atteinte à l'honneur dans les médias.

En matière de protection des données, les actions réparatrices sont plutôt rares, dans la mesure où la personne lésée ne subit bien souvent pas de dommage financier (ou alors qu'un dommage très faible).

b) Atteinte illicite

Selon la conception traditionnelle, le dommage causé est illicite lorsqu'une obligation légale générale est violée, qu'il s'agisse de la violation d'un droit absolu du lésé (illicéité de résultat; *Erfolgsunrecht*) ou d'un pur dommage patrimonial causé par une infraction à une règle de droit dont le but est de protéger contre ce genre de dommage (illicéité de comportement; *Verhaltensunrecht*)[266].

Les droits absolus sont en particulier les droits de la personnalité et les droits de la propriété intellectuelle (droits d'auteur, des brevets, des marques et du design)[267].

Il existe aussi des normes de protection du patrimoine dans le droit de la concurrence, mais il faut d'abord vérifier si la norme en question a pour but de protéger le patrimoine d'un concurrent spécifique ou simplement de protéger la collectivité[268]. C'est uniquement dans le premier cas que le concurrent pourra ouvrir une action en dommages-intérêts.

Celui qui concourt au dommage causé de manière illicite par un tiers en qualité d'instigateur ou de complice cause lui aussi un dommage de manière illicite (voir art. 50, al. 1, CO). Conformément à la théorie traditionnelle de l'illicéité objective, le caractère illicite peut généralement être admis, car les dommages causés par les contenus diffusés sur Internet résultent presque toujours de violations des droits de la personnalité ou de la propriété intellectuelle (droits absolus) ou de normes de protection relevant du droit de la concurrence.

c) Lien de causalité

Le comportement dommageable doit aussi présenter un lien de causalité naturelle et adéquate avec l'atteinte au bien juridiquement protégé et avec le dommage qui en découle. Selon la formule de la condition *sine qua non* adoptée par le Tribunal fédéral, la causalité naturelle est établie lorsqu'on ne peut imaginer le résultat sans le comportement en question[269]. D'après la formule de la causalité adéquate du Tribunal fédéral, il faut en outre que, selon le cours ordinaire des choses et l'expérience générale de la vie, l'événement qui a causé le dommage soit propre en soi à entraîner un résultat du genre de celui qui est survenu, que donc la survenance du résultat apparaisse de manière générale comme ayant été favorisée par l'événement[270]. Comme nous l'avons vu précédemment, une partie de la doctrine n'admet pas la causalité adéquate pour ce qui est de la participation des *fournisseurs d'accès*, car le simple

---

[266] Conception appelée « théorie de l'illicéité objective », voir notamment BSK OR I-*Kessler*, ad art. 41 n° 31. S'agissant de la qualification en tant qu'action ou omission, voir également le ch. 3.1.2 et en particulier la note 54. Si l'on suppose une omission, il faudrait aussi vérifier si le fournisseur Internet a violé une obligation d'agir, par ex. s'il a omis de prendre les mesures de protection qui lui incombaient au vu de la dangerosité de la situation qu'il a créée ou entretenue. Il est cependant peu probable que l'illicéité de l'atteinte puisse être confirmée sous cet angle.

[267] Voir notamment BSK OR I-*Kessler*, ad art. 41 n° 33.

[268] *Schwenzer*, n° 50.20.

[269] ATF 117 V 359, consid. 4.a. En revanche, en cas d'omission, on examine si une action conforme aux obligations légales aurait permis de prévenir le dommage (causalité hypothétique), voir par ex. *Fellmann/Kottmann*, Haftpflichtrecht I, n° 410.

[270] Voir par ex. ATF 123 III 110, consid. 3.a; voir également le ch. 3.2.2.

fait de donner accès à Internet ou de mettre à disposition une infrastructure est une contribution trop accessoire[271]. S'agissant des *fournisseurs d'hébergement* et des exploitants de plateformes, la doctrine dominante estime qu'il existe un lien de causalité adéquate, car selon le cours ordinaire des choses et l'expérience générale de la vie, la mise à disposition d'espace mémoire ou d'infrastructures de communication est de nature à favoriser une violation du droit[272].

d) Faute

À l'inverse de l'action défensive, l'action en dommages-intérêts ne peut être admise que si le défendeur a commis une faute. La responsabilité d'un fournisseur Internet n'est donc engagée que si une faute intentionnelle ou une négligence peuvent lui être reprochées. Sauf dans les cas où un fournisseur inciterait ses utilisateurs à violer le droit, ce qui permettrait d'établir une faute intentionnelle de sa part, il convient donc, pour établir la faute par négligence, d'examiner s'il existe des devoirs de diligence spéciaux qu'il aurait violés[273]. Voyons donc quels sont ces devoirs de diligence.

aa) Devoirs de diligence des fournisseurs d'hébergement, des exploitants de plateformes et prestataires de services connexes

i) Remarques générales

Il n'existe actuellement, en Suisse, ni règlementation légale ni précédent pertinent qui concrétise les obligations de diligence des fournisseurs[274]. La Swiss Internet Industry Association (simsa) a toutefois élaboré le Code de conduite Hébergement (CCH)[275], qui est en vigueur depuis le 1er février 2013. Le ch. 2 du CCH définit les destinataires et le champ d'application du code comme suit: « *Le CCH s'adresse aux entreprises et particuliers soumis au droit suisse qui exploitent des services d'hébergement. Les services d'hébergement sont des services qui permettent aux exploitants de sites Internet et d'application de sauvegarder des contenus, de les traiter et les rendre publiquement accessibles à des tiers[276] […]. Les prestations dépassant le cadre des simples services d'hébergement de l'hébergeur sortent [toutefois] du champ d'application du CCH.* » Pour élaborer le CCH, la simsa s'est inspirée de diverses règlementations internationales et en particulier des règles définies dans la directive européenne sur le commerce électronique[277]. Le CCH énonce qu'un fournisseur

[271] Voir ch. 3.2.2 ainsi que les renvois de la note 82.
[272] Voir *Rosenthal*, Internet- Provider-Haftung – ein Sonderfall?, n° 104 ; *auf der Maur/Steiner*, 423.
[273] Selon une partie de la doctrine récente – divergente de la théorie de l'illicéité objective –, la violation d'une obligation particulière d'agir ou de se comporter est nécessaire pour pouvoir établir l'illicéité d'une omission *ou d'une action* (voir *Roberto*, n° 04.08 ss.; *Schwenzer*, n° 50.29 ss.; *Fellmann/Kottmann*, Haftpflichtrecht I, n° 334 ss.). Si l'on suit ce raisonnement, la question des devoirs de diligence incombant au fournisseur Internet se pose déjà lors de l'établissement de l'illicéité de l'atteinte – même si le comportement qu'on lui reproche est une action. Cette obligation de comportement peut aussi découler – mais pas seulement – du principe de l'interdiction de créer un danger pour autrui (à ce sujet, voir la note 54). Des devoirs de diligence émanant d'autres sources entrent aussi en ligne de compte. La doctrine est ainsi favorable à la définition d'obligations de protection par catégories de cas (voir *Fellmann/Kottmann*, Haftpflichtrecht I, n° 343; *Schwenzer*, n° 50.04; voir également *Roberto*, n° 04.26 ss.).
[274] Voir *Frech*, 332 ss.
[275] À consulter à l'adresse www.simsa.ch > Services > Code of conduct Hosting.
[276] S'agissant des autres catégories de fournisseurs d'hébergement envisagées par la doctrine et la jurisprudence ainsi que de la description de leurs rôles au sens du présent rapport, voir le ch. 2.4.
[277] Voir ch. 3.3.1.

d'hébergement n'a aucune obligation de surveillance active (ch. 5). Le ch. 7 du CCH définit une procédure de notification et de retrait de contenu illicite (*notice and take down procedure*) qui permet au fournisseur d'hébergement de bloquer l'accès à un site Internet lorsqu'il reçoit une notification (remplissant certains critères), s'il est très probable que celle-ci concerne des contenus illicites. Il faut que les conditions générales du fournisseur d'hébergement attirent l'attention des clients sur la procédure de notification et de retrait de contenu illicite et indiquent que les services d'hébergement doivent être utilisés dans le respect des lois en vigueur (ch. 8). Étant donné que le CCH a été élaboré avec les acteurs majeurs du secteur[278], on peut estimer qu'il jouit d'une certaine adhésion au sein de la branche. La reconnaissance de ces règles par les tribunaux est toutefois encore incertaine.

Une partie de la doctrine est aussi favorable à une application par analogie de la règlementation européenne[279]. En ce sens, elle rejette unanimement une obligation générale de contrôle des contenus illicites pour le *fournisseur d'hébergement*[280]. Sans circonstances particulières, d'après la doctrine dominante, les fournisseurs d'hébergement ne peuvent se voir reprocher la violation d'un devoir de diligence lorsque leur infrastructure est utilisée pour commettre des actes illicites.

ii) En présence d'indices d'une violation du droit

Par contre, en présence d'indices détaillés d'une violation du droit, le *fournisseur d'hébergement* doit intervenir et prendre les mesures défensives qui s'imposent. Si le fournisseur n'agit pas après avoir reçu une notification de cette nature, la doctrine dominante estime qu'une faute peut lui être imputée en cas de violations flagrantes du droit[281].

La doctrine exige que l'indice dont la non-observation peut être qualifiée de violation du devoir de diligence rende vraisemblable la violation du droit pour le fournisseur, même si celui-ci est peu expérimenté en matière juridique[282]. Cela signifie d'abord que le contenu visé doit être désigné précisément (notamment par son URL)[283]. Il est également exigé que le dénonciateur se fasse connaître et qu'il rende vraisemblable son intérêt juridiquement protégé à ce que le contenu en question soit supprimé ou bloqué – sauf si la violation est identifiable au premier coup d'œil (par ex. en cas de pédopornographie)[284]. Pour une part prépondérante de la doctrine, la violation du droit doit être flagrante pour un non-juriste[285]. Dans des domaines juridiques aussi complexes que le droit d'auteur, il sera parfois difficile d'établir que la violation du droit est flagrante pour un non-juriste et, par conséquent, de reprocher au fournisseur une violation de son devoir de diligence. C'est pourquoi d'autres auteurs sont d'avis qu'un fournisseur d'hébergement diligent doit intervenir même en cas de doute quant à la légalité

[278] Voir les indications fournies à l'adresse www.simsa.ch > Services > Code of conduct Hosting.
[279] *Weber*, E-Commerce, 517 s. ; *Briner*, sic! 2006, 398 s. ; *Hug*, medialex 2014, 56.
[280] *Weber*, E-Commerce, 517 ; *Rosenthal*, Internet-Provider-Haftung – ein Sonderfall?, n° 95 ; *Rohn*, 224 ; *Fountoulakis/Francey*, medialex 2014, 181 s.
[281] *Weber*, E-Commerce, 517 ; *Rosenthal*, Internet-Provider-Haftung – ein Sonderfall?, n° 96 ss. ; *Fountoulakis/Francey*, medialex 2014, 179 ss. ; s'agissant des hébergeurs de fichiers (*filehoster): Beranek Zanon*, Jusletter IT du 11.12.2013, n° 118, 127 ss.
[282] *Rosenthal*, Internet-Provider-Haftung – ein Sonderfall?, n° 98.
[283] *Rosenthal*, Internet-Provider-Haftung – ein Sonderfall?, n° 98 ; *Fountoulakis/Francey*, medialex 2014, 180.
[284] Voir *Fountoulakis/Francey*, medialex 2014, 179 s.
[285] *Rosenthal*, Internet-Provider-Haftung – ein Sonderfall?, n° 98 ; *auf der Maur/Steiner*, 424 s. ; *Rohn*, 202, 208 s.

d'un contenu et doit le supprimer provisoirement[286]. En cas de contestation, le contenu pourra toujours être restauré par la suite.

Le ch. 4.3 du CCH définit les critères formels et matériels de cette notification et exige en particulier que l'auteur soit particulièrement concerné par le contenu visé:

> « [l]l est nécessaire que l'auteur de la notification soit concerné par la prétendue infraction juridique davantage qu'un tiers ou que l'opinion publique: la personne visée en cas d'infraction aux droits de la personnalité (ou son représentant), la personne considérée comme détentrice des droits de propriété ou licence sur les contenus en cas d'infraction aux droits immatériels. Pour les délits officiels, la personne qui émet la notification n'a pas besoin d'être concernée en particulier.
>
> Sur les plans matériel et formel, 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 officiels); (c) adresse URL de la page ou de la rubrique en question; (d) désignation précise des contenus illicites; (e) justification du caractère illicite des contenus. »

iii) Devoirs de diligence accrus motivés par des circonstances particulières

Enfin, une partie de la doctrine s'est penchée sur les devoirs de diligence accrus qui s'appliquent dans certaines configurations – et ce, indépendamment d'une notification concrète. Les auteurs en question se réfèrent souvent à l'arrêt, déjà évoqué dans le présent rapport, que le Tribunal fédéral a rendu au sujet des devoirs de diligence d'une imprimerie[287]. Ils estiment que les critères qui y sont développés peuvent être transposés aux *fournisseurs d'hébergement* et, donc, que des devoirs de diligence accrus s'appliquent au fournisseur hébergeant des pages qui ont déjà attiré l'attention sur elles par le passé en raison de violations du droit et qui, de par leur nature, sont susceptibles d'en commettre d'autres; ce devoir de diligence accru ne concerne que les pages en question[288]. La transposabilité des conclusions de cet arrêt aux fournisseurs d'hébergement n'est cependant pas incontestée[289]. Enfin, certains défendent l'idée que ces devoirs de diligence accrus sont aussi valables pour les acteurs qui exercent plus d'influence sur les contenus que les fournisseurs d'hébergement classiques. En s'appuyant sur un arrêt de la Cour EDH (affaire Delfi), ils prennent l'exemple d'un portail d'informations qui accepterait les commentaires diffamatoires de ses lecteurs. Pour eux, dans des situations particulières où il faut s'attendre à des violations du droit – comme ce fut le cas dans l'affaire Delfi, notamment en raison de la nature polémique de l'article – une plus grande attention est de mise[290].

---

[286] *Fountoulakis/Francey*, medialex 2014, 180 s.

[287] ATF 126 III 161, voir ch. 3.2.6 a).

[288] Voir *Gilliéron*, RDS 2002, 435; *Frech*, 335 et *Fountoulakis/Francey*, medialex 2014, 181, qui se déclarent cependant tous opposés à une obligation de surveillance *générale*.

[289] Contre la transposition aux fournisseurs d'hébergement: *Rosenthal*, Internet-Provider-Haftung – ein Sonderfall?, n° 95 et en particulier la note de bas de page 115.

[290] Voir *Weber*, E-Commerce, 518; *Fountoulakis/Francey*, medialex 2014, 181; au sujet de l'arrêt Delfi c. Estonie, voir aussi le ch. 4.2. S'agissant de la délimitation des fournisseurs en fonction de leur proximité avec le contenu, voir également ch. 2.4 ; voir enfin l'avis du Conseil fédéral du 19.11.2014 concernant le postulat Tornare 14.3908 « Internet. Zéro tolérance envers l'intolérance » du 25.9.2014.

bb) Devoirs de diligence des fournisseurs d'accès

La doctrine dominante apparaît largement opposée à une responsabilité civile des fournisseurs d'accès, en arguant que le simple fait de permettre l'accès à Internet ou de mettre à disposition une infrastructure constitue une contribution trop accessoire[291]. Une obligation généralisée de surveillance ou de contrôle de la part des *fournisseurs d'accès* est donc plutôt fermement rejetée – par analogie à la règlementation de l'UE[292].

cc) Devoirs de diligence des exploitants de moteurs de recherche

S'agissant des exploitants de moteurs de recherche, une obligation générale de contrôler les résultats des recherches est aussi majoritairement rejetée[293]. Dans l'affaire Google Suggest, le Tribunal cantonal du Jura était d'ailleurs parvenu à la conclusion que l'on ne saurait exiger de Google qu'il élimine une proposition de recherche, même s'il savait que celle-ci pourrait éventuellement constituer une atteinte à la personnalité[294]. La doctrine a toutefois critiqué cet arrêt, notamment en se référant à des décisions contraires prises dans d'autres pays[295]. Elle envisage donc également une obligation de contrôler les indices de violations du droit par les contenus auxquels renvoie un lien hypertexte[296] et conçoit que, dans certaines circonstances, l'exploitant du moteur de recherche puisse avoir à répondre d'une violation flagrante du droit[297].

e) Responsabilité solidaire selon l'art. 50 CO

Relevons encore que la partie lésée devrait en général pouvoir agir contre *l'utilisateur* du fournisseur de services Internet qui, en téléchargeant par exemple de manière illégale des contenus ou des fichiers sur des plateformes d'échange, des sites ou d'autres services du fournisseur, est à la source du dommage.

Selon l'art. 50, al. 1, CO, plusieurs auteurs ayant causé ensemble un dommage, que ce soit en qualité d'auteur principal, d'instigateur ou de complice, en répondent solidairement à l'égard du lésé. La *faute commune* n'implique pas que les auteurs se soient entendus, mais uniquement qu'ils aient eu réciproquement connaissance de leur contribution à l'acte et qu'ils se soient accommodés du préjudice consécutif[298]. Comme nous l'avons vu précédemment, une violation du devoir de diligence pourra éventuellement être reprochée au fournisseur d'hébergement s'il ne prend pas de mesures pour empêcher le dommage de se produire. C'est ici justement sa connaissance de la participation à l'acte de l'utilisateur qui lui est reprochée. Les conditions prévues à l'art. 50, al. 1, CO seront donc généralement remplies, de sorte que le fournisseur et l'utilisateur devront répondre solidairement de l'ensemble du dommage à l'égard du lésé[299]. Conformément à l'al. 2 de cette disposition, il appartient au juge d'apprécier si les participants ont un droit de recours les uns contre les autres et de déterminer, le cas échéant, l'étendue de ce recours.

---

[291] Pour des références, voir note 82.
[292] *Weber*, E-Commerce, 509 ; *Rosenthal*, Internet-Provider-Haftung – ein Sonderfall?, n° 95.
[293] Voir *Hürlimann*, 110 ss.
[294] Arrêt du Tribunal cantonal du Jura du 12.2.2011 (CC117/2010) (voir note 91), n° 13 ss.; voir également ch. 3.2.2.
[295] Pour des références, voir note 94.
[296] *Hürlimann*, 112 ss.
[297] *Hürlimann*, 114 s.
[298] BSK OR I-*Graber*, ad art. 50 OR n° 6 ss. ; voir également ch. 3.2.5 a).
[299] Voir *Rosenthal,* Internet-Provider-Haftung – ein Sonderfall?, n° 105.

f) Conclusions

S'agissant de l'examen des devoirs de diligence qui s'appliquent aux fournisseurs, la doctrine s'appuie largement sur la directive européenne sur le commerce électronique[300]. Le Code de conduite Hébergement (CCH) de la simsa, qui est a priori la seule règlementation actuellement en vigueur dans la branche en Suisse, est lui aussi inspiré de cette directive et n'oblige ni les fournisseurs d'accès ni les fournisseurs d'hébergement à contrôler en continu les contenus publiés par leurs utilisateurs.

En revanche, lorsqu'un *fournisseur d'hébergement* reçoit des indications détaillées relatives à des contenus spécifiques qui violeraient le droit de manière flagrante, il a l'obligation d'effectuer une vérification et, le cas échéant, de supprimer les contenus en question. S'il ne le fait pas, il est possible de lui reprocher une violation de la diligence consacrée par l'usage, ce qui, en cas de préjudice patrimonial, pourrait conduire à une action en dommages-intérêts contre lui. La doctrine envisage aussi une violation des devoirs de diligence des fournisseurs d'hébergement en présence de circonstances spécifiques permettant d'anticiper des violations concrètes du droit dans le futur. Elle est plus réticente en ce qui concerne les *fournisseurs d'accès*, dans la mesure où le simple fait de mettre à disposition une infrastructure technique ne permet pas, selon elle, d'établir un rapport de causalité adéquate liant le préjudice à l'atteinte.

Si l'auteur des contenus peut être tenu pour responsable au sens de l'art. 41 CO, le fournisseur solidairement responsable pourra éventuellement recourir contre lui, à la discrétion du juge (art. 50, al. 2, CO).

4.1.2 Action en réparation du tort moral

En cas d'atteinte grave à la personnalité, la victime peut exiger une somme d'argent à titre de réparation morale si le préjudice subi n'a pas été réparé autrement (art. 49 CO)[301]. Cette réparation est sans lien avec les conséquences économiques du dommage et a pour but de compenser le préjudice immatériel[302]. Selon la doctrine, les conditions de l'atteinte à la personnalité définies à l'art. 49 CO doivent aussi être remplies dans les autres domaines juridiques qui comportent des normes spéciales renvoyant aux règles du CO sur la réparation du tort moral[303].

Selon la jurisprudence du Tribunal fédéral, l'action en réparation du tort moral n'est admissible qu'en relation avec une norme de responsabilité, car l'art. 49 CO n'est pas en soi une norme de responsabilité. Hormis dans les cas de responsabilité objective, il faut donc aussi pouvoir reprocher une *faute* au défendeur[304]. Si tel est le cas, l'action peut également viser un

---

[300] Pour des références, voir notes 279 et 280.

[301] ATF 129 III 715, consid. 4.4.

[302] ATF 123 III 204, consid. 2.e ; BSK OR I-*Kessler*, ad art. 47 n° 4.

[303] On trouve de ces renvois à l'art. 9, al. 3, LCD, à l'art. 12, al. 1, let. c, de la loi du 6.10.1995 sur les cartels (LCart; RS 251), à l'art. 62, al. 2, LDA, à l'art. 55, al. 2, LPM et à l'art. 35, al. 2, LDes. La doctrine les qualifie de *Rechtsgrundverweis* et non de *Rechtsfolgeverweis*, en ce sens que le renvoi porte sur le fondement et non uniquement sur les conséquences juridiques: voir BSK UWG-*Rüetschi/Roth*, ad art. 9 n° 77 ss.; *Barrelet/Egloff*, ad art. 62 LDA n° 14 (atteinte au droit de la personnalité de l'auteur) ; *Schlosser*, CR PI, ad art. 62 LDA n° 84 ss. Voir également le ch. 4.1.3 au sujet de la jurisprudence divergente du Tribunal fédéral dans le cas de l'action en remise du gain.

[304] ATF 126 III 161, consid. 5b/aa.

participant indirect – donc, théoriquement, un fournisseur Internet. Dans l'ATF 126 III 161, le Tribunal fédéral a admis la réparation du tort moral par une imprimerie qui était impliquée dans la diffusion d'une série d'articles diffamatoires et qui avait connaissance de violations du droit antérieures[305].

La réparation du tort moral consiste généralement en une somme d'argent, mais un « autre mode de réparation » (art. 49, al. 2, CO) comme la publication d'un jugement[306] est également envisageable.

4.1.3 Action en remise du gain

L'art. 28*a*, al. 3, CC, l'art. 9, al. 3, LCD, l'art. 12, al. 1, let. c, LCart, l'art. 62, al. 2, LDA, l'art. 55, al. 2, LPM et l'art. 35, al. 2, LDes renvoient tous – s'agissant de l'action en remise du gain – aux dispositions sur la *gestion d'affaires*. Selon un arrêt du Tribunal fédéral concernant l'art. 28*a*, al. 3, CC – qui renvoie lui-même aux normes analogues contenues dans d'autres normes –, il renvoie en l'occurrence uniquement aux conséquences juridiques (*Rechtsfolgeverweis*): les conditions de la naissance d'une prétention au sens de l'art. 423 CO ne doivent pas être remplies. Dans le contexte d'une atteinte à la personnalité, les preuves à administrer sont l'atteinte illicite, l'existence d'un gain et un rapport de causalité entre l'atteinte illicite et le gain réalisé[307]. Selon cet arrêt, la remise du gain ne nécessite pas une faute de l'auteur[308], ce qu'une partie de la doctrine a critiqué[309]. De plus, la jurisprudence du Tribunal fédéral en matière de concurrence déloyale et de droits de propriété intellectuelle va en sens opposé en exigeant systématiquement que le gérant ait agit de mauvaise foi[310]. Cette divergence est vraisemblablement due au fait que les arrêts en question ont été rendus par des chambres différentes[311].

En matière de droit de la personnalité, la remise du gain au sens de l'art. 423 CO a été admise dans le cas d'un journal qui, grâce à des articles portant atteinte à la personnalité, était parvenu à maintenir son tirage et les recettes publicitaires connexes[312]. Il est donc possible qu'une action similaire contre un exploitant de plateforme de blog soit aussi admise. A priori, la doctrine ne s'est pas encore véritablement penchée sur la question de la remise des gains réalisés par les fournisseurs. Une auteure souligne qu'un hébergeur de fichiers n'est qu'indirectement associé à la diffusion des œuvres violant le droit et que, par conséquent, il ne peut en principe pas être considéré comme un gérant au sens de l'art. 423 CO. Il ne pourrait en être autrement que dans une situation où l'hébergeur proposerait, dans sa publicité, de l'espace mémoire pour des fichiers violant le droit[313].

---

[305] Au sujet de la transposition de cet arrêt aux fournisseurs d'hébergement, voir ch. 4.1.1, d), aa), iii).
[306] ATF 131 III 26.
[307] ATF 133 III 153, consid. 2.4 et 3.3; *Hausheer/Aebi-Müller*, n° 14.71 ss.
[308] *Hausheer/Aebi-Müller*, n° 14.72 ; *Steinauer/Fountoulakis*, n° 614b.
[309] *Schwenzer*, n° 59.17. Au sujet de la LCD: BSK UWG-*Rüetschi/Roth*, ad art. 9 n° 77 et 118 ss. avec d'autres références. Au sujet de la LDA et de la LPM: *Schlosser*, CR PI, ad art. 62 LDA n° 91 et 98, ad art. 55 LPM n° 48. Voir également *Cramer*, recht 2007, 128.
[310] La mauvaise foi a été posée comme condition dans des arrêts relatifs à la LCD (références dans BSK UWG-*Rüetschi/Roth*, ad art. 9 n° 118 ss.) et à la LDA (arrêt du Tribunal fédéral 4C.101/2003 du 17.7.2003 [logotype], consid. 6.2).
[311] Voir BSK UWG-*Rüetschi/Roth*, ad art. 9 n° 121 s.
[312] ATF 133 III 153 (père de Patty Schnyder).
[313] *Beranek Zanon*, Jusletter IT du 11.12.2013, n° 145.

4.1.4 Cas particulier: prétentions contractuelles du client envers le fournisseur pour cause de blocage ou de suppression de données

Le fournisseur Internet qui supprime ou bloque des contenus illicites pourrait éventuellement violer ses propres obligations contractuelles envers son client, si par exemple des tiers ne peuvent plus accéder aux données de ce dernier.

Selon l'art. 97, al. 1, CO, celui qui n'exécute pas le contrat, ou qui ne l'exécute qu'imparfaitement, est tenu de réparer le dommage qui en résulte, à moins qu'il ne prouve qu'aucune faute ne lui est imputable. L'action en réparation du dommage contractuel repose donc essentiellement sur la violation du contrat. Pour établir s'il y a violation du contrat, il faut donc avant tout examiner le contenu du contrat. Généralement, le *fournisseur d'accès* permet à ses clients d'accéder à Internet contre rémunération[314]. La doctrine qualifie la relation contractuelle qui lie ce type de fournisseur à ses clients de contrat innomé[315]. Les obligations principales du fournisseur d'accès sont la mise à disposition d'un raccordement et l'établissement de la connexion dans les règles de l'art[316]. Le *fournisseur d'hébergement* met à disposition, contre rémunération, une infrastructure technique (espace mémoire, capacités de calcul, capacités de transmission) permettant la mise en ligne automatisée de données[317]. Les principales obligations qui incombent à ce type de fournisseur consistent, d'une part, à fournir de l'espace mémoire et, d'autre part, à garantir l'accès des utilisateurs tiers aux données hébergées[318]. D'après la doctrine, le contrat liant le fournisseur d'hébergement à ses clients comporte deux composantes: l'une assimilable à un bail à loyer, l'autre à un contrat d'entreprise[319].

Lorsque le fournisseur d'accès bloque certaines pages, empêchant ainsi ses clients d'accéder à l'ensemble des pages Internet, ou lorsque le fournisseur d'hébergement supprime des données, les rendant donc inaccessibles aux tiers, cela constitue en principe une violation de leurs obligations contractuelles envers leurs clients. Pour se prémunir contre les actions des clients agissant de manière illicite, la plupart des fournisseurs ont dans leurs conditions générales (CG) ce qu'il est convenu d'appeler une « *Acceptable Use Policy* », qui interdit par exemple à l'utilisateur de porter atteinte aux droits d'autrui et autorise contractuellement le fournisseur à bloquer ou à supprimer le compte ou des contenus de l'utilisateur, voire à résilier son contrat, en cas d'infraction. Le ch. 8 du Code de conduite Hébergement (CCH) de la simsa[320] oblige les fournisseurs d'hébergement à se protéger de leurs clients: « *[l]'hébergeur a le droit de bloquer complètement ou partiellement l'accès au site Internet du client et de suspendre les services d'hébergement si les conditions de la procédure de notification et de retrait de contenu illicite […] sont remplies ou si l'hébergeur y est contraint par un tribunal ou une autorité* ». Le fournisseur d'hébergement doit également se réserver le droit de bloquer complètement ou partiellement l'accès au site Internet du client et de suspendre les services d'hébergement « *s'il risque d'être tenu responsable sur le plan pénal ou civil* ».

Dans la plupart des cas, les *exploitants de plateformes et de moteurs de recherche* fournissent leurs services gratuitement. En règle générale, ils concluent néanmoins des accords avec

[314] Voir ch. 2.2.2.
[315] *Weber*, E-Commerce, 371 avec d'autres références dans la note de bas de page 1878.
[316] *Weber*, E-Commerce, 372.
[317] Voir ch. 2.2.2.
[318] Voir *Weber*, E-Commerce, 375.
[319] *Weber*, E-Commerce, 377 s.
[320] Voir ch. 4.1.1, d), aa).

leurs utilisateurs, par lesquels ces derniers acceptent diverses dispositions contractuelles qui comprennent le plus souvent une « *Acceptable Use Policy* ».

La validité de ces clauses d'exclusion de responsabilité doit être appréciée selon les règles générales du droit des contrats, dont le fondement est le principe de la liberté contractuelle, et notamment de la liberté du contenu du contrat: l'objet d'un contrat peut être librement déterminé, dans les limites de la loi (art. 19, al. 1, CO). Dans le contexte qui nous intéresse, l'une de ces limites est posée par l'art. 8 LCD qui prévoit, depuis le 1er juillet 2012, un contrôle du contenu des clauses des CG. Selon cette disposition, celui qui utilise des conditions générales qui, en contradiction avec les règles de la bonne foi, prévoient une disproportion notable et injustifiée entre les droits et les obligations découlant du contrat au détriment du consommateur, agit de façon déloyale. Selon la doctrine dominante, une clause de ce type est réputée nulle et non avenue[321]. Cette disposition s'applique uniquement aux CG des contrats conclus avec des consommateurs. Les contrats conclus entre personnes morales ou les contrats conclus dans l'exercice d'une activité professionnelle ou commerciale ne sont pas concernés[322]. Pour établir s'il y a une disproportion notable entre les droits et les obligations contractuels au détriment du consommateur, il faut examiner la situation juridique qui prévaudrait entre les parties sans les CG en question[323]. Une clause n'est par ailleurs frappée de nullité que si la disproportion notable est également injustifiée et contraire aux règles de la bonne foi. Il s'agit là d'effectuer une pesée de tous les intérêts dignes de protection de l'utilisateur des CG et du partenaire contractuel[324].

Une réserve contractuelle du fournisseur l'autorisant à limiter certaines de ses prestations ou à ne pas les fournir pour se protéger d'actions en responsabilité semble fondamentalement compatible avec l'art. 8 LCD, mais une pesée des intérêts en présence dans le cas d'espèce demeure inévitable.

Il convient également de rappeler que les art. 100, al. 1, et 101, al. 2, CO autorisent sans restriction les clauses contractuelles d'exclusion et de limitation de la responsabilité des auxiliaires, mais que, pour ce qui est des actes des fournisseurs eux-mêmes, ces clauses ne sont licites qu'en cas de négligence légère ou moyenne[325]. Dans les rares cas où un fournisseur Internet supprimerait ou bloquerait des contenus licites en faisant preuve d'une négligence grave et sans recourir à des auxiliaires, l'exclusion contractuelle de la responsabilité resterait sans effet.

Notons encore que lorsque des utilisateurs publient des contenus sur Internet en dehors de toute relation contractuelle préalable (par ex. les commentaires d'un blog), leur suppression ou leur blocage par l'exploitant de la plateforme ou par le fournisseur d'hébergement ne posera généralement aucun problème car, dans ce cas, l'auteur n'a en principe aucun droit contractuel à ce que son contenu soit publié[326].

---

321 *Schwenzer*, n° 46.05.

322 Voir *Gauch/Schluep/Schmid*, OR AT I, n° 1152b.

323 *Gauch/Schluep/Schmid*, OR AT I, n° 1153a ss.

324 Message du 2.9.2009 concernant la modification de la loi fédérale contre la concurrence déloyale (LCD), FF 2009 5539, 5567; *Gauch/Schluep/Schmid*, OR AT I, n° 1154a.

325 Sur l'ensemble de la question, voir *Schwenzer*, n° 24.04 ss.

326 La question de la qualification de la relation juridique entre l'auteur d'un commentaire et le média en ligne concerné peut rester ouverte, car même si un contrat liait les parties, le droit à la publication des contenus ne serait opposable que s'il était prévu explicitement. Il n'existe a priori aucune (autre) base permettant d'exiger la publication. De fait, une obligation de contracter découlant du droit de la

4.2 Jurisprudence de la Cour EDH

Dans l'affaire Delfi AS contre Estonie[327], la Cour EDH s'est penchée sur une action en dommages-intérêts contre un portail d'actualités sur Internet. Le portail Delfi avait publié un article critique au sujet du propriétaire d'une société de navigation par ferry. Les utilisateurs du site Internet pouvaient écrire des commentaires dans une rubrique intitulée « *add your comment* ». Plusieurs des commentaires déposés contenaient des menaces personnelles et des insultes dirigées contre le propriétaire de la société de navigation. Après l'intervention de ce dernier, Delfi avait immédiatement effacé les commentaires en question, mais six semaines s'étaient déjà écoulées depuis leur publication[328]. Delfi avait en outre refusé de payer un dédommagement. Par la suite, la justice civile estonienne a accordé une indemnité pour tort moral équivalente à 320 euros au propriétaire de la société de navigation, en invoquant le fait que Delfi exerçait un contrôle sur les contenus qu'elle publiait. La Grande Chambre de la Cour EDH a estimé que cela ne contrevenait pas à l'art. 10 CEDH[329] car l'ingérence dans l'exercice de la liberté d'expression n'était pas disproportionnée. Les juges ont surtout fondé leur argumentation sur les aspects suivants du cas d'espèce: Delfi est un grand portail d'actualités sur Internet qui agit à titre professionnel, en encourageant ses lecteurs à rédiger des commentaires sur les articles publiés, commentaires dont il tire un avantage économique. Les commentaires en question étaient clairement diffamatoires et certains contenaient même des incitations à la violence. Leur teneur était donc clairement illicite. De plus, Delfi n'avait été condamnée qu'au paiement d'une petite réparation pour tort moral. La Cour s'attarde notamment sur le fait que, selon son interprétation du jugement estonien, Delfi aurait été tenue de retirer les commentaires litigieux sans délai, de sa propre initiative, après leur publication, mais pas d'intervenir en amont pour en empêcher la mise en ligne[330]. Enfin, le jugement en question visait les seuls portails d'actualités professionnels, excluant explicitement les forums de discussion et les sites de diffusion électronique, ou encore les plateformes de médias sociaux où le fournisseur ne produit aucun contenu[331].

Delfi avait objecté que, s'agissant des commentaires de ses lecteurs, elle avait qualité de fournisseur d'hébergement et qu'elle pouvait donc faire valoir l'exonération de responsabilité prévue par la disposition du droit estonien qui transpose l'art. 14 de la directive européenne sur le commerce électronique. La Cour EDH n'est pas entrée en matière sur cet argument, estimant qu'il appartient aux tribunaux nationaux d'interpréter le droit national. La Cour d'État (juridiction suprême d'Estonie) avait certes admis que les portails Internet ne pouvaient être assimilés à des médias traditionnels, mais elle avait estimé que sur le plan économique, Delfi devait être considéré comme l'éditeur des commentaires[332]. La Cour n'a vu aucune raison de remettre en question ce raisonnement[333] et, dans son argumentation sur la proportionnalité, elle a aussi fait sien le point de vue de la Cour d'État selon lequel le contrôle que Delfi exerce

---

personnalité ou des « bonnes mœurs » ne peut être envisagée que dans des conditions strictement définies (voir *Gauch/Schluep/Schmid*, OR AT I, n° 1101a ss.).

327 Cour EDH, 16.6.2015, n° 64569/09, Delfi AS c. Estonie (Grande Chambre) ; la première section de la Cour avait déjà rendu une décision le 10.10.2013.

328 Cour EDH, 16.6.2015, n° 64569/09, Delfi AS c. Estonie, ch. 17 ss.

329 Voir également les explications au ch. 1.3.2 c) au sujet de l'art. 16 Cst., qui vise pratiquement les mêmes droits.

330 Cour EDH, 16.6.2015, n° 64569/09, Delfi AS c. Estonie, ch. 153.

331 Cour EDH, 16.6.2015, n° 64569/09, Delfi AS c. Estonie, ch. 116 s.

332 Cour EDH, 16.6.2015, n° 64569/09, Delfi AS c. Estonie, ch. 112.

333 Cour EDH, 16.6.2015, n° 64569/09, Delfi AS c. Estonie, ch. 113.

sur les commentaires de lecteurs va au-delà du rôle d'un prestataire passif de services purement techniques[334].

4.3 Droit étranger

4.3.1 Union européenne

a) Droit en vigueur

aa) Directive sur le commerce électronique

Comme nous l'avons déjà vu[335], les art. 12 ss. de la directive sur le commerce électronique prévoient une limitation de la responsabilité des fournisseurs. Celle-ci s'applique dans tous les domaines juridiques – horizontalement – pour toutes les actions réparatrices contre les fournisseurs ayant des fonctions de simple transport, de *caching* et d'hébergement. Si une partie des États membres continuent à admettre les actions en suppression et en cessation de l'atteinte malgré ce privilège en matière de responsabilité[336], la doctrine estime quant à elle unanimement que, en raison des art. 12 ss. de la directive sur le commerce électronique, les actions réparatrices contre les fournisseurs devraient être totalement exclues, pour autant que les conditions énoncées soient remplies[337]. Jusqu'à présent, la jurisprudence est a priori sur la même ligne.

Pour les fournisseurs d'hébergement, l'art. 14, al. 1, de la directive prévoit ceci:

> « (1) Les États membres veillent à ce que, en cas de fourniture d'un service de la société de l'information consistant à stocker des informations fournies par un destinataire du service, le prestataire ne soit pas responsable des informations stockées à la demande d'un destinataire du service à condition que:
>
> a) le prestataire n'ait pas effectivement connaissance de l'activité ou de l'information illicites et, en ce qui concerne une demande en dommages et intérêts, n'ait pas connaissance de faits ou de circonstances selon lesquels l'activité ou l'information illicite est apparente ou
>
> b) le prestataire, dès le moment où il a de telles connaissances, agisse promptement pour retirer les informations ou rendre l'accès à celles-ci impossible. »

Le champ d'application de l'art. 14 de la directive sur le commerce électronique a été concrétisé par plusieurs arrêts de la CJUE qui ont déjà été présentés ici[338].

bb) Protection des données

Pour ce qui est de la responsabilité en cas de dommage causé dans le cadre du traitement de données à caractère personnel, la directive sur la protection des données[339] prévoit ceci (art. 23):

> « (1) Les États membres prévoient que toute personne ayant subi un dommage du fait d'un traitement illicite ou de toute action incompatible avec les dispositions nationales

[334] Cour EDH, 16.6.2015, n° 64569/09, Delfi AS c. Estonie, ch. 146.
[335] Ch. 3.3.1 a), bb).
[336] Voir ch. 3.3.1 c) et d)
[337] Voir *Härting*, n° 2131 ss. ; *Frech*, 286 s. avec d'autres références.
[338] Voir ch. 3.3.1 b) et en particulier les arrêts Google c. France, Svensson et L'Oréal c. Ebay.
[339] Voir note 103.

> prises en application de la présente directive a le droit d'obtenir du responsable du traitement réparation du préjudice subi.
>
> (2) Le responsable du traitement peut être exonéré partiellement ou totalement de cette responsabilité s'il prouve que le fait qui a provoqué le dommage ne lui est pas imputable. »

b) Transposition dans les États membres

En *Allemagne*, le § 10 de la *Telemediengesetz* exclut la responsabilité en dommages-intérêts du fournisseur d'hébergement lorsque celui-ci n'a pas connaissance de faits ou de circonstances mettant en évidence de manière flagrante l'acte illicite ou l'information, ou lorsqu'il est intervenu sans délai pour supprimer l'information ou en bloquer l'accès dès qu'il en a eu connaissance. La doctrine interprète cette connaissance comme une connaissance positive de la teneur concrète de l'information. Un vague indice selon lequel des contenus illicites se trouveraient sur les serveurs du fournisseur serait insuffisant[340].

En *Autriche*, la jurisprudence n'a, a priori, pas beaucoup eu à se pencher sur la question de la responsabilité en dommages-intérêts des fournisseurs d'hébergement au sens du § 16 de la *E-Commerce-Gesetz*[341]. D'après les travaux préparatoires, la responsabilité du fournisseur ne devrait être engagée que si la violation du droit est flagrante pour un non-juriste, sans qu'il faille effectuer de recherches approfondies[342]. En d'autres termes, le législateur autrichien estime qu'il faut interpréter la notion de « connaissance effective » de façon étroite et que, par conséquent, la responsabilité pénale et administrative du fournisseur d'hébergement ne doit être engagée qu'en cas de certitude. Pour l'action en dommages-intérêts, il n'exige en revanche qu'un « devoir de connaissance » (*Kennenmüssen*)[343].

Une étude sur la responsabilité des fournisseurs dans les États membres réalisée sur mandat de la Commission européenne a conclu que, en ce qui concerne le privilège des fournisseurs d'hébergement (art. 14, al. 1, de la directive sur le commerce électronique), des interprétations divergentes du critère de la « connaissance de l'illégalité d'un contenu » avait conduit à un éparpillement législatif[344].

4.3.2 États-Unis

Aux *États-Unis*, comme nous l'avons déjà vu[345], la responsabilité des fournisseurs ne peut être limitée qu'en raison de la présence d'« *offensive material* » (à l'exclusion expresse des violations de droits de propriété intellectuelle) [346], de violations de droits d'auteur[347] et de

---

340 *Härting*, n° 2126 et autres références.
341 Voir ch. 3.3.1 d).
342 Voir le projet gouvernemental autrichien, n° 817, *Beilagen zu den Stenographischen Protokollen des Nationalrates XXI. Gesetzgebungsperiode*, ad § 16.
Disponible à l'adresse www.uibk.ac.at/strafrecht/strafrecht/ecgrv.pdf.
343 Projet gouvernemental autrichien (voir note 342), § 16.
344 *Verbiest/Spindler/Riccio Giovanni/van der Perré*, 14 ss.
345 Voir ch. 3.3.2.
346 § 230(c) *Communications Decency Act*.
347 § 512 *Digital Millennium Copyright Act*.

violations de droits de marque[348]. Les règles générales en matière de responsabilité à l'égard des fournisseurs s'appliquent dans les autres domaines.

5 Droits à l'information et droit d'accès

5.1 Droit suisse

5.1.1 Remarques générales

L'examen des droits à l'information à l'égard des fournisseurs vise à déterminer si et, si oui, à quelles conditions le titulaire d'un droit peut exiger que le fournisseur révèle les données d'un usager qui a commis une infraction. La procédure pénale occupe ici une place importante dans la pratique puisque, contrairement à la procédure civile, elle peut aussi être conduite contre un auteur inconnu. Dans certaines circonstances, le droit pénal est donc utilisé pour déterminer l'identité de la personne qui fera éventuellement l'objet de poursuites civiles. C'est la raison pour laquelle les aspects pénaux sont abordés ici avant les questions de droit civil.

5.1.2 Droit pénal

a) Droit à l'information des autorités de poursuite pénale selon la LSCPT et le CPP

La surveillance de la correspondance par télécommunications dans le cadre de la procédure pénale est régie par la LSCPT[349] et le code de procédure pénale (CPP)[350], en particulier par *l'art. 14, al. 4, LSCPT* pour l'*identification rétroactive des usagers* lorsqu'un acte punissable a été commis au moyen d'Internet. Cette identification nécessite que l'autorité de poursuite pénale demande au fournisseur d'accès des informations sur le raccordement auquel il a attribué une adresse IP dynamique donnée à un moment donné[351]. La question se pose de savoir si cette identification peut aussi être utilisée dans le cadre de la procédure civile.

Les *adresses IP dynamiques* (contrairement aux adresses statiques) font partie des données dites secondaires de la correspondance par télécommunications[352]. Les *données secondaires* ne révèlent pas le contenu des conversations mais permettent de savoir qui a été en communication avec qui, où et pendant combien de temps[353]. En vertu de l'art. 15, al. 3, LSCPT, les données secondaires doivent être conservées pendant six mois[354].

Conformément à l'*art. 273 CPP*, le ministère public ne peut exiger la remise des données secondaires et il ne peut exploiter ces dernières dans le cadre de la procédure pénale que s'il s'agit de poursuivre un crime ou un délit d'une certaine gravité dans le cas d'espèce (principe de proportionnalité). De plus, l'ordre de surveillance est *soumis à l'autorisation* du tribunal des

348 § 32(2) *Lanham Act*.
349 RS 780.1
350 RS 312.0
351 Au sujet de la fonction des adresses IP dynamiques, voir ATF 136 II 508, 514 s.
352 *Hansjakob*, Kommentar BÜPF, ad art. 14 LSCPT, n° 26.
353 Voir art. 273, al. 1, let. a, CPP.
354 Voir art. 273, al. 3, CPP (délai de collecte des données secondaires dans le cadre de la procédure pénale).

mesures de contrainte. Ainsi, les données secondaires ne peuvent pas être utilisées dans une procédure pénale en cas de contravention[355].

Cela entraîne des *points de friction* avec la règlementation sur l'identification rétroactive des usagers précitée, car le libellé de l'art. 14, al. 4, LSCPT élargit en quelque sorte le champ de l'art. 273 CPP, tout en comportant une restriction essentielle:

- contrairement à l'art. 273 CPP, l'art. 14, al. 4, LSCPT vise *uniquement à identifier* un usager d'Internet dans le cas d'un *acte punissable commis au moyen d'Internet;*
- cependant, l'art. 14, al. 4, LSCPT permet l'utilisation de « *toute indication* » permettant d'identifier l'auteur. L'identification de l'usager ne doit donc pas satisfaire aux conditions strictes posées à l'art. 273 CPP, et ce même lorsqu'il est nécessaire d'analyser l'attribution d'adresses IP dynamiques – et par conséquent des données secondaires[356];
- de plus, le terme utilisé à l'art. 14, al. 4, LSCPT (« acte punissable ») ne pose aucune restriction quant à la nature de l'infraction, contrairement à l'art. 273 CPP, ce qui permet donc aussi d'exiger l'identification d'un usager en cas de *contravention*[357]*;*
- selon une interprétation systématique et historique[358] de l'art. 14 LSCPT et de l'art. 16 de l'ordonnance du 31 octobre 2001 sur la surveillance de la correspondance par poste et télécommunication[359], l'identification des usagers au sens de l'art. 14, al. 4, LSCPT doit se dérouler dans le cadre d'une *procédure simplifiée*, autrement dit l'autorisation du tribunal des mesures de contrainte n'est pas requise[360].

---

[355] Seule exception: l'utilisation abusive d'une installation de télécommunication au sens de l'art. 179septies CP).

[356] *Hansjakob*, Kommentar BÜPF, ad art. 14 LSCPT n° 26. Cf. cependant ATF 141 IV 108; à ce sujet, voir note 360.

[357] *Hansjakob*, Kommentar BÜPF, ad art. 14 LSCPT n° 23.

[358] Décision de la Commission de recours du Département fédéral de l'environnement, des transports, de l'énergie et de la communication du 27.4.2004 dans la procédure de recours J-2003-162 (Fob), consid. 6.2.1 ss. (à consulter à l'adresse www.reko-inum.ch/dokumente/114010669724120.pdf). Cette décision fournit des informations exhaustives sur la genèse de l'art. 14, al. 4, LSCPT. D'un autre avis : *Trechsel/Lieber*, StGB Praxiskommentar, ad art. 179octies n° 5, avec renvoi à l'ATF 126 I 60.

[359] RS 780.11

[360] Voir *Hansjakob*, Entwicklungen, 176 s. Voir également, en passant, ATF 141 IV 108, consid. 5.1, selon lequel les exigences de l'art. 273 CPP seraient obligatoirement applicables dès lors que l'adresse IP liée à une activité de communication doit être identifiée avant toute démarche ultérieure. Le Tribunal fédéral motive cet avis en renvoyant à une décision datant d'avant l'entrée en vigueur de l'art. 14, al. 4, LSCPT, mais sans mentionner d'autre jurisprudence en la matière (voir décision J-2003-162 de la Commission de recours en matière d'infrastructures et d'environnement [CRINEN] du 27.4.2004 [note 358]). Dans son interprétation du droit en vigueur, il renvoie en outre au message relatif au projet de révision de la LSCPT (projet FF 2013 2483; message FF 2013 2379) dont l'examen parlementaire est actuellement en cours (septembre 2015). Il semble possible qu'il y ait ici confusion entre l'octroi de renseignements (section 5, art. 21 ss. P-LSCPT) et la surveillance (section 6, art. 26 ss. P-LSCPT), car l'arrêt du Tribunal fédéral ne fait aucune référence aux explications (voir message, p. 2431) données au sujet de l'art. 22 du projet – qui correspond aux dispositions en vigueur sur l'identification des usagers lors d'actes punissables commis au moyen d'Internet. En outre, l'avis incident exprimé par le Tribunal fédéral paraît peu compatible avec le considérant 4.8 de l'ATF 139 IV 98 et avec le libellé de l'art. 14, al. 4, LSCPT et restreint sans doute considérablement le champ d'application de cette *lex specialis* sur les actes punissables commis au moyen d'Internet (voir ATF 139 IV 98, 102). Des questions se posent également en matière de séquestre car, à première vue, on voit difficilement pourquoi d'autres données personnelles ou

L'emplacement des dispositions concernant l'identification rétroactive des usagers dans la LSCPT sous un titre « renseignements » soulève des questions et le rapport avec l'art. 273 CPP demande à être clarifié[361]. Amené à se prononcer sur la règle des délais de conservation et d'utilisation des données secondaires aux fins d'identification des usagers, le Tribunal fédéral a conclu que l'art. 14, al. 4, LSCPT était une *lex specialis* de l'art. 273 CPP[362].

En résumé, la situation en matière de droits à l'information se présente comme suit pour ce qui est de l'identification rétroactive des usagers au sens de la LSCPT et du CPP.

- On ne peut exiger une identification rétroactive des usagers selon l'art. 14, al. 4, LSCPT pour faire valoir uniquement des prétentions relevant du droit civil, car il doit exister un lien avec une procédure pénale. Le droit en vigueur n'offre donc la possibilité d'identifier les auteurs d'actes punissables pour faire valoir des conclusions civiles que *par adhésion*[363] à une procédure pénale[364].
- Une identification rétroactive des usagers selon l'art. 14, al. 4, LSCPT peut être exigée dans le cadre d'une procédure pénale pour *délit* contre les droits de propriété intellectuelle[365]. Dans ce type de procédure, les données secondaires peuvent aussi être exigées et utilisées conformément à l'art. 273 CPP. Il faut cependant relever que, au sens de l'art. 269, al. 1, let. b, CPP, il faut justifier de façon particulière la *gravité du cas d'espèce* pour pouvoir exiger la production des données secondaires. Le fait de devoir fonder la proportionnalité (pratiquement irréfutable en cas d'assassinat, par ex.) pourrait souvent se révéler problématique en matière de droit pénal de la propriété intellectuelle et n'être admise que lorsque quelqu'un viole de façon particulièrement grave (et systématique) les droits de propriété intellectuelle de tiers. On pense ici surtout aux cas de violation par métier.
- Une identification rétroactive de l'usager conformément à l'art. 14, al. 4, LSCPT est aussi envisageable en cas de *contravention* aux droits de propriété intellectuelle. En revanche, une surveillance rétroactive au sens de l'art. 273 CPP n'est pas possible.

même protégées par un secret (professionnel) pourraient continuer à faire l'objet d'un séquestre selon la procédure normale mais non les adresses IP. En effet, ces dernières ne sont même pas soumises au secret des télécommunications (les fournisseurs d'hébergement ou de plateformes n'étant pas des fournisseurs de services de télécommunication puisqu'ils ne transmettent pas d'informations pour le compte de tiers [voir art. 3, let. b, LTC et art. 321ter CP]). Le fait que le séquestre de courriels auprès du fournisseur de courrier électronique du prévenu ne doive pas être approuvé par le tribunal des mesures de contrainte serait également une incohérence (voir ATF 140 IV 181). Avis contraire à l'applicabilité de l'art. 273 CPP dans une argumentation en matière de télécommunications : *Roth*, Jusletter du 17.8.2015, n° 18 ss.

361 Voir *Heiniger*, Jusletter du 29.4.2013, n° 3.3.

362 ATF 139 IV 98, 102 (délivrance et utilisation de données secondaires conservées sans obligation au-delà du délai légal aux fins d'identification d'un usager en cas d'acte punissable commis au moyen d'Internet au sens de l'art. 14, al. 4, LSCPT). Le Tribunal fédéral a précisé cet arrêt dans l'ATF 139 IV 195, 198, s'agissant de la surveillance rétroactive au sens de l'art. 273 CPP (voir également ch. 5.1.2.b). Les renseignements sur les données de base visés à l'art. 14, al. 1, LSCPT, qui ne sont pas des données secondaires (et les adresses IP dynamiques n'en font donc pas partie), doivent pouvoir être produites rétroactivement pendant dix ans (voir ATF 141 IV 108, consid. 6.2).

363 Art. 122 ss. CPP.

364 Voir ATF 136 II 508, 522 ss. (Logistep), où des adresses IP collectées par des particuliers ont (aussi) été utilisées dans le cadre de la poursuite pénale.

365 Notamment art. 67 ou 69 LDA, ou encore art. 61, 62, 63 ou 64 LPM.

La LSCPT fait actuellement (septembre 2015) l'objet d'une *révision totale*. Le projet du Conseil fédéral[366] prévoit notamment d'étendre le champ d'application à raison des personnes à d'autres fournisseurs Internet (par ex. les purs fournisseurs de courrier électronique ou exploitants de plateforme, qui revêtent une grande importance pour la poursuite pénale) et de prolonger le délai de conservation des données secondaires de six à douze mois. Des dispositions pénales visent aussi à s'assurer la coopération des fournisseurs[367]. Par contre, le projet ne prévoit pas d'élargir la surveillance à des infractions moins graves que celles prévues dans le droit en vigueur.

b) Rapport entre surveillance rétroactive (art. 273 CPP) et séquestre (art. 263 ss. CPP)

Le relevé des données secondaires au sens de *l'art. 273 CPP* est un cas particulier du séquestre des moyens de preuve[368]. Cette activité, communément appelée « surveillance rétroactive », fait l'objet d'une règlementation particulière parce qu'il s'agit d'une mesure de contrainte secrète, qui est donc soumise à des règles de procédure plus strictes afin de protéger la personne surveillée[369]. De plus, elle vise des données qui sont couvertes par le secret des télécommunications[370]. Ce sont les raisons pour lesquelles cette mesure doit être approuvée par le tribunal des mesures de contrainte, comme cela a déjà été mentionné.

Mais des données secondaires peuvent aussi tomber entre les mains des autorités de poursuite pénale lors du séquestre (*art. 263 ss. CPP*) d'appareils techniques, que ce soit chez un prévenu ou chez un fournisseur de courrier électronique ou exploitant de plateforme irrépréhensible, sur la plateforme duquel des actes punissables ont été commis[371]. La question se pose alors de savoir si les règles strictes de l'art. 273 CPP (liste d'infractions, compétence d'autorisation du juge et délai) doivent aussi s'appliquer aux données secondaires obtenues par le biais d'un séquestre. Les éléments ci-après doivent être pris en compte.

- Le séquestre n'est *pas une mesure de contrainte secrète*[372].
- Lors du séquestre de serveurs et autres appareils chez le prévenu ou chez un autre usager (par ex. le service informatique interne d'une entreprise), *le secret des télécommunications n'est pas affecté* si des courriels et des données secondaires (contenus des communications) sont enregistrés sur ces appareils[373].

---

366 Projet FF 2013 2483; message FF 2013 2379.

367 Au sujet de la punissabilité d'un fournisseur pour entrave à l'action pénale (art. 305 CP) pour avoir effacé des adresses IP (non-respect de l'obligation de renseigner selon la LSCPT), voir l'arrêt du Tribunal fédéral 6B_766/2009 du 8.1.2010, consid. 3.

368 Selon la doctrine, l'art. 273 CPP prête à confusion (*Hansjakob*, Kommentar StPO, ad art. 273 n° 2): l'identification des usagers figure certes dans le titre de l'article, mais n'apparaît pas dans ses dispositions. De plus, les données de la catégorie « renseignements » (selon l'art. 14 LSCPT, c'est-à-dire les ressources d'adressage selon la LTC, le nom et l'adresse de l'usager, etc.), qui permettent notamment d'identifier l'usager dans le domaine de la téléphonie, ne relèvent pas du secret des télécommunications et, par voie de conséquence, de l'art. 273 CPP (voir *Hansjakob*, Kommentar StPO, ad art. 272 n° 4).

369 *Hansjakob*, Kommentar StPO, ad art. 272 n° 1.

370 BSK StPO-*Jean-Richard-dit-Bressel*, ad art. 273 n° 1.

371 S'agissant de la perquisition antérieure du moyen de preuve devant éventuellement être séquestré, voir art. 246 ss. CPP; s'agissant des découvertes fortuites, voir art. 243 CPP.

372 Voir *Heimgartner*, Kommentar StPO, ad art. 263 n° 5 et *Hansjakob*, Kommentar StPO, ad art. 269 n° 9.

373 *Heimgartner*, Kommentar StPO, ad art. 263 n° 5, avec renvois. À propos du séquestre auprès d'un fournisseur de services de télécommunication (fournisseur d'accès): ATF 140 IV 181, 186.

- L'*art. 273 CPP* est vise des situations où les données doivent être acquises *auprès d'un fournisseur de services de télécommunication* (FST)[374]. Le libellé de l'art. 179^octies CP laisse en outre à penser que le motif justifiant la surveillance de la correspondance par télécommunication ne s'applique qu'aux fournisseurs *qui relèvent du champ d'application de la LSCPT* (voir également l'art. 274, al. 3, CPP)[375].
- Il y a une *controverse quant à la nature juridique et au champ d'application du délai de six mois* prévu à l'art. 273, al. 3, CPP: selon certains avis de doctrine, cette disposition vise exclusivement à protéger les intérêts des FST et n'est, de ce fait, pas une prescription en matière de moyens de preuve mais simplement une sorte de « prescription d'ordre »[376]. Dans ce cas, l'exploitation des données secondaires séquestrées ne serait également soumise à aucune restriction temporelle. Un autre avis défend le point de vue selon lequel le délai doit être appliqué strictement, même lorsque le fournisseur dispose de données plus anciennes[377]. Vu sous cet angle, l'interdiction d'exploiter les données secondaires séquestrées s'appliquerait pleinement aux données datant de plus de six mois[378]. La jurisprudence du Tribunal fédéral n'a pas encore fait toute la lumière sur ce point[379]. Même si, de fait, le libellé de l'art. 273, al. 3, CPP est clair, une interprétation restrictive semble hasardeuse pour les raisons suivantes:
    - il y a une incohérence entre ce délai et l'absence de limite absolue dans le temps pour la surveillance du contenu des communications[380], qui est pourtant une ingérence plus radicale que la surveillance rétroactive;

---

[374] Message du 21.12.2005 relatif à l'unification du droit de la procédure pénale, commentaire de l'art. 272 (FF 2006 1057, 1232). Dans le même sens: *Keller*, Kommentar StPO, ad art. 246 n° 8, en partant du champ d'application du secret des télécommunications. Les simples services d'hébergement (tels que les services *cloud*) et les services de téléphonie *peer-to-peer* sur Internet, mais aussi les simples services de courrier électronique ou exploitants de plateformes n'entrent pas dans le champ d'application actuel de la LSCPT, car ils ne sont pas fournis par des FST « traditionnels » (pas de transmission d'informations pour le compte de tiers au sens de l'art. 3, let. b, LTC). Le projet de révision de la LSCPT proposé par le Conseil fédéral introduit la notion de « fournisseurs de services de communication dérivés » pour englober tous ces fournisseurs de services (voir art. 2, let. c, P-LSCPT [FF 2013 2483, 2484] ainsi que les explications fournies dans le message LSCPT [FF 2013 2379, 2401 s.]).

[375] S'agissant de l'art. 179^octies, al. 2, CP, il est permis de se demander si le renvoi à la seule LSCPT est suffisant, puisque les dispositions de l'ancienne LSCPT en matière de procédure pénale sont aujourd'hui intégrées dans le CPP. Ainsi, dans tous les cas de figure, l'art. 179^octies CP n'a guère plus qu'une valeur déclaratoire (voir également la disposition déclaratoire de l'art. 14 CP).

[376] *Zufferey/Bacher*, CR CPP, ad art. 273 n° 7. Voir cependant le délai correspondant à l'art. 15, al. 3, LSCPT.

[377] *Hansjakob*, Kommentar BÜPF, ad. art. 5 LSCPT, n° 20.

[378] *Hansjakob*, Kommentar StPO, ad art. 273 n° 16, parle de deux objectifs, sans toutefois approfondir la question. Commentaires et critique sur la problématique des délais : *Hansjakob* (*ibid.*) n° 17 s.

[379] Dans l'ATF 139 IV 98, 101 s. – qui ne concernait pas une surveillance rétroactive au sens de l'art. 273 CPP mais l'identification d'un usager d'Internet selon l'art. 14, al. 4, LSCPT –, le Tribunal fédéral constate qu'aucun des deux avis précités n'est convaincant. Selon lui, le délai permet dans tous les cas et sans autre justification le relevé rétroactif jusqu'à six mois et même au-delà, si des motifs particuliers le justifient. Le Tribunal fédéral ne dit cependant pas quels pourraient être ces motifs particuliers (sur ce point, voir *Hansjakob*, Kommentar StPO, ad art. 273 n° 15 ss., notamment sur la problématique du calcul des délais). Peu de temps après, il a toutefois précisé, voire relativisé ce point de vue dans l'ATF 139 IV 195, 198, et décidé que pour une surveillance rétroactive au sens de l'art. 273 CPP, le délai prévu à l'art. 273, al. 3, CPP s'appliquait de manière stricte.

[380] Voir art. 274, al. 5, CPP.

- si le contenu des communications peut aussi être exploité au-delà du délai lorsque celles-ci proviennent d'un séquestre effectué auprès de personnes qui n'entrent pas dans le champ d'application de la LSCPT, il est peu probable que le délai prévu à l'art. 273, al. 3, CPP serve uniquement la protection du prévenu;
- il se peut que le poids soit mis principalement sur les intérêts des personnes – irrépréhensibles – dont les données sont conservées en masse chez le FST, car la conservation des données secondaires constitue une atteinte grave aux droits fondamentaux des personnes concernées. Ce point occupe en tout cas une place centrale dans l'arrêt de la Cour EDH concernant la directive européenne sur la conservation des données[381]. Or, si la Cour met l'accent sur les personnes visées par la conservation des données, il semble qu'en Suisse, jusqu'ici, la discussion a surtout porté sur le point de vue de la personne qui fait effectivement l'objet d'une surveillance rétroactive, autrement dit le prévenu[382]. Dans un arrêt[383] en relation avec l'art. 273, al. 3, CPP, le Tribunal fédéral aborde tout de même (brièvement) la question de la sphère privée des personnes irrépréhensibles concernées par la conservation des données;
- attribuer au délai prévu à l'art. 273, al. 3, CPP une portée générale en matière de protection des données semble tout aussi hasardé que d'y voir une volonté de protéger les intérêts économiques des FST. Il serait plus juste de dériver ces buts à partir des restrictions de la LSCPT en matière de conservation des données[384] qui, contrairement aux dispositions du CPP, visent directement les FST qui conservent des données en masse.

Sous l'angle du droit régissant le séquestre, la situation se présente donc comme suit.

- Le séquestre du contenu des communications ou des données secondaires *auprès des fournisseurs assujettis à la LSCPT* est en principe *interdit*[385].
- Le séquestre du contenu des communications (lettres et courriels enregistrés) *auprès de personnes et d'entreprises qui ne sont pas assujetties à la LSCPT* (par ex. auprès du prévenu ou d'un simple fournisseur de courrier électronique ou exploitant de plateforme) est *autorisé*, indépendamment du fait que la correspondance visée date d'un mois ou d'un an: les règles en matière de surveillance des télécommunications ne s'appliquent pas[386]. Cela devrait donc *aussi* être le cas *pour le séquestre des données secondaires*, l'atteinte aux droits fondamentaux de la personne concernée étant ici

[381] Arrêt de la CJUE du 8.4.2014 dans les affaires jointes C-293/12 et C-594/12 (Digital Rights Ireland et Seitlinger et al.) ; pour plus de détails, voir ch. 5.3.1 a).
[382] Message CPP, commentaire de l'art. 272 (FF 2006 1057, 1232).
[383] ATF 139 IV 195, 198.
[384] Voir art. 15, al. 3, LSCPT.
[385] Le séquestre n'est possible que dans des cas particuliers, car les règles spéciales de la LSCPT en matière de production des preuves sont normalement prépondérantes. Lorsque le prévenu consulte son compte de courrier électronique auprès du FST et qu'il laisse ses courriels sur le serveur (le FST ne se limite donc pas à transmettre des données, mais il offre aussi des services de courrier et de la mémoire), les courriels en question doivent être séquestrés chez le FST car les conditions préalables à une surveillance des télécommunications ne sont plus remplies (voir ATF 140 IV 181, 186 s.).
[386] Cependant, le projet du Conseil fédéral élargit considérablement le champ d'application de la LSCPT, raison pour laquelle les règles en matière de surveillance des télécommunications s'appliqueront si le fournisseur y est aussi assujetti.

moins grave[387]. Il faut souligner que la remise et l'exploitation des objets séquestrés doivent être autorisées par le tribunal si le propriétaire a exigé leur mise sous scellés (art. 248, al. 3, CPP). Au final, il n'existe donc pas de compétence impérative du juge pour les données secondaires séquestrées (contrairement à ce qui est le cas pour une surveillance secrète des télécommunications), mais il y a tout de même un contrôle judiciaire en cas de procédure de levée des scellés.

- Les règles régissant le séquestre ne contiennent aucune restriction à certaines infractions ou types d'infractions, comme à l'art. 273 CPP. Il faut cependant relever que, en vertu de l'art. 197, al. 1, let. c et d, CPP, le séquestre doit respecter le *principe de proportionnalité* dans chaque cas d'espèce[388]. S'agissant des cas de contravention, la mesure ne devrait pouvoir être qualifiée de proportionnelle que dans des configurations particulières[389] ou dans des situations exceptionnelles[390].
- La protection des sources des professionnels des médias (art. 172 CPP) entraîne en principe une *interdiction de séquestre* (art. 264 CPP) et ce, quel que soit l'endroit où les documents et objets visés se trouvent. L'interdiction de séquestre ne s'applique donc pas uniquement à la documentation journalistique conservée chez les professionnels des médias mais aussi à celle qui se trouve chez le prévenu ou chez des tiers[391].

c) Droit à l'information découlant de l'art. 322 CP (obligation de renseigner des entreprises de médias)

Un droit à l'information découle aussi, du moins de manière ponctuelle, de l'obligation des médias de renseigner qui est réglée à l'art. 322 CP. Le but premier de cette norme est certes de faciliter le déroulement de la *procédure pénale* contre les personnes qui ont une responsabilité subsidiaire dans des déclarations punissables (et qui peuvent taire l'identité de leur auteur si les conditions énoncées à l'art. 28*a* CP sont remplies). Mais dans les faits, les renseignements acquis par les entreprises de médias peuvent aussi être utilisés dans la procédure civile: selon l'art. 322 CP, les entreprises de médias sont en effet tenues d'indiquer immédiatement à toute personne qui le demande l'identité du rédacteur responsable ou du responsable de la publication. Et ensuite, ces personnes peuvent (aussi) faire l'objet d'une action civile.

Dans le domaine examiné, à savoir les communications en ligne, la portée de l'art. 322 CP est limitée car l'obligation de renseigner n'est opposable qu'aux *entreprises de média* à

---

[387] Cette incohérence du droit de la surveillance trouve ainsi son prolongement dans le droit en matière de séquestre. Illustration: une surveillance rétroactive au sens de l'art. 273 CPP menée auprès d'un FST (délai de 6 mois) débouche sur des indices d'actes punissables graves et systématiques commis sur la plateforme d'un fournisseur (non assujetti à la LSCPT). La procédure est donc élargie (en cas de découverte fortuite: nouvelle procédure), les serveurs du fournisseur sont perquisitionnés et les données sont séquestrées en qualité de moyen de preuve. Dans le cadre de la procédure pénale, toutes les données séquestrées peuvent être utilisées comme moyen de preuve, même si elles datent de plus de six mois.

[388] Voir l'arrêt du Tribunal fédéral 1B_294/2014 du 19.3.2015, consid. 4.4.

[389] Par ex. une enquête pour crime ou délit dans le cadre de laquelle la contravention est accessoire ou n'est versée au dossier que lors du séquestre des moyens de preuve.

[390] Par ex. un enquête en rapport avec la punissabilité des entreprises selon l'art. 102 CP.

[391] Arrêts du Tribunal fédéral 1B_424/2013 et 1B_436/2013 du 22.7.2014, consid. 6. En cas de surveillance des télécommunications, la protection des sources découle de l'art. 271 CPP.

proprement parler. Il existe toutefois quelques incertitudes au sujet de cette notion: elle a une signification plutôt large et ne couvre pas que les contenus journalistiques et rédactionnels publiés dans des médias de masse paraissant périodiquement. L'art. 322 CP s'applique par exemple aussi aux produits médiatiques qui n'ont que des contenus commerciaux (comme les prospectus publicitaires) et, d'une manière générale, à toutes les entreprises qui ont une activité dans un domaine quelconque de la communication et qui fournissent une contribution spécifique à la création d'un produit médiatique[392]. Une activité lucrative ou une inscription au registre du commerce ne sont que des indices, mais pas une condition de l'existence d'une entreprise de médias[393]. La question de savoir si les fournisseurs Internet doivent être considérés comme des entreprises de médias lorsqu'ils ne s'occupent pas du volet rédactionnel des contenus diffusés n'a pas été réglée. Pour les *fournisseurs d'accès* qui n'enregistrent aucun contenu sur leurs propres serveurs, la réponse est forcément négative[394]. En revanche, s'agissant des *fournisseurs d'hébergement* ou des *exploitants de plateformes*, la situation n'est pas aussi claire. Sur la base de leurs relations contractuelles avec les fournisseurs de contenus, ils pourraient souvent fournir des indications sur l'identité d'une personne responsable d'une publication précise. A priori, l'applicabilité de l'art. 322 CP aux fournisseurs ou aux exploitants de plateformes n'a pas encore été examinée par les tribunaux.

5.1.3 Droit civil

a) Introduction

Comme on l'a déjà mentionné, le droit civil suisse ne connaît pas l'action contre inconnu. Même la possibilité d'administrer des preuves à titre provisionnel inscrite dans le code de procédure civile (art. 158 du code de procédure civile [CPC][395]) ne permet pas d'obtenir l'*identité* d'un contrevenant inconnu. Cette procédure permet d'assurer la conservation de la preuve et d'évaluer les chances d'obtenir gain de cause ou d'apporter une preuve[396], mais ne peut, conformément aux règles générales, être introduite qu'à l'encontre d'un adversaire déjà connu[397]. Importante avant tout dans le droit d'auteur, la problématique de l'auteur inconnu est présentée ci-après dans le détail.

b) Obtention des données utilisateurs via la procédure pénale: la jurisprudence Logistep du Tribunal fédéral

Les titulaires de droits ont tenté par différents moyens de connaître l'identité des clients anonymes de fournisseurs qui ont échangé illicitement sur Internet des œuvres protégées par le droit d'auteur. Ils ont, à cet effet, souvent déposé une plainte pénale contre inconnu. En déposant une plainte pénale, puis en faisant usage du droit de consulter le dossier, les

[392] *Donatsch/Wohlers*, Strafrecht IV, 583.
[393] *Trechsel/Jean-Richard-dit-Bressel*, Praxiskommentar StGB, ad art. 322 n° 2.
[394] *Donatsch/Wohlers*, Strafrecht IV, 584 ; *Dupuis et al.*, Petit Commentaire Code pénal, ad art. 322 n° 11; BSK StGB II-*Zeller*, ad art. 322 n° 7.
[395] RS 272.
[396] Message du 28.6.2006 relatif au code de procédure civile suisse (CPC), FF 2006 6841, 6924.
[397] Implicitement : *Killias/Kramer/Rohner*, 941 ss. : rendre vraisemblable est un droit matériel *vis-à-vis de l'adversaire*. La preuve à futur est soumise à la procédure des mesures provisionnelles (art. 158, al. 2, CPC). L'adversaire (présumé) doit être entendu. (art. 253 CPC), voir message CPC (note 396), FF 2006 6841, 6924.

titulaires de droits parviennent à se procurer l'identité du contrevenant. Celle-ci est ensuite utilisée en général pour demander des dommages-intérêts.

Les titulaires de droits optent en général pour cette démarche dans le seul but de faire valoir ensuite des prétentions civiles envers l'auteur de l'infraction. Cette manière de procéder est cependant problématique, car les données d'identification (qui ne sont connues que par le fournisseur d'un accès Internet) sont en principe protégées par le secret des télécommunications[398].

Or, comme l'identification du détenteur d'un accès à Internet est possible seulement par le biais de la plainte pénale et qu'elle est une condition préalable pour que le titulaire de droits d'auteur puisse invoquer ses droits en procédure civile, ce dernier n'a *de lege lata* d'autre possibilité de lever le secret des télécommunications que par l'introduction d'une procédure pénale. Le PFPDT a jugé une telle démarche comme contraire au principe de la bonne foi et devant donc être considérée comme un abus de droit[399].

L'arrêt du Tribunal fédéral dans l'affaire Logistep[400] s'inscrit également dans ce contexte. Sur mandat des titulaires de droits, la société Logistep a collecté des adresses IP d'internautes (anonymes) présumés coupables d'infractions aux droits d'auteur pour avoir échangé principalement des fichiers musicaux et vidéo via des réseaux pair-à-pair. Sur la base de ces adresses IP, les titulaires de droits ont déposé une plainte pénale afin de se procurer, grâce au droit d'accès au dossier, les noms et les adresses des internautes concernés et de les mettre en demeure de verser des dommages-intérêts. Le PFPDT a considéré les agissements de Logistep comme abusifs.

La Cour suprême a admis que les adresses IP collectées constituaient des données personnelles[401] et qu'elles relevaient, comme telles, de la LPD. Elle était en outre d'avis que la collecte d'adresses IP par Logistep n'était pas conforme à la LPD. Elle a considéré que la protection de la personnalité et des droits fondamentaux des personnes concernées était plus importante que les intérêts des titulaires de droits[402]. Elle a cependant souligné qu'il ne s'agissait pas de faire primer de manière générale la protection des données sur la protection du droit d'auteur[403].

De l'avis du PFPDT, l'arrêt Logistep a été source d'insécurités. Si les procureurs ont considéré toute collecte d'adresses IP comme contraire à la loi et les preuves ainsi récoltées comme illicites, le PFPDT était d'avis que la collecte et le traitement de ces données personnelles continuaient d'être possibles après l'arrêt Logistep pour autant que certaines conditions soient respectées (par ex. la communication du dépôt d'une plainte pénale avant l'ouverture d'une action civile)[404].

A la lumière de l'arrêt Logistep du Tribunal fédéral, les cours suprêmes des cantons de Berne et de Zurich ont dû évaluer la possibilité d'utiliser des adresses IP collectées sur une base privée dans le cadre d'un procès. Alors que la Cour suprême du canton de Berne a rejeté leur

---

398 Art. 13 Cst., art. 43 et 46 LTC et art. 321ter CP; voir ATF 140 I 353 consid. 8.3 concernant la protection des données secondaires; pour cette notion, voir ch. 5.1.2 a).

399 Recommandation du 9.1.2008 du PFPDT : Bearbeitung und Weitergabe von elektronischen Datenspuren durch die Firma X im Auftrag von Urheberrechtsinhabern (en allemand), ch. 12.

400 ATF 136 II 508.

401 ATF 136 II 508, consid. 3.8.

402 ATF 136 II 508, consid. 6.3 s.

403 ATF 136 II 508, consid. 6.4.

404 Voir le 20^{e} rapport d'activités 2012/2013 du PFPDT, Echange de contenus sur Internet – situation juridique après l'arrêt Logistep.

utilisation[405], celle du canton de Zurich ne les a pas jugées manifestement inutilisables dans le cas concret et a annulé la décision de non-lieu du Ministère public[406]. Même après Logistep, l'utilisabilité des données sur les utilisateurs ne semble dès lors pas exclue, les circonstances du cas d'espèce étant déterminantes. Un tribunal de dernière instance doit toutefois encore trancher la question.

Compte tenu des insécurités décrites, la question se pose de savoir s'il existe un autre moyen d'obtenir les informations essentielles pour faire valoir des prétentions civiles.

c) Action en exécution d'une prestation en droit de la propriété intellectuelle

Les actions en exécution d'une prestation inscrites aux art. 62, al. 1, LDA, 55, al. 1, LPM et 35, al. 1, LDes mettent à la disposition de la personne qui subit une violation de son droit d'auteur, de son droit à la marque ou de son droit au design divers instruments pour dénoncer une telle infraction. Examinons ci-après si l'un de ces instruments prévoit un droit à l'information du titulaire de droits à l'égard du fournisseur ou si le législateur doit, comme il a été requis dans l'arrêt Logistep, prendre des mesures pour garantir une protection du droit d'auteur qui tienne compte de l'évolution technologique[407].

Les art. 62, al. 1, let. c, LDA, 55, al. 1, let. c, LPM et 35, al. 1, let. c, LDes prévoient dans une certaine mesure un droit à l'information. En vertu de ces dispositions, le défendeur est tenu d'indiquer la provenance et la quantité des objets confectionnés ou mis en circulation de manière illicite ou sur lesquels la marque ou l'indication de provenance ont été illicitement apposées et qui se trouvent en sa possession et de désigner les destinataires et la quantité des objets qui ont été remis à des acheteurs commerciaux. La question est de savoir si le lésé peut, sur la base de ces dispositions, exiger d'un fournisseur qu'il lui révèle des données sur son client. Ces dispositions ne présupposent apparemment pas une infraction de la partie saisie. Il suffit que le fournisseur participe à l'infraction de son client pour être tenu de fournir des renseignements[408].

Nous renvoyons à ce qui a été dit plus haut concernant la question de la légitimation passive des fournisseurs[409]. La question de savoir si les art. 62, al. 1, let. c, LDA, 55, al. 1, LPM et 35, al. 1, let. c, LDes s'appliquent aussi aux fournisseurs n’a pas encore été tranchée. La doctrine n'aborde ces dispositions généralement que de façon marginale, sans approfondir la réflexion sur les opérations en ligne.

Un auteur est d'avis que l'art. 62, al. 1, let. c, LDA ne s'applique qu'aux œuvres matérielles et non aux opérations immatérielles telles qu'elles ont lieu notamment sur Internet; selon elle, le champ d'application de cette disposition ne s'étend en particulier pas à la communication de l'identité de l'auteur de l'infraction obtenue par le biais de l'adresse IP[410]. Un autre avis de doctrine considère la formulation « objets […] qui se trouvent en sa possession » comme problématique. Les *fournisseurs d'accès* fournissent à leur client l'accès à la Toile. Ils transmettent des données à travers le réseau sans les sauvegarder sur leurs serveurs. Aussi les œuvres protégées par le droit d'auteur qui sont mises illicitement à la disposition d'autres

[405] Cour suprême du canton de Berne, décision de la Chambre de recours pénale du 22.3.2011, BK 11/9.
[406] Tribunal cantonal de Zurich, décision de la III^e Chambre pénale du 3.2.2014, UE130087-O/U/br.
[407] ATF 136 II 508, consid. 6.4.
[408] Voir *Frech*, 221.
[409] Ch. 3.2.5.
[410] *Beranek Zanon*, Jusletter IT du 11.12.2013, n^o 69.

utilisateurs par le biais d'Internet ne sont-elles jamais « en possession » des fournisseurs d'accès[411]. La situation est similaire en ce qui concerne les violations de droits de marque. Quant au *fournisseur d'hébergement*, il héberge certes, selon les circonstances, une plateforme sur laquelle ses clients placent des offres d'achat ou de vente. Mais ce sont les clients qui stockent les produits auxquels ils se réfèrent et non le fournisseur. Les objets ne se trouvent dès lors pas non plus « en sa possession »[412]. Un troisième avis de doctrine se prononce toutefois en faveur d'une interprétation large de la notion de « possession d'objets ». Les fournisseurs ne possédant en règle générale pas d'objets, le but que s'est fixé la loi de lutter contre le piratage perdrait son sens dans un domaine particulièrement touché par ce fléau. Il faudrait dès lors que la « possession d'objets » englobe aussi les données stockées sur un serveur lorsque des marchandises portant atteinte à un droit de marque sont proposées par le biais de ces données[413]. En droit d'auteur aussi, on considère qu'un intermédiaire peut être en possession d'une œuvre protégée par le droit d'auteur qui serait stockée dans une mémoire[414].

d) Droits à l'information selon l'art. 3 LCD (commerce électronique)

La LCD ne connaît pas de droit à l'information autonome, contrairement au droit de la propriété intellectuelle[415]. Cependant, les indications pertinentes pour une procédure civile peuvent être obtenues grâce aux obligations d'information prévues à l'art. 3, al. 1, let. s, ch. 1, LCD, lequel oblige toute personne qui propose des marchandises, des œuvres ou des prestations au moyen du commerce électronique à indiquer de manière claire et complète son identité, son adresse de contact et une adresse électronique valable. Si ces informations font défaut, l'offre est réputée déloyale. Cette prescription devrait englober, outre les sites Internet permettant de passer commande, d'autres plateformes et canaux de distribution électroniques. Elle pourrait ainsi s'appliquer à l'offre d'œuvres payantes sur les plateformes de téléchargement[416].

5.1.4 Droit de la protection des données

L'art. LPD prévoit un droit, pour tout un chacun, de savoir si des données personnelles le concernant sont traitées. Ce droit, appelé « droit d'accès », ne peut être exercé par une personne que pour ses données personnelles, à l'exclusion des données personnelles de tiers. Le débiteur du droit d'accès est le maître du fichier – c'est-à-dire celui qui décide du but et du contenu du fichier (art. 3, let. i, LPD) – voire, dans certains cas, le délégataire du traitement (art. 8, al. 1 et 4, LPD). Lorsque des données personnelles sont effectivement traitées, le maître du fichier doit les communiquer à la personne concernée. Il doit également lui communiquer leur origine, les catégories de destinataires ainsi que le but du traitement. Compte tenu de l'objet et des conditions d'exercice du droit d'accès, il paraît très peu probable qu'une personne puisse obtenir l'identité d'un tiers par ce biais.

411 Voir *Frech*, 222; *Wullschleger*, nº 277.
412 Voir *Frech*, 222.
413 *Staub*, Handkommentar MSchG, ad art. 55 nº 62.
414 *Wullschleger, nº 265 ss.*
415 *Spitz*, Handkommentar UWG, art. 9 nº 114.
416 *Kut/Stauber*, Jusletter du 20.2.2012, n° 58; *Weber/Wolf*, Jusletter du 18.6.2012, n° 32.

5.2 Jurisprudence de la Cour EDH

Dans certains cas de figure, l'État peut être tenu de mettre en place des instruments efficaces pour identifier les personnes responsables de publications illicites. C'est ainsi que, dans son arrêt K.U. contre Finlande, la Cour EDH a estimé que la législation finlandaise ne respectait pas l'art. 8 CEDH[417], car elle n'offrait aucun cadre légal pour obliger un fournisseur à communiquer à la police l'adresse IP d'un inconnu qui, sous une fausse identité, avait publié une annonce choquante au nom d'un enfant de douze ans sur un site de rencontres. La Cour a jugé insuffisant l'argument selon lequel le lésé aurait pu ouvrir une action en dommages-intérêts contre le fournisseur[418] et elle a balayé le renvoi au secret des télécommunications dès lors qu'il y avait soupçon d'infractions contre l'intégrité sexuelle d'enfants:

> « Même si la liberté d'expression et la confidentialité des communications sont des préoccupations primordiales et si les utilisateurs des télécommunications et des services Internet doivent avoir la garantie que leur intimité et leur liberté d'expression seront respectées, cette garantie ne peut être absolue, et elle doit parfois s'effacer devant d'autres impératifs légitimes tels que la défense de l'ordre et la prévention des infractions pénales ou la protection des droits et libertés d'autrui. »[419]

5.3 Droit étranger

5.3.1 Droits à l'information dans l'UE

a) Droit de l'Union

Le droit de l'Union ne prévoit pas de droits à l'information relevant du droit civil à l'égard des fournisseurs. Selon la CJUE[420], la directive vie privée et communications électroniques (2002/58/CE) n'interdit cependant pas de tels droits. À l'inverse, ni la directive sur le commerce électronique (2000/31/CE) ni la directive sur le droit d'auteur (2001/29/CE) ne contiennent de dispositions prévoyant un droit à l'information. Selon l'art. 8, al. 1, de la directive sur les droits de propriété intellectuelle (2004/48/CE), les États membres doivent certes veiller à ce que les autorités judiciaires compétentes puissent ordonner que des *informations* sur l'origine et les réseaux de distribution des marchandises ou des services qui portent atteinte à un droit de propriété intellectuelle soient fournies. Il faut cependant que les atteintes aient été perpétrées à l'échelle commerciale[421]. La CJUE estime toutefois que cette disposition, en relation avec l'art. 8, al. 3, de la directive sur les droits de propriété intellectuelle, ne doit pas être interprétée comme une obligation faite aux États membres de prévoir dans leur législation l'obligation de transmettre des données à caractère personnel dans le cadre de la procédure civile, dans le but de garantir une protection efficace du droit d'auteur[422].

La situation n'est pas claire quant à savoir si les privilèges des fournisseurs (selon les art. 12 à 14 de la directive sur le commerce électronique) s'appliqueraient aussi en matière de droits à l'information. Le libellé de la directive sur le commerce électronique n'apporte aucune réponse. La doctrine elle-même n'est a priori pas unanime sur la question, mais de nombreux

---

[417] Le droit au respect de la vie privée est garanti aussi par les art. 10 et 13 Cst.
[418] Cour EDH, 2.12.2008, n° 2872/02, K.U. c. Finlande, ch. 47; voir également ch. 1.3.2.
[419] Cour EDH, 2.12.2008, n° 2872/02, K.U. c. Finlande, ch. 49.
[420] Arrêt de la CJUE C-275/06 du 29.1.2008 (Promusicae c. Telefónica).
[421] Voir le libellé de l'art. 8, al. 1, et le considérant 14 de la directive sur les droits de propriété intellectuelle.
[422] Arrêt C-275/06 de la CJUE du 29.1.2008 (Promusicae c. Telefónica), ch. 58.

éléments concourent pour conclure que le droit à l'information *n'est pas* affecté par les privilèges au sens de la directive[423].

En d'autres termes, le droit de l'Union européenne laisse aux États membres le soin de décider s'ils veulent instituer dans leur droit interne un droit à l'information dans la procédure civile. Le cas échéant, la norme doit accorder suffisamment de poids aux droits fondamentaux, en particulier à la protection des données à caractère personnel et au respect de la vie privée. Elle doit également respecter le principe de proportionnalité. Un autre arrêt de la CJUE rendu en avril 2014 sur la question de la conservation des données à titre préventif[424] est important à cet égard car la Cour y conclut que la directive 2006/24/CE du 15 mars 2006 sur la conservation de données générées ou traitées dans le cadre de la fourniture de services de communications électroniques accessibles au public ou de réseaux publics de communications et modifiant la directive 2002/58/CE[425] est invalide. Selon cette directive, les fournisseurs, entre autres, auraient dû conserver les données de tous les usagers d'Internet pendant six mois et autoriser les enquêteurs à y accéder en cas de soupçon de délit grave. La Cour a motivé sa décision en arguant que, en l'espèce, la directive ne respectait pas le principe de proportionnalité parce qu'elle vise de manière généralisée les données de toutes les personnes, sans qu'aucune différenciation, limitation ni exception ne soient opérées en fonction de l'objectif de lutte contre les infractions graves. Simultanément, la Cour a aussi constaté que la conservation des données ne portait pas atteinte au contenu essentiel des droits fondamentaux au respect de la vie privée et à la protection des données à caractère personnel car les fournisseurs de services ou de réseaux doivent aussi respecter des principes en matière de protection et de sécurité des données. Elle a aussi constaté que la conservation des données dans le but de permettre aux autorités nationales compétentes de disposer d'un accès éventuel à celles-ci répondait à un objectif d'intérêt général[426].

Il s'ensuit donc que, dans l'UE, la conservation des données en soi n'est pas interdite. Elle répond même à un objectif d'intérêt général et peut donc porter atteinte à certains droits fondamentaux. Mais de ce fait, il est essentiel que la règlementation sur la conservation des données respecte le principe de proportionnalité. Pour que tel soit le cas, la CJUE a rappelé que les limitations de la protection des données à caractère personnel devaient s'opérer dans les limites du strict nécessaire, et que la portée et l'application des mesures devaient être régies par des règles claires et précises. Elle a en outre souligné que des garanties suffisantes devaient permettre de protéger efficacement les données à caractère personnel contre les risques d'abus et contre toute utilisation illicite. Si tous ces éléments sont pris en compte, rien ne s'oppose à la conservation des données sous l'angle du droit européen.

---

[423] Voir *Frech*, 188 ss. avec renvois au processus législatif et analyse de l'arrêt C-275/06 de la CJUE du 29.1.2008 dans l'affaire Promusicae c. Telefónica, dans lequel Frech relève que ni le juge ni le procureur général n'ont évoqué, de quelque façon que ce soit, les privilèges des fournisseurs. Ce qui l'amène à supposer que les juges étaient tellement loin de penser que le droit à l'information puisse dépendre des normes régissant les privilèges des fournisseurs qu'ils n'ont même pas pensé qu'une clarification judiciaire de cette question pourrait avoir un quelconque intérêt.

[424] Arrêts de la CJUE C-293/12 et C-594/12 du 8.4.2014 (Digital Rights Ireland et Seitlinger et al.).

[425] JO L 105 du 13.4.2006, 54.

[426] Arrêts C-293/12 et C-594/12 de la CJUE du 8.4.2014 (Digital Rights Ireland et Seitlinger et al.), ch. 38 ss.

b) Transposition dans les États membres

En Autriche, le § 18 de la *E-Commerce-Gesetz (ECG)*[427] prévoit une obligation d'informer plus étendue que la directive sur le commerce électronique, pour les fournisseurs d'hébergement. Selon l'al. 4 de cette disposition, le fournisseur d'hébergement doit, sur demande, fournir le nom et l'adresse de l'usager de ses services avec lequel il a conclu un contrat visant la conservation d'informations. Cette exigence lui est opposable par des tiers, pour autant que ceux-ci rendent vraisemblable un intérêt juridique prépondérant à la constatation de l'identité d'un usager et d'une atteinte illicite particulière. Ils doivent aussi rendre vraisemblable le fait que la connaissance de cette information constitue une condition essentielle de la poursuite judiciaire. S'il s'agit d'une atteinte au droit d'auteur, il faut également tenir compte du § 87*b*, al. 3, de la *Urheberrechtsgesetz*[428], selon lequel, dans certaines circonstances, des tiers peuvent également exiger d'autres informations que le nom et l'adresse de l'usager. Se fondant sur cette norme, le tribunal de commerce de Vienne a contraint un fournisseur d'accès à communiquer le nom et l'adresse des titulaires de certaines adresses IP à l'industrie musicale[429]. Dans un autre cas, la Cour suprême fédérale a appliqué le § 18, al. 4, ECG par analogie pour octroyer à un fournisseur de services téléphoniques à valeur ajoutée le droit d'obtenir des données relatives à un usager, et ce après que le fournisseur ait plusieurs fois intenté une action en prévention de l'atteinte – sans succès – contre la défenderesse, une entreprise de télécommunication mettant des numéros à valeur ajoutée à la disposition de tiers[430].

En Allemagne, le législateur a transposé l'art. 8 de la directive sur les droits de propriété intellectuelle dans le § 19 de la *Markengesetz (MarkenG)* et le § 101 de la *Urheberrechtsgesetz (UrhG)*. Ces dispositions contiennent une règlementation détaillée des droits à l'information pouvant être exercés dans le but de faire respecter d'autres droits. Si le renseignement souhaité concerne l'adresse IP d'une personne, une ordonnance judiciaire est requise préalablement pour attester de l'admissibilité de l'utilisation de l'adresse IP (§ 101, al. 9, UrhG et § 19, al. 9, MarkenG)[431]. Cette ordonnance est de la compétence exclusive de la Chambre civile du *Landgericht* du domicile, du siège ou de l'établissement de la personne qui doit fournir des renseignements.

5.3.2 Droits à l'information aux Etats-Unis

Dans le domaine du droit d'auteur, le *Digital Millennium Copyright Act*[432] a créé, avec le titre 17, § 512 (h), du *United States Code*, une procédure permettant au titulaire de droits d'auteur lésé d'exiger du *fournisseur d'hébergement*, par des moyens simples, qu'il livre les informations nécessaires à l'identification de l'auteur du dommage[433]. Pour introduire cette procédure, le titulaire de droits subissant une atteinte à ses droits n'a pas besoin d'intenter une action; il lui suffit de présenter les documents mentionnés au § 512 (h)(2). Le greffier délivre ensuite un document spécial, appelé « *subpoena* », au titulaire de droits, que celui-ci transmet au fournisseur. Ce dernier est dès lors tenu de communiquer au titulaire les données

[427] Voir ch. 3.3.1 d).
[428] Voir ch. 3.3.1 d).
[429] Arrêt du *Handelsgericht* de Vienne 18 Cg 67/05 du 21.6.2006.
[430] Arrêt de l'*Obergerichtshof* 4 Ob 7/04i du 16.3.2004.
[431] *Busch*, 776.
[432] Voir ch. 3.3.2.
[433] Voir *Frech*, 186 s.

personnelles du contrevenant. Le client du fournisseur concerné par le renseignement n'a aucune possibilité de s'opposer à la communication de ses données personnelles[434].

Selon la jurisprudence connue, le titre 17, § 512 (h), du *United States Code* n'est pas applicable à l'égard des *fournisseurs d'accès* du fait qu'ils ne sauvegardent pas sur leurs serveurs le matériel portant atteinte au droit d'auteur[435]. Dans ces cas, le titulaire des droits doit introduire une procédure complexe, puis intenter une action contre inconnu (« *John* ou *Jane Doe* »). Il doit ensuite présenter une demande dite d'« *expedited discovery* », qui ressemble à la procédure probatoire accélérée. Si elle est admise, le demandeur est autorisé à contacter le fournisseur par le biais d'une injonction (*subpoena*) de communiquer les données personnelles du client. Les dispositions de procédure prévoient la possibilité tant pour le fournisseur que pour le client concernés de contester la *subpoena*. Après avoir mis en rapport le droit à la liberté d'expression anonyme et l'intérêt d'appliquer la loi, le juge arrête s'il faut octroyer ou non le droit au demandeur de contraindre le fournisseur d'accès à communiquer des données personnelles[436]. Les dispositions du droit américain sur le privilège dont bénéficient les fournisseurs ne s'étendent pas à un éventuel droit à l'information à l'encontre des fournisseurs[437].

6 Droit de procédure

6.1 Cas purement nationaux

6.1.1 Compétence

La compétence à raison du lieu est régie par le CPC pour les cas purement nationaux. D'une manière générale, le for est celui du domicile ou du siège du défendeur (art. 10, al. 1, let. a et b, CPC), voire celui du lieu où il a son établissement (art. 12 CPC). Mais pour les actions en matière de protection de la personnalité et de protection des données, le tribunal du domicile ou du siège du demandeur est également compétent (art. 20 CPC). Lorsqu'il s'agit de statuer sur des actions fondées sur un acte illicite (y compris les actions en contrefaçon fondées sur le droit de la propriété intellectuelle et sur le droit de la concurrence)[438], l'art. 36 CPC offre quatre fors au choix: le domicile ou le siège de l'une des parties, le lieu de l'acte ou le lieu du résultat. Notons encore que l'art. 37 CPC, en tant que *lex specialis* de l'art. 36 CPC[439], prévoit un for spécifique pour les actions en dommages-intérêts consécutives à des mesures provisionnelles injustifiées.

Le tribunal compétent pour ordonner des mesures provisionnelles est impérativement celui qui est compétent pour statuer sur l'action principale ou celui du lieu où la mesure doit être exécutée (art. 13 CPC). La compétence matérielle et fonctionnelle des tribunaux est réglée dans le droit cantonal (art. 4, al. 1, CPC).

---

[434] Voir *Frech*, 162 s.

[435] Voir à ce sujet l'arrêt de référence du 19.12.2003 dans l'affaire Recording Industry Association of America c. Verizon Internet Services, United States Court of Appeals, District of Columbia Circuit, 351 F.3d 1129, 1233 : « *We conclude from both the terms of § 512(h) and the overall structure of § 512 that, as Verizon contends, a subpoena may be issued only to an ISP engaged in storing on its servers material that is infringing or the subject of infringing activity* ».

[436] Voir *Frech*, 168 ss. et 187.

[437] Voir *Frech*, 160 s.

[438] *Spühler/Dolge/Gehri*, n° 65.

[439] *Spühler/Dolge/Gehri*, n° 68.

6.1.2 Mesures provisionnelles

Dans le cadre des actions défensives, la première intervention que l'on sollicite est généralement l'adoption de mesures provisionnelles[440], qui sont centrales en cas d'atteinte à la personnalité sur Internet[441]. Il est possible d'ordonner de telles mesures lorsque le requérant rend vraisemblable qu'une atteinte est réellement imminente ou qu'elle est déjà effective, et que celle-ci risque de lui causer un préjudice difficilement réparable (art. 261, al. 1, CPC). Le tribunal peut ordonner toute mesure provisionnelle propre à prévenir ou à faire cesser le préjudice (art. 262 CPC). En cas d'urgence particulière, il peut ordonner des mesures provisionnelles immédiatement, sans entendre la partie adverse (mesures dites « superprovisionnelles », art. 265, al. 1, CPC). Les mesures provisionnelles – comme pour toute action en prévention de l'atteinte[442] – peuvent être assorties de la menace d'une amende en cas d'insoumission à la décision de l'autorité (art. 292 CP)[443].

Pour éviter une « censure privée »[444] des médias à caractère périodique, qui n'est fondamentalement pas souhaitable, l'art. 266 CPC contient une disposition particulière concernant les mesures provisionnelles à leur égard. Ainsi, des mesures provisionnelles ne peuvent être ordonnées contre ce type de médias que si:

> « a. l'atteinte est imminente et propre à causer un préjudice particulièrement grave;
>
> b. l'atteinte n'est manifestement pas justifiée;
>
> c. la mesure ne paraît pas disproportionnée. »

A priori, ni la jurisprudence ni la doctrine ne se sont encore penchées sur les particularités des mesures provisionnelles prises à l'égard des fournisseurs. Vu l'importance que revêt Internet pour la diversité d'opinion et le risque de censure privée dans ce domaine, il est cependant concevable que la règle particulière de l'art. 266 CPC puisse aussi être appliquée à certains types de fournisseurs qui sont comparables à des médias à caractère périodique[445].

6.1.3 Frais de procédure

La doctrine a critiqué l'arrêt Tribune de Genève[446] pour avoir maintenu la décision du tribunal de première instance de condamner l'hébergeur du blog au paiement d'un quart des frais sans lui avoir donné (a priori) d'avertissement préalable ni lui avoir permis de satisfaire de son plein gré à la demande formée contre elle[447]. Il faut cependant relever que la Tribune de Genève avait conclu principalement à ce que la demande de mesures provisionnelles soit déclarée irrecevable et, subsidiairement, à ce qu'elle soit rejetée. Elle avait aussi indiqué n'avoir aucune objection à supprimer le contenu d'un blog *sur ordre de la justice*[448]. Il n'est donc pas possible

---

[440] Voir notamment l'arrêt Tribune de Genève, ch. 3.2.2 c), et l'affaire Basler Facebook présentée dans *Schneider-Marfels*, Jusletter du 20.2.2012.
[441] Par ex. *Cramer*, recht 2007, 128.
[442] Voir ch. 3.2.6 a).
[443] Voir BSK ZPO-*Sprecher*, ad art. 262 n° 15.
[444] Par ex. *Hausheer/Aebi-Müller*, n° 14.88.
[445] Voir BSK ZPO-*Sprecher*, ad art. 266 n° 18 s. ; voir également ch. 3.2.2 a) au sujet du droit de réponse.
[446] Voir ch. 3.2.2 c).
[447] Voir *Rosenthal*, La pratique de l'avocat 2013, 728 ; *Schoch/Schüepp*, Jusletter du 13.5.2012, n° 36.
[448] Arrêt du Tribunal fédéral 5A_792/2011 du 14.1.2013, exposé des faits: C.

de savoir si elle aurait effectivement accédé à la demande de son plein gré après un avertissement. Le fait est qu'elle ne l'a justement pas fait après l'ouverture de la procédure.

En vertu de l'art. 106, al. 1, CPC, les frais sont en principe mis à la charge de la partie qui succombe. Les frais se composent des frais judiciaires et des dépens, et sont fixés conformément aux tarifs cantonaux (art. 105 et 96 CPC). Lorsque plusieurs personnes participent au procès en tant que parties principales ou accessoires, le tribunal détermine la part de chacune au frais du procès et il peut les tenir pour solidairement responsables (art. 106, al. 3, CPC). Avant l'introduction du CPC, plusieurs codes de procédure cantonaux contenaient des dispositions selon lesquelles les frais devaient être mis à la charge du demandeur lorsque la demande n'avait pas été provoquée par l'attitude du défendeur et que celui-ci en reconnaissait immédiatement le bien-fondé[449]. Le législateur fédéral a cependant renoncé à introduire cette règle dans le CPC. À la suite des critiques reçues dans le cadre de la procédure de consultation, il a également décidé de ne pas reprendre une autre règle appliquée dans de nombreux cantons, selon laquelle les frais devaient être supportés par la partie dont le gain n'était pas nettement supérieur à une offre de transaction qui lui avait été faite[450]. En vertu de l'art. 107 CPC, le tribunal peut s'écarter des règles générales énoncées à l'art. 106 CPC et répartir les frais selon sa libre appréciation lorsqu'une partie a intenté le procès de bonne foi (let. b), lorsque la procédure est devenue sans objet et que la loi n'en dispose pas autrement (let. e) ou lorsque des circonstances particulières rendent la répartition en fonction du sort de la cause inéquitable (let. f).

La question se pose donc de savoir si le défendeur qui reconnaît le bien-fondé d'une action défensive, immédiatement et sans réserve, peut être exempté des frais en vertu de l'art. 107, let. b, e ou f, CPC et si ceux-ci peuvent être mis à la charge du demandeur qui a eu gain de cause. Tel pourrait être le cas, par exemple, lorsque le demandeur omet de donner l'occasion au défendeur de satisfaire à sa demande de son plein gré avant l'introduction de la demande. Plusieurs auteurs de doctrine estiment que le défendeur devrait aussi pouvoir invoquer l'art. 107, al. 1, let. b, CPC[451]. Selon l'un des exemples cités, les frais devraient être supportés par le demandeur lorsque la demande a été admise pour des motifs que le défendeur ne pouvait connaître au préalable[452]. L'acquiescement aux conclusions de la demande conduit à la radiation de l'affaire du rôle, la procédure étant dès lors sans objet (art. 241 CPC). Dans cette situation, le tribunal est expressément tenu de répartir les frais selon sa libre appréciation (art. 107, al. 1, let. e, CPC). La doctrine propose aussi des exemples allant en ce sens pour la let. f: les auteurs estiment que cette disposition devrait aussi s'appliquer lorsque quelqu'un ouvre une action à l'échéance d'une créance, sans délai et sans mise en demeure, et que le défendeur acquiesce immédiatement à la demande[453], ou lorsque la partie qui obtient gain de cause avait refusé une offre de transaction raisonnable et n'a pas obtenu un gain nettement supérieur à la fin de la procédure[454]. Enfin, lorsque les parties transigent en justice, elles supportent les frais conformément à la transaction (art. 109, al. 1, CPC). Dans les rares cas

[449] Voir l'ancien art. 60 du code de procédure civile du Canton de Berne et l'ancien art. 59 du code de procédure civile de la République et Canton du Jura.
[450] Message CPC (note 396), FF 2006 6909.
[451] *Jenny*, Kommentar ZPO, ad art. 107 n° 9 ; CPC-*Tappy*, ad art. 107 n° 17.
[452] CPC-*Tappy*, ad art. 107 n° 17.
[453] *Staehelin/Staehelin/Grolimund*, 253.
[454] CPC-*Tappy*, ad art. 107, n° 30. Dans ce cas, une certaine réserve est toutefois de mise, car cette règle avait été abandonnée durant le processus législatif, en raison des fortes critiques qu'elle avait suscitées, message CPC (FF 2006 6909; voir également note 396).

où la transaction ne règle pas la répartition des frais, le tribunal peut également appliquer l'art. 107 CPC (art. 109, al. 2, let. a, CPC).

En conclusion, le fournisseur qui n'avait pas connaissance des contenus illicites et qui les a supprimés sans délai dès qu'il a été informé de leur existence peut, au regard du droit de procédure suisse, être exonéré des frais d'une procédure ouverte hâtivement.

6.2 Cas présentant un caractère international

6.2.1 Remarque liminaire

Les affaires en relation avec l'utilisation d'Internet sont souvent de nature internationale. Par exemple, la plupart des exploitants de plateformes ont leur siège à l'étranger[455]. Dans ce contexte, les règles du droit international privé en matière de compétence, de droit applicable ainsi que de reconnaissance et d'exécution des décisions sont centrales.

6.2.2 Compétence

a) Selon la Convention de Lugano

La Convention du 30 octobre 2007 concernant la compétence judiciaire, la reconnaissance et l'exécution des décisions en matière civile et commerciale (Convention de Lugano, CL)[456] s'applique dès lors que le *défendeur* a son domicile ou son siège dans l'un des États couverts par le traité, à savoir l'UE et l'AELE (exception faite du Liechtenstein). L'existence d'un domicile dans l'un des États liés par la convention se détermine au regard du droit interne de cet État (art. 59 CL). Les sociétés et les personnes morales sont domiciliées là où se situe leur siège statutaire, leur administration centrale ou leur principal établissement (art. 60, al. 1, CL). En Suisse, conformément à la jurisprudence Owusu de la CJUE[457] qui a été reprise par le Tribunal fédéral[458], la CL s'applique aussi lorsque le domicile ou le siège du défendeur se trouve dans le pays et qu'il n'y a aucun autre lien avec un autre État lié par la convention.

Dans le régime de la CL, le domicile ou le siège du défendeur est également le *for ordinaire* (art. 2 CL). Le droit interne de l'État concerné reste cependant déterminant pour les questions de compétence à raison du lieu. En Suisse, cet aspect est réglé dans la loi fédérale du 18 décembre 1987 sur le droit international privé (LDIP)[459]. Si le défendeur a agi par l'une de ses succursales, il peut être attrait au lieu où se situe celle-ci (art. 5, ch. 5, CL). La convention offre des fors alternatifs.

L'un de ces fors alternatifs s'applique justement aux *prétentions fondées sur un acte illicite* auxquelles nous nous intéressons. Selon l'art. 5, ch. 3, CL, en matière délictuelle, une personne peut être attraite « devant le tribunal du lieu où le fait dommageable s'est produit » pour autant que ce lieu soit situé dans un autre État lié par la convention. Selon la jurisprudence constante de la CJUE (à laquelle le Tribunal fédéral, s'agissant de la CL, s'est rallié[460]), il est ici question de deux fors alternatifs, l'un au lieu de l'acte (« lieu de l'événement

[455] Voir le rapport du Conseil fédéral « Cadre juridique pour les médias sociaux » (note 1), 10.
[456] RS 0.275.12.
[457] Arrêt de la CJUE C-281/02 du 1.3.2005.
[458] ATF 135 III 185, consid. 3.3.
[459] RS 291; voir également ch. 6.2.2 b.
[460] ATF 132 III 778, consid. 3.

causal ») et l'un au lieu du du résultat (« lieu où le dommage est survenu »), les deux pouvant coïncider dans les faits. Si le dommage survient simultanément dans plusieurs États liés par la convention, la compétence de chaque tribunal est limitée aux dommages causés localement (solution dite « mosaïque »)[461].

Lorsque la procédure concerne une atteinte aux *droits de la personnalité* par la publication de contenus sur Internet, la CJUE situe le *lieu de l'acte* là où se trouve l'établissement de l'auteur des contenus illicites et le lieu, ou plutôt les *lieux du résultat* partout où les contenus en question étaient accessibles. Elle envisage aussi un lieu du résultat à l'endroit où le lésé a le centre de ses intérêts. Ce for-là est valable pour l'intégralité du dommage subi (arrêt eDate Advertising GmbH et Martinez)[462].

Dans son arrêt Wintersteiger AG[463], la CJUE a déterminé de la même manière le lieu où s'est produit l'acte conduisant à une *atteinte à une marque* commise à travers Internet. Elle a arrêté que le lieu du résultat était celui où la marque prétendument violée est enregistrée. Dans la doctrine également, il est considéré qu'en droit de la propriété intellectuelle, le lieu où se matérialise le dommage ne peut se trouver que dans l'Etat où le titre concerné est enregistré.[464] En effet, les droits de propriété intellectuelle n'étant protégés qu'au lieu où ils ont été enregistrés, ils ne peuvent dès lors être violés qu'en ce même lieu[465].

L'arrêt Wintersteiger AG ne peut être transposé que de manière très limitée dans les cas d'atteinte aux *droits d'auteur*, dont la protection naît de plein droit au moment de la création de l'œuvre, sans inscription aucune dans un registre. La Convention de Berne du 24 juillet 1971 pour la protection des œuvres littéraires et artistiques[466], valable dans toute l'Europe et à une échelle quasi mondiale, garantit une protection internationale des droits d'auteur, même si elle ne définit que des *normes minimales* concernant les différents droits et que, au demeurant, leur contenu se juge selon le droit national. Dans ses arrêts Pinckney[467] et Hejduk[468], la CJUE a dès lors conclu que dans le cas de violations de droits d'auteur sur Internet, c'est la solution mosaïque qui s'applique pour déterminer le lieu du résultat. Elle a laissé provisoirement ouverte la question de savoir s'il existe aussi, à l'instar des cas d'atteinte à la personnalité sur Internet, un lieu du dommage central au lieu où se situe le centre des intérêts de la personne lésée. Elle a en revanche confirmé la détermination du lieu de l'acte donnée dans l'arrêt Wintersteiger AG dans la motivation de la décision Hejduk.

La jurisprudence n'a pas encore apporté de réponse à la question de savoir dans quelle mesure la pratique exposée en matière d'atteintes à la personnalité s'applique aussi aux actes relevant du *droit de la concurrence* ni dans quelle mesure le lieu du résultat, dans ce domaine, se détermine en application du principe des effets, dit aussi de territorialité objective (qui prend pour point de rattachement le marché sur lequel le comportement déloyal déploie ses effets)[469]. La notion de lieu du résultat unique à l'endroit où se trouve le centre des intérêts du lésé, que la CJUE a introduite avec l'arrêt eDate Advertising GmbH et Martinez, vise très

[461] Arrêt de la CJUE C-68/93 du 7.3.1995 (Shevill).
[462] Pour plus de détail, voir l'arrêt de la CJUE C-509/09 et C-161/10 du 25.10.2011 (eDate Advertising GmbH et Martinez).
[463] Arrêt de la CJUE C-523/10 du 19.4.2012.
[464] Voir notamment BSK LugÜ-*Hofmann/Kunz*, ad art. 5 nº 607.
[465] Concernant les violations de brevets, le Tribunal fédéral va dans ce sens dans son ATF 132 III 778 consid. 3.
[466] RS 0.231.15.
[467] Arrêt de la CJUE C-170/12 du 3 octobre 2013.
[468] Arrêt de la CJUE C-441/13 du 22 janvier 2015.
[469] Voir BSK LugÜ-*Hofmann/Kunz*, ad art. 5 n° 598, et *Schnyder*, LugÜ Kommentar, ad art. 5 n° 405.

spécifiquement les atteintes à la personnalité et ne peut vraisemblablement pas être transposée aux cas de concurrence déloyale. S'agissant des autres lieux du résultat, un examen plus approfondi montre qu'il n'y a pas de contradiction, a priori, avec le principe des effets. Du fait de l'application de la solution mosaïque dans ce domaine, on considère qu'à chaque endroit où le contenu illicite peut être consulté, un dommage est survenu localement. Par transposition de la jurisprudence eDate Advertising GmbH et Martinez au domaine de la concurrence déloyale, il faut donc aussi qu'au final, le contenu visé ait eu un effet local sur la concurrence à tous les endroits où il a été diffusé.

L'arrêt eDate Advertising GmbH et Martinez concernait deux fournisseurs de contenus. Ni la CJUE ni le Tribunal fédéral ne se sont encore exprimés sur la responsabilité des fournisseurs d'hébergement et des fournisseurs d'accès ou sur celle des exploitants de plateformes, en cas de diffusion de contenus illicites par des utilisateurs d'Internet (ou par des fournisseurs de contenus). De la jurisprudence actuelle de la CJUE, il ressort uniquement que pour déterminer le lieu de l'acte d'un complice, il faut se baser exclusivement sur sa contribution à l'infraction[470]. Il faut donc partir de l'idée que le lieu de l'acte sera, pour chaque fournisseur ou exploitant de plateforme, le sien propre. Dans ce contexte, il s'impose de recourir aussi pour ce dernier au rattachement au lieu d'établissement, puisque c'est là qu'il exerce en principe son activité[471]. S'agissant du lieu du résultat, celui-ci étant le même pour tous les acteurs que pour l'auteur principal, il faut appliquer les mêmes règles que dans le cas des actions contre des utilisateurs d'Internet[472].

Lorsque l'action est introduite au domicile de l'utilisateur fautif, une autre procédure peut être ouverte au même endroit à l'encontre du fournisseur ou de l'exploitant de plateforme à qui il est reproché d'avoir concouru à l'acte illicite (art. 6, ch. 1, CL).

b) Selon la loi fédérale sur le droit international privé

La règle de base de la LDIP, énoncée à l'art. 129, est la même que celle de la CL: une *action fondée sur un acte illicite* peut être introduite aussi bien au lieu du domicile du défendeur qu'au lieu de l'acte ou du résultat. Toutefois, le for du domicile prévu par la LDIP est sans importance pour la question de la compétence internationale du fait que, si le défendeur a son domicile en Suisse, c'est la CL qui s'applique. L'art. 129 LDIP prévoit aussi un for au lieu de résidence habituelle du défendeur si celui-ci n'a pas de domicile en Suisse et – encore une fois comme la CL – un for au lieu de l'établissement pour les actions relatives à l'activité de ce dernier. Une disposition analogue règle la situation en cas de violation de droits de propriété intellectuelle (art. 109, al. 2, LDIP).

Dans son interprétation de la notion de *lieu de l'acte*, le Tribunal fédéral s'appuie sur la jurisprudence de la CJUE[473]. Il est donc fort probable qu'il fera de même lorsqu'il s'agira d'interpréter la notion de *lieu du résultat*[474]. La doctrine y serait favorable, alors qu'elle est opposée à une reprise de la solution mosaïque décrite par la CJUE[475], ce qui est tout à fait

[470] Arrêt de la CJUE C-228/11 du 16.5.2013 (Melzer), confirmé par l'arrêt C-387/12 du 3.4.2014 (Hi Hotel).
[471] Voir *Kernen*, n° 453 ss.
[472] Voir *Neumann*, 496 s. et 504.
[473] ATF 131 III 153, consid. 6.2.
[474] Voir *Kernen*, n° 553.
[475] BSK IPRG-*Umbricht/Rodriguez/Krüsi*, ad art. 129 n° 16 et 27, avec d'autres références; du même avis, *Bonomi*, CR LDIP, ad art. 129 n° 27, et *Kernen*, n° 275, 608 ss. et 641.

défendable au vu du libellé actuel de la loi. Il devrait donc s'ensuivre qu'en cas d'atteintes à la personnalité par le biais d'Internet, il n'y ait qu'un seul lieu du résultat, à savoir le lieu de résidence habituelle du lésé (par analogie au centre des intérêts au sens de la jurisprudence de la CJUE)[476].

Si l'utilisateur fautif est attrait à l'un de ces endroits, le for choisi pourra aussi être utilisé pour une éventuelle action additionnelle contre le fournisseur ou contre l'exploitant de la plateforme, pour autant que ce dernier puisse aussi être poursuivi en Suisse, en application des règles exposées précédemment (art. 8*a*, al. 1, LDIP).

L'art. 130, al. 3, LDIP prévoit un for alternatif supplémentaire pour *l'action en exécution du droit d'accès* (art. 8 LPD). Cette dernière peut être introduite non seulement devant les tribunaux désignés à l'art. 129, al. 1, LDIP, mais aussi devant les tribunaux suisses du lieu où le fichier est géré ou utilisé. Il peut s'agir de la gestion et de l'utilisation comme telles, mais aussi de la collecte, de la conservation ou de la destruction des données[477]. La simple possibilité d'accès par un tiers, au moyen d'Internet par exemple, ne suffit pas[478].

c) Mesures provisionnelles

Les divers fors mentionnés dans les paragraphes précédents sont aussi valables pour les mesures provisionnelles. Si ces mesures doivent être exécutées en Suisse, l'art. 10 LDIP – qui s'applique également sous le régime de la CL (art. 31 CL) – prévoit une compétence supplémentaire pour les tribunaux du lieu de l'exécution. En règle générale, ce lieu correspond toutefois au domicile du défendeur, où un for peut de toute façon être constitué en vertu de l'art. 2 CL et de l'art. 129 LDIP.

6.2.3 Droit applicable

a) Selon la loi fédérale sur le droit international privé

Lorsqu'un dommage est survenu, les parties peuvent convenir à tout moment de l'application du droit du for, autrement dit du droit suisse lorsque l'action est introduite en Suisse (art. 132 LDIP). À défaut d'un tel accord, la règle applicable est la suivante: lorsque l'auteur et le lésé ont leur résidence habituelle dans le même État, les prétentions fondées sur un acte illicite sont régies par le droit de cet État (art. 133, al. 1, LDIP). Sinon, le droit en vigueur au lieu du résultat est applicable si l'auteur devait prévoir que le résultat s'y produirait. Dans tous les autres cas, c'est le droit en vigueur au lieu de l'acte qui s'applique (art. 133, al. 2, LDIP). Lorsqu'un dommage découle de la publication de certains contenus sur Internet, on peut admettre que la consultation des contenus en question dans le monde entier était pour le moins prévisible. Cela ne veut cependant pas encore dire que lesdits contenus sont de nature à engendrer un dommage dans tous les États où ils sont consultés. La prévisibilité du dommage doit donc être évaluée pour chaque État selon les circonstances du cas d'espèce[479].

La portée matérielle de la loi applicable ainsi définie découle de l'art. 142 LDIP. Selon cette disposition, la loi applicable détermine notamment « les conditions et l'étendue de la

[476] Voir BSK IPRG-*Umbricht/Rodriguez/Krüsi*, ad art. 129 n° 29, et ZK IRPG-*Heini*, ad art. 133 n° 10a.
[477] *Meier*, n° 1854.
[478] *Meier*, n° 1854 ; *Rosenthal*, in : Rosenthal/Jöhri, ad art. 15 LPD n° 73, qui cite l'avis contraire de ZK IRPG-*Volken*, ad art. 130 n° 30.
[479] Voir *Bonomi*, CR LDIP, ad art. 139, n° 7, et BSK IPRG-*Dasser*, ad art. 139 n° 17.

responsabilité, ainsi que la personne du responsable », ce qui inclut aussi la question de la responsabilité des co-auteurs et des complices[480]. Si elle pose comme condition l'illicéité de l'acte, l'appréciation doit tenir compte des règles de comportement valables au lieu de l'acte (art. 142, al. 2, LDIP). La portée exacte de cette disposition paraît floue, mais comme nous le montrerons par la suite, cet aspect ne pèse pas très lourd dans le contexte qui nous intéresse.

Des règles particulières s'appliquent pour les prétentions fondées sur une atteinte à la personnalité *par les médias ou tout autre moyen public d'information* (dont l'Internet fait également partie selon plusieurs avis de doctrine)[481]. Conformément à l'art. 139, al. 1, LDIP, le lésé peut choisir entre:

> « a. [le] droit de l'État dans lequel [il] a sa résidence habituelle, pour autant que l'auteur du dommage ait dû s'attendre à ce que le résultat se produise dans cet État;
>
> b. [le] droit de l'État dans lequel l'auteur de l'atteinte a son établissement ou sa résidence habituelle; ou
>
> c. [le] droit de l'État dans lequel le résultat de l'atteinte se produit, pour autant que l'auteur du dommage ait dû s'attendre à ce que le résultat se produise dans cet État. »

L'art. 139, al. 3, LDIP prévoit que l'art. 139, al. 1, LDIP s'applique aussi aux atteintes à la personnalité résultant du *traitement de données personnelles* ainsi qu'aux entraves mises à l'exercice du droit d'accès aux données personnelles. L'analogie est peu adaptée à l'action en exécution du droit d'accès, dans la mesure où l'on ne peut dans ce cas véritablement parler d'« auteur », et où il n'y a pas d'atteinte illicite comparable à celle commise par un média. La doctrine propose de comprendre « maître du fichier » lorsque la loi parle d'« auteur » et « lieu où le fichier est utilisé ou géré » lorsque la loi parle de « lieu du résultat » de l'atteinte. Les auteurs proposent, pour les mêmes raisons, de renoncer pour cette action à l'exigence de la prévisibilité posée à l'art. 139, al. 1, let. a et c, LDIP[482].

Les critères de rattachement mentionnés à l'art. 139, al. 1, LDIP correspondent largement à ceux définis par la CJUE en matière de compétence (le lieu de résidence habituelle du lésé [let. a] étant la plupart du temps le lieu où se trouve le centre de ses intérêts). S'il y a plusieurs lieux du résultat au sens de la let. c, le droit applicable dans chaque État concerné doit être déterminé séparément[483]. Ce point de vue n'est cependant pas unanime[484].

Les auteurs cités estiment que la loi applicable est également déterminante pour établir s'il y a atteinte à la personnalité. L'art. 142, al. 2, LDIP examiné précédemment ne joue donc aucun rôle ici.

Des règles particulières s'appliquent aussi en cas de *concurrence déloyale*. C'est le droit de l'État sur le marché duquel le résultat s'est produit qui régit les prétentions (art. 136, al. 1, LDIP). Pour les infractions dirigées contre l'entreprise elle-même et qui n'ont pas d'effets publics, le droit applicable est celui du siège de l'établissement lésé (art. 136, al. 2, LDIP)[485]. En vertu de l'art. 136, al. 3, LDIP, l'application de l'art. 133, al. 3, LDIP est réservée en cas de violation d'un rapport juridique préexistant entre l'auteur et le lésé. La loi applicable règle ici

---

480 BSK IPRG-*Umbricht/Rodriguez/Krüsi*, ad art. 142 n° 8.
481 Voir BSK IPRG-*Dasser*, ad art. 139, n° 8, et *Reymond*, n° 650 avec d'autres références.
482 *Meier*, n° 1860 ss. avec d'autres références.
483 BSK IPRG-*Dasser*, ad art. 139 n° 18 ss. avec d'autres références ; *Bonomi*, CR LDIP, ad art. 139 n° 8.
484 Voir renvois dans BSK IPRG-*Dasser*, ad art. 139 n° 18, et *Reymond*, n° 653.
485 BSK IPRG-*Dasser*, ad art. 136 n° 18.

aussi la question de l'illicéité dans le cas d'espèce. L'art. 142, al. 2, LDIP ne joue aucun rôle dans ce cas[486].

S'agissant de la *violation* de *droits de propriété intellectuelle*, c'est l'art. 110 LDIP qui s'applique. Celui-ci renvoie au droit de l'Etat pour lequel la protection de la propriété intellectuelle est revendiquée. En d'autres mots, le droit de l'Etat qui accorde au demandeur le droit prétendument violé est déterminant. Cette règle se fonde sur le principe de la limitation territoriale des droits de propriété intellectuelle. En général, un titre de propriété intellectuelle n'est protégé que dans l'Etat dans lequel il est enregistré. Le demandeur doit dès lors invoquer la violation d'un droit de propriété intellectuelle protégé dans un Etat déterminé. L'atteinte ou non à ce droit sera appréciée au regard de l'ordre juridique de cet Etat, ce qui présuppose, entre autres, que l'acte de violation présente, aux termes de la législation de cet Etat, un lien territorial pertinent avec ce dernier[487]. Tout cela vaut également pour les *droits d'auteur*. Quand bien même ils ne naissent pas par le biais d'un enregistrement, mais automatiquement avec la création de l'œuvre, puis sont protégés dans tous les Etats membres de la Convention de Berne pour la protection des œuvres littéraires et artistiques (toute l'Europe et une grande partie du monde) dans la mesure où l'œuvre concernée peut être attribuée à l'un de ces Etats selon les règles de la Convention. Dans ce cas également, l'aménagement concret de la protection et son champ d'application territorial sont définis en fonction de l'ordre juridique de l'Etat concerné[488]. La Convention de Berne garantit néanmoins une étendue minimale de la protection.

b) Digression: droit applicable selon le droit de l'UE

Dans une optique de droit comparé, nous faisons ici un bref état des lieux des règles applicables en droit européen (et qui ne lient pas les tribunaux suisses). La responsabilité délictuelle y est régie par le règlement (CE) n° 864/2007 du Parlement européen et du Conseil du 11 juillet 2007 sur la loi applicable aux obligations non contractuelles (« Rome II »), qui exclut toutefois de son champ d'application les atteintes aux droits de la personnalité (art. 1, al. 2, let. g). En matière de concurrence déloyale et d'atteinte aux droits de propriété intellectuelle, le règlement suit les mêmes principes fondamentaux que la LDIP, à savoir le principe des effets et le principe du pays de protection (art. 6 et 8 du règlement).

c) Droit applicable en matière de mesures provisionnelles

Lorsqu'il ordonne des mesures provisionnelles, un tribunal suisse reste lié par les art. 261 ss. CPC même s'il s'agit d'une affaire internationale[489]. L'existence d'une atteinte au sens de l'art. 261, al. 1, let. a, CPC, se détermine au regard du droit applicable en vertu de la LDIP.

6.2.4 Notification d'actes judiciaires au défendeur à l'étranger

Pour qu'une ordonnance ou une décision judiciaire puisse déployer ses effets à l'égard d'un défendeur situé à l'étranger, elle doit lui être dûment notifiée. En principe, lorsque les tribunaux civils suisses veulent notifier des actes à l'étranger, ils doivent recourir à l'*entraide judiciaire*.

---

[486] BSK IPRG-*Umbricht/Rodriguez/Krüsi*, ad art. 142 n° 18, et ZK IRPG-*Heini*, ad art. 142 n° 22.
[487] Sur l'ensemble de la question, voir BSK IPRG-*Jegher/Vasella*, ad art. 110 n° 25.
[488] L'art. 5 de la Convention de Berne va également dans ce sens (voir à ce sujet *Neumann*, 95 ss).
[489] Voir ch. 6.1.2.

Dans les relations avec pratiquement tous les pays européens, mais aussi avec de nombreux autres États comme les États-Unis, le Canada, la Chine, l'Inde, la Corée du Sud et Israël, la Suisse applique la Convention de la Haye du 15 novembre 1965 relative à la signification et la notification à l'étranger des actes judiciaires et extrajudiciaires en matière civile ou commerciale[490]. La voie ordinaire prévue par cette convention est la transmission des actes à notifier à une autorité centrale désignée par l'État de destination. La Suisse a émis une réserve au sujet de certaines voies de transmission alternatives, en particulier la transmission directe des actes par voie postale à destination de la Suisse. Par conséquent, la *transmission directe par voie postale* de la Suisse à l'étranger ou par le biais de la représentation suisse dans l'État de destination n'est possible que si cet État admet ce mode de transmission et qu'il renonce simultanément à la réciprocité. Cette condition est remplie avec quelques pays européens (dont l'Irlande) et, entre autres, avec les États-Unis, le Canada, le Japon, l'Inde et Israël[491]. Le Conseil fédéral a par ailleurs adopté, début 2014, un mandat pour l'ouverture de négociations avec l'UE, l'Irlande, la Norvège et le Danemark en vue de définir une règlementation commune dans le domaine de l'entraide judiciaire internationale en matière civile (signification et notification, production des preuves). Sur le fond, l'idée est de s'aligner sur les instruments communautaires en la matière, en particulier le règlement européen sur la signification et la notification des actes[492], qui prévoit aussi la transmission directe par voie postale. Il faut être conscient qu'une notification par la voie ordinaire de l'entraide judiciaire peut prendre plusieurs mois.

6.2.5 Mise en œuvre à l'étranger: reconnaissance et exécution des décisions

Les jugements suisses rendus en matière de responsabilité délictuelle doivent en principe être reconnus dans les autres États liés par la CL. Lorsqu'une décision suisse doit être exécutée hors de l'espace UE/AELE (notamment parce que le fournisseur y a son siège), la reconnaissance est normalement régie par le droit interne de l'État concerné. S'il faut s'attendre à des difficultés, le lésé est contraint d'introduire une nouvelle demande dans l'État en question ou d'y poursuivre le fournisseur dès le début. Le droit applicable en matière de responsabilité du fournisseur dans le cas d'espèce sera alors déterminé par le droit interne de cet État. À cause de la nécessité de faire exécuter la décision à l'étranger, force est de constater que l'élimination de contenus illicites peut parfois engendrer de grandes difficultés pratiques et des retards[493].

Dans les États liés par la CL, le lésé peut adresser directement à l'autorité d'exécution de l'État concerné un jugement émis en Suisse. Il n'y a pas besoin de procédure supplémentaire pour obtenir une déclaration de force obligatoire[494]. Tel n'est pas toujours le cas avec les autres pays. Les dispositions de la CL relatives à la reconnaissance et à l'exécution sont aussi

---

[490] RS 0.274.131.

[491] Voir les lignes directrices « Entraide judiciaire internationale en matière civile » de l'OFJ et les aide-mémoire complémentaires en matière de notification sur www.rhf.admin.ch/rhf/fr/home/zivil/wegleitungen.html, et plus particulièrement l'index des pays à l'adresse www.rhf.admin.ch/rhf/fr/home/rhf/index/laenderindex.html.

[492] Règlement (CE) n° 1393/2007 du Parlement européen et du Conseil du 13.11.2007 relatif à la signification et à la notification dans les États membres des actes judiciaires et extrajudiciaires en matière civile ou commerciale (signification ou notification des actes), et abrogeant le règlement (CE) n° 1348/2000 du Conseil.

[493] Voir l'article de *Schneider-Marfels*, Jusletter du 20.2.2012, sur l'ordonnance de mesures superprovisionnelles à l'encontre de Facebook.

[494] Voir art. 33, al. 1, CL.

valables pour les mesures provisionnelles. En revanche, les ordonnances de mesures superprovisionnelles ne peuvent pas être reconnues[495].

6.2.6 Conclusion

Celui qui veut poursuivre un fournisseur en Suisse peut choisir entre *plusieurs fors* (pour autant que les lieux concernés se trouvent en Suisse). La demande peut notamment être déposée au lieu du siège de la société ou du siège de la succursale du fournisseur impliquée dans les faits, au lieu où le fait dommageable a été perpétré (lieu de l'acte) et au lieu où le dommage est survenu (lieu du résultat). Pour les prétentions à l'égard d'un fournisseur, le lieu de l'acte coïncide généralement avec le lieu du siège de la succursale concernée. Lorsqu'il s'agit de déterminer le lieu du résultat, différents critères s'appliquent en fonction du type de droit violé. En cas d'atteinte à la personnalité, le rattachement au lieu du résultat aboutit régulièrement à l'établissement d'un for au lieu de la résidence habituelle du lésé.

Le *droit applicable* en cas de litige en Suisse dépend de la nature de l'atteinte. S'il s'agit d'atteinte à la personnalité, le demandeur peut opter entre le droit de l'État où il a son lieu de résidence habituelle, le droit de l'État où le fournisseur a sa succursale et le droit de l'État où le résultat de l'atteinte s'est produit. La première et la troisième option ne sont toutefois possibles que si l'auteur du dommage devait s'attendre à la survenance du dommage dans l'État en question. Si le lésé fonde ses prétentions sur la concurrence déloyale, le litige doit être soumis au droit de l'État sur le marché duquel le résultat du comportement déloyal s'est produit ou, si l'infraction ne déploie pas d'effets publics, le droit de l'État dans lequel se trouve la succursale concernée du lésé. Enfin, s'il s'agit d'une atteinte à un droit de propriété intellectuelle, le droit applicable est celui de l'État dans lequel la protection du droit visé est sollicitée.

Pour déterminer s'il est judicieux d'ouvrir l'action en Suisse, il faut savoir où le jugement devra être *exécuté* et, s'il s'agit d'un pays étranger, si ce dernier le reconnaîtra. Pour les actions introduites à l'étranger, le droit à appliquer se détermine selon les règles du droit interne de l'État concerné, sous réserve de conventions internationales.

7 Appréciation et perspectives

7.1 Actions défensives

7.1.1 Légitimation passive

- En cas d'atteinte à la personnalité, le lésé peut introduire une action défensive contre toute personne qui participe à l'atteinte (art. 28, al. 1, CC)[496]. Les actions défensives peuvent ainsi être dirigées contre les instigateurs, les complices et les co-auteurs, de sorte que la légitimation passive s'applique aussi à leur égard. L'étendue de la légitimation passive est identique ou semblable dans les autres domaines juridiques examinés (LPD, LCD, LDA, LPM)[497]. La légitimation passive ne peut cependant pas être de portée illimitée et l'importance de la participation doit être prise en compte.

[495] *Markus*, n° 1461 ss.
[496] Voir ch. 3.2.2 b).
[497] Pour la LCD, voir ch. 3.2.4 b) ; pour le droit de la propriété intellectuelle, voir ch. 3.2.5 a) (non sans avis contraires, voir renvois des notes 146 et 147).

Ainsi, il serait infondé d'admettre des prétentions contre les entreprises d'approvisionnement en électricité des fournisseurs.

- Le droit en vigueur fournit d'ores et déjà aux tribunaux les instruments nécessaires pour restreindre l'étendue de la légitimation passive à un cercle de personnes correspondant à ce qui est souhaitable. Ainsi, même si une participation très accessoire est déjà suffisante pour admettre l'action défensive, la participation ne saurait être prise en considération que s'il y a un lien de causalité adéquate[498]. L'action ne peut être admise que si la proportionnalité est garantie. Une pesée d'intérêts est nécessaire, celle-ci devant aussi tenir compte du fait que l'application de la décision du tribunal pourrait léser d'autres intérêts du défendeur ou de tiers[499]. Lorsque le lien avec l'atteinte illicite confine au néant ou que le fournisseur ne peut pas raisonnablement prévenir ou faire cesser l'atteinte (entièrement ou pour l'essentiel), il paraît judicieux de rejeter l'action défensive.
- S'agissant de la responsabilité à l'égard des contenus mis en ligne, le critère déterminant est la proximité du fournisseur avec le contenu. Pour garantir la protection des droits des personnes concernées, le Conseil fédéral estime souhaitable que les fournisseurs ayant une certaine maîtrise des contenus, comme les exploitants de plateformes ou les fournisseurs d'hébergement, puissent faire l'objet d'actions défensives visant à les obliger à éliminer des contenus illicites.
- Quant aux simples fournisseurs d'accès, les prestations qu'ils fournissent sont en grande partie automatisées et permettent d'accéder à l'ensemble d'Internet, dans le monde entier. On ne peut donc raisonnablement attendre d'eux qu'ils exercent une influence directe sur les contenus enregistrés. Par conséquent, les actions défensives dirigées contre ces fournisseurs risquent généralement d'être vouées à l'échec, faute d'un lien de causalité adéquate entre leur participation et l'atteinte[500].
- L'idée de restreindre dans la loi la légitimation passive est rejetée en raison de la difficulté d'englober dans une seule norme les nombreux cas de figure techniques possibles, en constante évolution.

7.1.2 Ordre de blocage – Verrouillage des adresses IP et DNS

a) De lege lata

- Si les fournisseurs d'hébergement ont la possibilité technique de supprimer des contenus qu'ils mettent en ligne sur leurs serveurs, les *fournisseurs d'accès* ne peuvent quant à eux guère satisfaire à une action en cessation de l'atteinte qu'en bloquant l'accès aux pages incriminées, ceci étant le seul moyen technique dont ils disposent[501].
- Le *verrouillage d'une adresse IP* vise à empêcher l'accès à un serveur donné: le fournisseur d'accès supprime l'accès de ses clients à l'adresse IP attribuée au serveur en cause et les empêche ainsi de trouver le chemin pour y accéder. Le *verrouillage d'une adresse DNS* consiste, pour le fournisseur d'accès, à bloquer la conversion de l'adresse Internet sous sa forme parlante – le nom de domaine – en une adresse IP.

[498] Voir ch. 3.2.2 b) et les renvois de la note 76.
[499] Voir ch. 3.2.2 b).
[500] Voir ch. 3.2.2 b) et les renvois de la note 76.
[501] Voir ch. 3.2.6 b).

C'est comme s'il effaçait le numéro de téléphone en face d'une personne dans son annuaire téléphonique[502].

- Ces mesures de blocage peuvent certes être contournées par des utilisateurs ayant de bonnes connaissances techniques, mais elles rendent tout de même les contenus illicites inaccessibles à une bonne part de la population[503].
- Une autre difficulté à laquelle se heurte l'action en cessation de l'atteinte dirigée contre le fournisseur d'accès est qu'il existe un grand nombre de fournisseurs et que ceux-ci devraient tous être visés par les mesures, afin d'interdire l'accès aux informations en question à large échelle (soit au moins tous les fournisseurs d'accès de Suisse, s'il s'agit de bloquer l'accès en Suisse).
- La proportionnalité des mesures techniques doit être examinée scrupuleusement dans chaque cas d'espèce. Il convient notamment d'éviter un *overblocking*, c'est-à-dire le blocage d'une adresse IP entraînant le blocage de l'accès à l'ensemble d'un serveur (donc également à des contenus se trouvant sur le même serveur que les contenus incriminés, mais qui ne sont pas visés par l'action).

b) Perspectives

- La mise en œuvre de la recommandation de l'AGUR12 selon laquelle les fournisseurs d'accès établis en Suisse devraient être tenus, sur ordre de l'autorité compétente dans les cas graves, de bloquer, par le biais du verrouillage des adresses IP et DNS, l'accès aux portails proposant des sources manifestement illégales[504] se traduira très certainement par une mesure relevant du droit administratif.
- Le projet de loi fédérale sur les jeux d'argent prévoit aussi une possibilité de blocage pour les offres de jeux d'argent enregistrées à l'étranger (voir art. 84 à 90 du projet[505]).

7.1.3 Action en prévention de l'atteinte (*stay down*)

- Dans le cadre des actions en prévention de l'atteinte, la question se pose de savoir dans quelle mesure les fournisseurs peuvent être tenus de surveiller activement des contenus et de les supprimer, et plus précisément d'en empêcher le téléchargement. Cette question ne se pose en fait que pour les fournisseurs d'hébergement, car les fournisseurs d'accès ne sont pas en mesure de surveiller les contenus qu'ils transmettent, ou alors moyennant un effort disproportionné.
- A priori, l'idée d'une décision de type « *stay down* » contraignant les fournisseurs d'hébergement à surveiller activement l'ensemble des contenus ou à les examiner à la recherche d'atteintes illicites fait aussi l'unanimité contre elle dans la doctrine[506].

---

[502] Voir ch. 3.2.6 b).
[503] Voir également le rapport final de l'AGUR12 (note 19), recommandation 9.3.4.
[504] Voir le rapport final de l'AGUR12 (note 19), recommandation 9.3.4, et le mandat du Conseil fédéral du 6.6.2014 sur la création des bases légales nécessaires dans le cadre de la suite des travaux de l'AGUR12.
[505] Voir ch. 3.2.6 b) cc) ii) (note 197).
[506] Voir ch. 3.2.6 a) et les renvois de la note 176.

- Dans le cadre des actions en prévention de l'atteinte, les tribunaux doivent être particulièrement attentifs à la proportionnalité des mesures dans le cas d'espèce. Il semble en tout cas que, selon le droit en vigueur, le tribunal ne puisse interdire que la participation à une (nouvelle) atteinte imminente, spécifique et concrète[507].
- Dans le domaine du droit d'auteur, la mise en œuvre des recommandations de l'AGUR12[508] devrait conduire à une codification de la situation juridique actuelle.
- En revanche, le Conseil fédéral ne voit pas la nécessité d'une règlementation globale de l'action en prévention de l'atteinte à l'encontre des fournisseurs.

7.2 Actions réparatrices

- Un fournisseur n'est tenu pour responsable que si une faute intentionnelle ou grave peut lui être imputée. Le point central est ici, comme souvent dans le domaine du droit de la responsabilité civile, la question de la diligence. Il n'existe actuellement, en Suisse, ni règlementation légale ni précédent pertinent qui concrétise les obligations de diligence des fournisseurs[509].
- Le Code de conduite Hébergement (CCH) de la simsa, qui relève de l'autorégulation, définit une procédure de notification et de retrait de contenu illicite (*notice and take down procedure*)[510]. Des réseaux sociaux tels que Facebook et Twitter prévoient aussi une procédure de ce type dans leurs conditions générales. Le Conseil fédéral est favorable à ces mesures d'autorégulation. La codification de ce système pourrait toutefois produire des effets pervers. Les (petits) fournisseurs ne disposent généralement pas des connaissances juridiques permettant d'effectuer une appréciation de la situation pertinente (y a-t-il atteinte ou non ?). Dans ces circonstances, il est à redouter qu'ils pèchent par excès de zèle en supprimant des contenus sur simple notification, ce qui pourrait avoir des répercussions sur la liberté d'expression des utilisateurs. Inversement, là où ce type de système a été mis en place, on a pu craindre que les fournisseurs – n'étant plus tenus d'intervenir que sur notification – n'aient plus d'incitation à développer et à mettre en œuvre des améliorations techniques permettant de renforcer la lutte contre les contenus clairement illicites[511].
- En accord avec la doctrine dominante, il faut exiger qu'un manque de diligence ne puisse être reproché au *fournisseur d'hébergement* que s'il est resté inactif après avoir reçu des indications précises d'une violation *flagrante* du droit et s'il n'a pas pris les mesures que l'on pouvait attendre de lui. Le fournisseur ne devrait être incité à supprimer des contenus de sa propre initiative qu'en cas de violation flagrante du droit[512]. Si l'on voulait obliger les fournisseurs à supprimer provisoirement des contenus

[507] Voir ch. 3.2.6 a).
[508] Voir le rapport final de l'AGUR12 (note 19), recommandation 9.3.3., et le mandat du Conseil fédéral du 6.6.2014.
[509] Voir *Frech*, 332 ss.
[510] Voir ch. 4.1.1.
[511] Voir ch. 3.3.2 au sujet de la discussion sur l'appréciation des conséquences juridiques aux États-Unis.
[512] Voir ch. 4.1.1 d) aa).

en cas de simple soupçon de violation du droit, on risquerait de verser dans la censure privée et d'effacer des contenus licites[513].

- Le Conseil fédéral est en outre favorable à une gradation des devoirs de diligence en fonction de la proximité avec le contenu. Les aspects ci-après doivent notamment être pris en compte dans les cas où le fournisseur n'a reçu aucune indication de violation du droit de la part d'une tierce partie.
    - L'obligation de prévenir ou de faire cesser les atteintes de sa propre initiative ne peut viser que les catégories de fournisseurs ayant une certaine proximité avec les contenus. Elle est vouée à l'échec s'agissant des *fournisseurs d'accès*, car ceux-ci ne peuvent pas surveiller les contenus qu'ils transmettent, ou alors moyennant un effort disproportionné. Les *fournisseurs d'hébergement* classiques, dont les prestations sont en grande partie automatisées, ne peuvent pas non plus être tenus d'exercer un contrôle préventif des contenus qu'ils mettent en ligne, car cela conduirait au report de la diffusion des contenus licites[514]. Pour le Conseil fédéral, une obligation de rechercher et de supprimer les atteintes sans disposer d'indications précises ne pourrait concerner, tout au plus, que les fournisseurs proches du contenu, comme les portails d'actualités ou les hébergeurs de forums et de blogs, car l'on peut admettre qu'ils peuvent avoir une certaine vue d'ensemble et exercer un contrôle des contenus mis en ligne sur leurs serveurs.
    - Mais même pour cette catégorie de fournisseurs, cette obligation ne saurait leur être imposée que si des atteintes paraissent probables compte tenu des circonstances particulières du cas d'espèce, par exemple si des atteintes ont déjà été constatées par le passé. Tel serait aussi le cas pour un portail d'actualités ou un hébergeur de blogs chez qui, en raison de la nature du contenu des articles qu'ils mettent en ligne, il y a lieu de s'attendre à des commentaires de lecteurs sujets à controverse.
- Mais une exclusion de la responsabilité des fournisseurs pourrait aussi avoir des effets pervers, notamment en raison du risque déjà évoqué de suppression de contenus à tout-va. On peut aussi estimer que les fournisseurs ont la possibilité de régler les questions de responsabilité à l'égard de leurs partenaires contractuels de façon adéquate par contrat[515].

La diligence requise est donc une question qui doit être appréciée par les tribunaux pour chaque cas d'espèce et qui ne se prête pas à une normalisation légale. Les principes décrits ci-dessus peuvent en revanche être utiles pour l'appréciation concrète des cas d'espèce.

7.3 Droits à l'information

L'impossibilité d'ouvrir une action civile contre inconnu n'est pas un problème spécifique à Internet et à ses fournisseurs, mais cet aspect revêt une importance accrue pour les atteintes commises sur Internet. Une action civile peut en principe être introduite contre les auteurs

[513] Voir ch. 1.3.2 c).
[514] La doctrine n'est pas unanime sur ce point, voir ch. 4.1.1 d) aa) et les renvois des notes 288 et 289.
[515] Théoriquement, les conditions contractuelles pourraient même prévoir la remise des données aux autorités. Cela n'est toutefois possible que pour les fournisseurs qui ne transportent pas les données en question et qui ne se sont donc pas assujettis au secret des télécommunications.

inconnus d'une atteinte – y compris sur la base de la jurisprudence Logistep du Tribunal fédéral[516] – mais cela nécessite préalablement l'ouverture d'une procédure pénale. Actuellement, il faut qu'un comportement soit punissable au regard du droit pénal pour justifier la levée du secret des télécommunications, soit de l'anonymat sur Internet, aux fins de faire valoir des prétentions civiles. Selon le Conseil fédéral, cette pesée d'intérêts doit demeurer.

Dans l'arrêt Logistep, le Tribunal fédéral avait déjà constaté qu'il appartenait au législateur de prendre les mesures éventuellement nécessaires pour garantir une *protection du droit d'auteur* adaptée aux nouvelles technologies. L'AGUR12 a émis à ce sujet une recommandation concrète, qui vise précisément les utilisateurs qui portent gravement atteinte au droit d'auteur en utilisant des réseaux pair-à-pair[517]. Le Conseil fédéral a chargé le DFJP de préparer les bases légales nécessaires dans le cadre de la suite des travaux de l'AGUR12. En revanche, il juge qu'une règlementation couvrant tous les domaines du droit n'est pas judicieuse pour le moment.

7.4 Droit de procédure

7.4.1 Cas nationaux: répartition des frais

Les actions défensives ne sont pas fondées sur la faute[518]. Dès lors, il peut arriver que, à la fin de la procédure, un défendeur n'ayant commis aucune faute succombe et que les frais soient mis à sa charge conformément à la règle générale de répartition des frais prévue à l'art. 106 CPC. Cela peut même déboucher sur des situations étranges, par exemple si le défendeur s'est soumis volontairement à la demande. C'est un effet collatéral inhérent aux actions qui ne sont pas fondées sur la faute. Dans ces actions, la légitimation passive nécessite uniquement – mais tout de même – une action ou une omission illicite[519]. Celui qui remplit ces conditions peut donc être entraîné dans une procédure civile sans préavis, y compris dans d'autres domaines du droit civil[520].

Dans certains cas, en vertu de l'art. 107, al. 1, let. b, e et f, CPC, le tribunal a la possibilité de répartir les frais selon sa libre appréciation, en les mettant par exemple à la charge du demandeur qui a eu gain de cause mais qui a omis de mettre en demeure le défendeur avant d'introduire l'action. Il faut cependant souligner que l'on ne peut pas toujours attendre du demandeur qu'il fasse une mise en demeure. Dans bien des cas, il est même justifié de chercher immédiatement la protection de la justice. Plusieurs aspects doivent être pris en compte: la nature du bien juridique violé, la gravité de l'atteinte et la probabilité que le défendeur accède volontairement à la demande. L'art. 107 CPC permet justement de tenir compte judicieusement des particularités du cas d'espèce. En revanche, une nouvelle norme spéciale selon laquelle les frais devraient être mis à la charge du demandeur s'il n'a pas mis en demeure le fournisseur et si ce dernier a immédiatement reconnu la demande ne semble pas appropriée. De toute manière, la question de la répartition des frais sera abordée à une plus large échelle dans le cadre de la prochaine évaluation globale du CPC[521].

---

[516] ATF 136 II 508, voir ch. 5.1.3 b).
[517] Rapport final de l'AGUR12 (note 19), recommandations 9.3.5 et 9.3.6.
[518] Voir ch. 3.2.2 ss.
[519] Voir ch. 3.2.2 ss.
[520] Par ex. les actions défensives dans le droit de voisinage, etc.
[521] Voir postulat Vogler 14.3804 « Code de procédure civile. Premiers enseignements et améliorations » du 24.9.2014 et motion CAJ-E 14.4008 « Adaptation du Code de procédure civile » du 17.11.2014.

7.4.2 Cas internationaux: for, droit applicable et exécution des décisions

La marge de manœuvre est limitée du point de vue suisse dans la mesure où les actions en responsabilité introduites en Suisse entrent dans le champ d'application de la Convention de Lugano. Quant aux dispositions de la LDIP sur la compétence en matière de responsabilité délictuelle, elles ont été révisées il y a quelques années. Elles permettent désormais de se conformer au régime de la CL, ce qui paraît sensé. A priori, une nouvelle réforme ne s'impose pas pour le moment. De plus, il conviendrait d'abord d'attendre l'évolution de la jurisprudence de la CJUE (qui est actuellement très active dans le domaine délictuel).

Les problèmes qui se posent (obligation de verser une avance, difficultés dans l'exécution des décisions à l'étranger) sont de nature générale et ne sauraient être résolus au moyen d'une règlementation unilatérale de la Suisse. Les auteurs du présent rapport ont tout de même examiné de manière approfondie s'il serait possible d'obliger les fournisseurs à indiquer un domicile de notification en Suisse, afin de faciliter l'exécution des décisions les concernant. En vertu de l'art. 140 CPC, les tribunaux peuvent certes ordonner aux parties dont le domicile ou le siège se trouve à l'étranger d'élire en Suisse un domicile de notification. Mais cette décision – puisqu'elle déploie des effets juridiques – doit elle-même être notifiée par la voie officielle[522], ce qui peut parfois occasionner une grande perte de temps[523]. Une norme légale pourrait éventuellement permettre de réduire la durée de cette étape.

On trouve par exemple une disposition en ce sens à l'art. 4, al. 4, de l'ordonnance du 6 octobre 1997 sur les ressources d'adressage dans le domaine des télécommunications (ORAT)[524]:

> « Les requérants établis à l'étranger doivent indiquer une adresse de correspondance en Suisse à laquelle des communications, des citations et des décisions peuvent notamment leur être valablement notifiées. »

Si cette disposition n'est pas respectée, l'OFCOM a la possibilité de révoquer l'attribution de ressources d'adressage (art. 11, al. 1, let. b, ORAT).

Il existe aussi une règle comparable dans le droit des marques (art. 42 LPM et art. 21 de l'ordonnance du 23 décembre 1992 sur la protection des marques[525]). Toutes ces dispositions ont en commun que la partie domiciliée à l'étranger est déjà en contact avec une autorité suisse et qu'une conséquence juridique claire est prévue si elle omet d'indiquer un domicile de notification (révocation du nom de domaine ou exclusion de la procédure d'opposition à l'enregistrement d'une marque). S'agissant des fournisseurs, une obligation générale de déclarer un domicile de notification en Suisse devrait plutôt être associée à une commination d'amende. En tout état de cause, le cercle des destinataires de cette obligation devrait être défini précisément et dépendre, par exemple, du nombre d'utilisateurs en Suisse.

Globalement, il semble toutefois plus pertinent de mettre l'accent sur la conclusion de traités bilatéraux ou multilatéraux d'entraide judiciaire en matière civile prévoyant la transmission directe par voie postale des actes devant être notifiés à l'étranger. Des traités de ce type ont déjà été conclus avec quelques États qui accueillent le siège social d'exploitants de

---

[522] Voir BSK ZPO-*Gschwend/Bornatico*, ad art. 140 n° 2.
[523] Voir ch. 6.2.4.
[524] RS 784.104 ; voir également art. 15, al. 3, 16, al. 3, 17, al. 2, let. b, et 23, al. 3, ODI.
[525] RS 232.111

plateformes bien connus[526]. En outre, la Suisse est en négociation avec l'UE et les autres États parties à la Convention de Lugano au sujet d'un éventuel traité parallèle au règlement européen sur la signification et la notification des actes, lequel prévoit aussi la transmission des actes par voie postale[527]. Dans ces circonstances, il est préférable de s'abstenir de développer unilatéralement une législation propre à la Suisse.

[526] États-Unis, Irlande, voir ch. 6.2.4.
[527] Voir ch. 6.2.4.

8 Appendices

8.1 Table des abréviations

ABGB	*Allgemeines Bürgerliches Gesetzbuch* (Autriche)
ACTA	Accord commercial anti-contrefaçon (*Anti-Counterfeiting Trade Agreement*
ADSL	*asymmetric digital subscriber line*
AEPD	*Agencia Española de Protección de Datos*
AGUR12	groupe de travail chargé d'améliorer la gestion collective des droits d'auteur et des droits voisins (*Arbeitsgruppe zum Urheberrecht)*
al.	alinéa(s)
art.	article(s)
ATF	Recueil officiel des arrêts du Tribunal fédéral suisse
BDSG	*Bundesdatenschutzgesetz* (Allemagne)
BGH	*Bundesgerichtshof* (Cour suprême fédérale, Allemagne)
blog	*weblog*, journal personnel tenu sur Internet
BSK	*Basler Kommentar* (Commentaire Bâlois)
CC	code civil (RS 210)
CCH	Code de conduite Hébergement de la simsa
CDA	*Communications Decency Act* (États-Unis)
CEDH	Convention de sauvegarde des droits de l'homme et des libertés fondamentales (RS 0.101)
cf.	*confer* (comparer, voir)
CG	conditions générales
ch.	chiffre(s)
CJUE	Cour de justice de l'Union européenne
CL	Convention concernant la compétence judiciaire, la reconnaissance et l'exécution des décisions en matière civile et commerciale (Convention de Lugano) (RS 0.275.12)
CO	Code des obligations (RS 220)
Cour EDH	Cour européenne des droits de l'homme
CP	code pénal (RS 311.0)
CPC	code de procédure civile (RS 272)
CPP	code de procédure pénale (RS 312.0)

Cst.	Constitution (RS 101)
DFJP	Département fédéral de justice et police
DMCA	*Digital Millennium Copyright Act* (États-Unis)
DNS	*domain name system*
ECG	*E-Commerce-Gesetz* (Autriche)
fedpol	Office fédéral de la police
FF	Feuille fédérale
FST	fournisseur de services de télécommunication
IP	*Internet protocol*
IPI	Institut fédéral de la propriété intellectuelle
ISDC	Institut suisse de droit comparé
JO	Journal officiel de l'Union européenne
LBI	loi sur les brevets (RS 232.14)
LCart	loi sur les cartels (RS 251)
LCD	loi fédérale contre la concurrence déloyale (RS 241)
LDA	loi sur le droit d'auteur (RS 231.1)
LDes	Loi sur les designs (RS 232.12)
LDIP	loi fédérale sur le droit international privé (RS 291)
let.	lettre(s)
LMSI	loi fédérale instituant des mesures visant au maintien de la sûreté intérieure (RS 120)
LPD	loi fédérale sur la protection des données (RS 235.1)
LPM	loi sur la protection des marques (RS 232.11)
LSCPT	loi fédérale sur la surveillance de la correspondance par poste et télécommunication (RS 780.1)
LTC	loi sur les télécommunications (RS 784.10)
ODI	ordonnance sur les domaines Internet (RS 784.104.2)
OEA	Organisation des États Américains
OFCOM	Office fédéral de la communication
OFJ	Office fédéral de la justice
OGH	*Oberster Gerichtshof* (Cour suprême fédérale, Autriche)
OLG	*Oberlandesgericht* (cour d'appel du Land, Allemagne / Autriche)
OMPI	Organisation mondiale de la propriété intellectuelle
ONU	Organisation des Nations Unies

OPM	ordonnance sur la protection des marques (RS 232.111)
ORAT	ordonnance sur les ressources d'adressage dans le domaine des télécommunications (RS 784.104)
OSCE	Organisation pour la sécurité et la coopération en Europe
Pacte II ONU	Pacte international du 16 décembre 1966 relatif aux droits civils et politiques, approuvé par l'Assemblée fédérale le 13 décembre 1991 (RS 0.103.2)
PFPDT	Préposé fédéral à la protection des données et à la transparence
PTT	Administration publique suisse des postes, téléphones et télégraphes (dissoute le 1er janvier 1998)
RS	Recueil systématique
s. / ss.	et suivant(e) / et suivant(e)s (page[s], note[s], etc.)
SECO	Secrétariat d'État à l'économie
simsa	Swiss Internet Industry Association
SIWR	Schweizerisches Immaterialgüter- und Wettbewerbsrecht (Helbing Lichtenhahn Verlag)
SOPA	*Stop Online Piracy Act* (États-Unis)
TF	Tribunal fédéral
TIC	technologie de l'information et de la communication
TMG	*Telemediengesetz* (Allemagne)
U.S.C	*United States Code* (États-Unis)
UE	Union européenne
UrhG	*Urheberrechtsgesetz* (Autriche)
WCT	Traité de l'OMPI du 20 décembre 1996 sur le droit d'auteur (*WIPO Copyright Treaty*)
WWW	*world wide web*

8.2 Bibliographie

Aebi-Müller Regina E., Personenbezogene Informationen im System des zivilrechtlichen Persönlichkeitsschutzes, Berne 2005

Auf der Maur Rolf/Steiner Thomas, Technologiegerechte Haftungsstandards für Online-Dienstanbieter, Selbstregulierungen als Benchmarks, in: Sethe Rolf et al. (édit.), Festschrift für Rolf H. Weber zum 60. Geburtstag, Berne 2011, 413 ss.

Barrelet Denis/Egloff Willi, Das neue Urheberrecht, 3e éd., Berne 2008

Baudenbacher Carl, in: Baudenbacher Carl (édit.), Lauterkeitsrecht: Kommentar zum Gesetz gegen den unlauteren Wettbewerb, Bâle 2001, ad art. 1 (cité Baudenbacher)

Baudenbacher Carl/*Glöckner Jochen*, in: Baudenbacher Carl (édit.), Lauterkeitsrecht, Kommentar zum Gesetz gegen der unlauteren Wettbewerb (UWG), Bâle 2001, ad art. 11 (cité Baudenbacher/Glöckner)

Beranek Zanon Nicole, Zivilrechtliche Haftung von Filehostern bei Urheberrechtsverletzungen nach Schweizer Recht, in: Jusletter IT du 11 décembre 2013 (cité Beranek Zanon, Jusletter IT du 11.12.2013)

Bommer Felix, Löschung als Einziehung von Daten, in: Schwarzenegger Christian/Arter Oliver/Jörg Florian S. (édit.), Internet-Recht und Strafrecht, Berne 2005, 171 ss.

Bonomi Andrea, in: Bucher Andreas (édit.), Commentaire Romand, Loi sur le droit international privé (LDIP) – Convention de Lugano (CL), Bâle 2011, ad art. 129 et 139 (cité Bonomi, CR LDIP)

Brehm Roland, in: Hausheer Heinz/Walter Hans Peter (édit.), Berner Kommentar. Das Obligationenrecht. Die Entstehung durch unerlaubte Handlungen, 4e éd., Berne 2013, ad art. 41 à 61 CO (cité BK-Brehm)

Briner Robert, Haftung der Internet-Provider für Unrecht Dritter, sic! 2006, 383 ss. (cité Briner, sic! 2006)

Bühler Gregor, Meta-Tags, Keywords und andere Mittel der Suchmaschinenoptimierung - eine Momentaufnahme aus Immaterialgüter- und wettbewerbsrechtlicher Sicht, in: Arter Oliver/Jörg Florian S. (édit.), Internet-Recht und Electronic Commerce Law, 9. Tagungsband, Berne 2007

Bühler Lukas, Schweizerisches und internationales Urheberrecht im Internet, Fribourg 1999

Busch Christoph, Secondary Liability of Service Providers, in: Schmidt-Kessel Martin (édit.), German National Reports on the 10th International Congress of Comparative Law, Tübingen 2014, 765 ss.

Cramer Conradin, Rechtsschutz bei Persönlichkeitsverletzungen durch Medien, recht 2007, 123 ss. (cité Cramer, recht 2007)

Dasser Felix, in: Schnyder Anton K./Vogt Nedim Peter/Honsell Heinrich/Berti Stephen V., Basler Kommentar Internationales Privatrecht, 3e éd., Bâle 2013, ad art. 139 (cité BSK IPRG-Dasser)

Donatsch Andreas/Wohlers Wolfgang, Strafrecht IV, 4e éd., Zurich 2011 (cité Donatsch/Wohlers, Strafrecht IV)

Dupuis Michel et al., Petit Commentaire Code pénal, 2e éd., Bâle 2011 (cité Dupuis et al., Petit Commentaire Code pénal)

Fanti Sébastien, Google suggest: analyse de la première jurisprudence helvétique à l'aune des décisions récentes sur le plan international, Jusletter du 26 mars 2012 (cité Fanti, Jusletter du 26.03.2012)

Fellmann Walter/Kottmann Andrea, Schweizerisches Haftpflichtrecht I, Berne 2012 (cité Fellmann/Kottmann, Haftpflichtrecht I)

Ficsor Mihály, The Law of Copyright and the Internet, Oxford 2002

Fountoulakis Christiana/Francey Julien, La diligence d'un hébergeur sur Internet et la réparation du préjudice, medialex 2014, 175 ss. (cité Fountoulakis/Francey, medialex 2014)

Frech, Philipp, Zivilrechtliche Haftung von Internet-Providern bei Rechtsverletzungen durch ihre Kunden, Zurich 2009

Gauch Peter/Schluep Walter/Schmid Jörg, Schweizerisches Obligationenrecht Allgemeiner Teil: Band 1, 10e éd., Zurich 2014 (cité Gauch/Schluep/Schmid, OR AT I)

Geiser Thomas, Zivilrechtliche Fragen des Kommunikationsrechts, medialex 1996, 203 ss. (cité Geiser, medialex 1996)

Gilliéron Philippe, La responsabilité des fournisseurs d'accès et d'hébergement, RDS 2002, 387 ss. (cité Gilliéron, RDS 2002)

Graber Christoph K., in: Honsell Heinrich/Vogt Nedim Peter/Wiegand Wolfgang (édit.), Basler Kommentar, Obligationenrecht I, 6e éd., Bâle 2015, ad art. 50 (cité BSK OR I-Graber)

Gschwend Julia/Bornatico Remo, in: Spühler Karl/Tenchio Luca/Infanger Dominik (édit.), Basler Kommentar Schweizerische Zivilprozessordnung (ZPO), 2e éd., Bâle 2013, ad art. 140 (cité BSK ZPO-Gschwend/Bornatico)

Hansjakob Thomas, in: Donatsch Andreas/Hansjakob Thomas/Lieber Viktor (édit.), Kommentar zur Schweizerischen Strafprozessordnung (StPO), 2e éd., Zurich 2014, ad art. 269, 272 et 273 (cité Hansjakob, Kommentar StPO)

Hansjakob Thomas, Kommentar zum Bundesgesetz und zur Verordnung über die Überwachung des Post- und Fernmeldeverkehrs, St-Gall 2006 (cité Hansjakob, Kommentar BÜPF)

Hansjakob Thomas, Wichtige Entwicklungen der Bundesgerichtspraxis zu Überwachungen des Post- und Fernmeldeverkehrs, forum poenale 2013, 173 ss. (cité Hansjakob, Entwicklungen)

Härting Niko, Internetrecht, 5e éd., Cologne 2014

Hausheer Heinz/Aebi-Müller Regina E., Das Personenrecht des schweizerischen Zivilgesetzbuches, 3e éd., Berne 2012

Heimgartner Stefan, in: Donatsch Andreas/Hansjakob Thomas/Lieber Viktor (édit.), Kommentar zur Schweizerischen Strafprozessordnung (StPO), 2e éd., Zurich 2014, ad art. 263 (cité Heimgartner, Kommentar StPO)

Heini Anton, in: Girsberger Daniel et al. (édit.), Zürcher Kommentar zum IPRG, 2e éd., Zurich 2004, ad art. 133 et 142 (cité ZK IRPG-Heini)

Heiniger Andreas, Das Bundesgericht geht in der Fernmeldeüberwachung weiter, als es das Gesetz erlaubt, in: Jusletter du 29 avril 2013 (cité Heiniger, Jusletter du 29.4.2013)

Hess-Blumer Andri, Teilnahmehandlungen im Immaterialgüterrecht unter zivilrechtlichen Aspekten, sic! 2003, 95 ss. (cité Hess-Blumer, sic! 2003)

Hofmann Dieter/Kunz Oliver, in: Oetiker Christian/Weibel Thomas (édit.), Basler Kommentar Lugano-Übereinkommen, Bâle 2011, ad art. 5 (cité BSK LugÜ-Hofmann/Kunz)

Hug Gitti, Haftung der Medien im Internetzeitalter, medialex 2014, 52 ss. (cité Hug, medialex 2014)

Hürlimann Daniel, Suchmaschinenhaftung, Berne 2012

Jean-Richard-dit-Bressel Marc, in: Niggli Marcel Alexander/Heer Marianne/Wiprächtiger Hans (édit.), Basler Kommentar, Schweizerische Strafprozessordnung, 2e éd., Bâle 2014 (cité BSK StPO-Jean-Richard-dit-Bressel)

Jenny David, in: Sutter-Somm Thomas/Hasenböhler Franz/Leuenberger Christoph (édit.), Kommentar zur Schweizerischen Zivilprozessordnung (ZPO), 2e éd., Zurich 2013, ad art. 107 (cité Jenny, Kommentar ZPO)

Keller Andreas J., in Donatsch Andreas/Hansjakob Thomas/Lieber Viktor (édit.), Kommentar zur Schweizerischen Strafprozessordnung (StPO), 2e éd., Zurich 2014, ad art. 246 (cité Keller, Kommentar StPO)

Kernen Alexander, Volle Verantwortlichkeit des Host Providers für persönlichkeitsverletzende Handlungen seines Kunden, in: Jusletter du 4 mars 2013 (cité Kernen, Jusletter du 4.3.2013)

Kessler Martin A., in: Honsell Heinrich/Vogt Nedim Peter/Wiegand Wolfgang (édit.), Basler Kommentar, Obligationenrecht I, 6e éd., Bâle 2015, ad art. 41 à 49 (cité BSK OR I-Kessler)

Killias Laurent/Kramer Michael/Rohner Thomas, Gewährt Art. 158 ZPO eine « pre-trial discovery » nach US-amerikanischem Recht?, in: Lorandi Franco/Staehelin Daniel (édit.), Innovatives Recht, Festschrift für Ivo Schwander, Zurich/St-Gall 2011, 933 ss.

Kley Andreas/Tophinke Esther, in: Ehrenzeller Bernhard/Schindler Benjamin/Schweizer Rainer J./Vallender Klaus A. (édit.), Die Schweizerische Bundesverfassung, St. Galler Kommentar, 3e éd., Zurich/St-Gall 2014, ad art. 16 (cité Kley/Tophinke, St. Galler Kommentar)

Kraft Nikolaus, Zugangssperren zu Webseiten als Mittel der Rechtsdurchsetzung, Medien und Recht 2014, 171 ss. (cité Kraft, Medien und Recht 2014)

Krüsi Melanie, Das Zensurverbot nach Art. 17 Abs. 2 der Schweizerischen Bundesverfassung, Zurich 2011

Kut Ahmet/Stauber Demian, Die UWG-Revision vom 17. Juni 2011 im Überblick, in: Jusletter du 20 février 2012 (cité Kut/Stauber, Jusletter du 20.2.2012)

Marbach Eugen, Markenrecht, in: von Büren Roland/David Lucas (édit.), Schweizerisches Immaterialgüter- und Wettbewerbsrecht (SIWR) III/1, 2e éd., Bâle 2009 (cité Marbach, SIWR III/1)

Markus Alexander R., Internationales Prozessrecht, Berne 2014

Mehra Salil K./Trimble Marketa, Secondary Liability, ISP Immunity, and Incumbent Entrenchment, American Journal of Comparative Law 2014, 685 ss. (cité Mehra/Trimble, AMJCL 2014)

Meier Philippe, Protection des données - Fondements, principes généraux et droit privé, Berne 2011

Meili Andreas, in: Honsell Heinrich/Vogt Nedim Peter/Geiser Thomas (édit.), Basler Kommentar, Zivilgesetzbuch I, 5e éd., Bâle 2014, ad art. 28 et 28*a* (cité BSK ZGB I-Meili)

Müller Barbara K., *in: Müller Barbara K./Oertli Reinhard*, Urheberrechtsgesetz, 2e éd., Berne 2012*,* ad art. 62 (cité Müller Barbara K., Handkommentar URG)

Müller Jürg, Lauterkeitsrecht, in: von Büren Roland/David Lucas (édit.), Schweizerisches Immaterialgüter- und Wettbewerbsrecht V/1, Bâle 1998 (cité Müller Jürg, SIWR V/1)

Neumann Sophie, Die Haftung der Intermediäre im Internationalen Immaterialgüterrecht, Munich 2014

Popp Peter/Berkemeier Anne, in: Niggli Marcel Alexander/Wiprächtiger Hans (édit.), Basler Kommentar, Strafrecht I, 3e éd., Bâle 2013 (cité BSK Strafrecht I-Popp/Berkemeier)

Rauber Georg, Lauterkeitsrecht, in: von Büren Roland /David Lucas (édit.), Schweizerisches Immaterialgüter- und Wettbewerbsrecht V/1, Bâle 1998 (cité Rauber, SIWR V/1)

Rehbinder Manfred/Viganò Adriano, URG, 3e éd., Zurich 2008 (cité Rehbinder/Viganò)

Reinle Michael/Obrecht Matthias, Markenrechtsverletzungen durch Google AdWords, sic! 2009, 112 ss. (cité Reinle/Obrecht, sic! 2009)

Reymond Michel, La compétence internationale en cas d'atteinte à la personnalité par Internet, Genève 2015

Rivara Irène, Keywords advertising – développements récents au regard du droit des marques, PJA 2012, 1546 ss. (cité Rivara, PJA 2012)

Rohn Patrick, Zivilrechtliche Verantwortlichkeit der Internet Provider nach schweizerischem Recht, Zurich 2004

Rosenthal David, in: Rosenthal/Jöhri (édit.), Handkommentar zum Datenschutzgesetz, Zurich/Bâle/Genève 2008, ad art. 15 (cité Rosenthal, in: Rosenthal/Jöhri)

Rosenthal David, Entwicklungen im privaten Datenschutzrecht, in: Furrer Andreas, La pratique de l'avocat 2013, 707 ss. (cité Rosenthal, La pratique de l'avocat 2013)

Rosenthal David, Internet-Provider-Haftung – ein Sonderfall?, in: Jung Peter (édit.), Aktuelle Entwicklungen im Haftungsrecht, Zurich 2007 (cité Rosenthal, Internet-Provider-Haftung – ein Sonderfall?)

Roth Simon, Die grenzüberschreitende Edition von IP-Adressen und Bestandesdaten im Strafprozess - Direkter Zugriff oder Rechtshilfe?, in: Jusletter du 17 août 2015 (cité Roth, Jusletter du 17.8.2015)

Rüetschi David, in: Hilty Reto M./Arpagaus Reto (édit.), Basler Kommentar Bundesgesetz gegen den unlauteren Wettbewerb (UWG), Bâle 2013, ad art. 11 (cité BSK UWG-Rüetschi)

Rüetschi David/Roth Simon, in: Hilty Reto M./Arpagaus Reto (édit.), Basler Kommentar Bundesgesetz gegen den unlauteren Wettbewerb (UWG), Bâle 2013, ad art. 9 (cité BSK UWG-Rüetschi/Roth)

Schaltegger Paul, Die Haftung der Presse aus unlauterem Wettbewerb, Zurich 1992

Schlosser Ralph, in: De Werra Jacques/Gilliéron Philippe (édit.), Commentaire Romand Propriété intellectuelle, Bâle 2013, ad art. 62 LDA (cité Schlosser, CR PI)

Schneider-Marfels, Karl-Jascha, Facebook, Twitter & Co. : « Imperium in imperio », in: Jusletter du 20 février 2012 (cité Schneider-Marfels, Jusletter du 20.2.2012)

Schnyder Anton K., in: Schnyder Anton K. (édit.), Lugano-Übereinkommen zum internationalen Zivilverfahrensrecht, Kommentar, Zurich 2011, ad art. 5 (cité Schnyder, LugÜ Kommentar)

Schoch Nik/Schüepp Michael, Provider-Haftung « de près ou de loin »?, in: Jusletter du 13 mai 2012 (cité Schoch/Schüepp, Jusletter du 13.5.2012)

Schwaibold Matthias, in: Honsell Heinrich/Vogt Nedim Peter/Geiser Thomas (édit.), Basler Kommentar, Zivilgesetzbuch I, 5e éd., Bâle 2014, ad art. 28*g* (cité BSK ZGB I-Schwaibold)

Schwarzenegger Christian, Sperrverfügungen gegen Access-Provider, in: Arter Oliver/Jörg Florian S. (édit.), Internet-Recht und Electronic Commerce Law, Berne 2003

Schwenzer Ingeborg, Schweizerisches Obligationenrecht Allgemeiner Teil, 6e éd., Berne 2012

Seelmann Kurt, Strafrecht Allgemeiner Teil, 5e éd., Bâle 2012

Smith Graham J. H., Internet Law and Regulation, 4e éd., Londres 2007

Spitz Philippe, in: Jung Peter/Spitz Philippe (édit.), Bundesgesetz gegen den unlauteren Wettbewerb /UWG), Stämpflis Handkommentar, Berne 2010, ad art. 9 (cité Spitz, Handkommentar UWG)

Sprecher Thomas, in: Spühler Karl/Tenchio Luca/Infanger Dominik (édit.), Basler Kommentar Schweizerische Zivilprozessordnung, 2e éd., Bâle 2013, ad art. 261 à 269 (cité BSK ZPO-Sprecher)

Spühler Karl/Dolge Annette/Gehri Myriam, Schweizerisches Zivilprozessrecht, 9e éd., Berne 2010

Staehelin Adrian/Staehelin Daniel/Grolimund Pascal, Zivilprozessrecht, 2e éd., Zurich 2013

Staub Roger, in: Thouvenin Florent/Bühler Gregor/Noth, Michael G. (édit.), Markenschutzgesetz (MSchG), Stämpflis Handkommentar, Berne 2009, ad art. 55 (cité Staub, Handkommentar MSchG)

Steinauer Paul-Henri/Fountoulakis Christiana, Droit des personnes physiques et de la protection de l'adulte, Berne 2014

Tappy Denis, in: Bohnet François/Haldy Jacques/Jeandin Nicolas/Schweizer Philippe/Tappy Denis, CPC Code de procédure civile commenté, Bâle 2011, ad art. 107 (cité CPC-Tappy)

Tercier Pierre, Le nouveau droit de la personnalité, Zurich 1984

Thouvenin Florent/Dorigo Lara, in: Thouvenin Florent/Bühler Gregor/Noth, Michael G. (édit.), Markenschutzgesetz (MSchG), Stämpflis Handkommentar, Berne 2009, ad art. 13 (cité Thouvenin/Dorigo, Handkommentar MSchG)

Trechsel Stefan/Jean-Richard-dit-Bressel Marc, in: Trechsel Stefan/Pieth Mark (édit.), Schweizerisches Strafgesetzbuch, Praxiskommentar, 2e éd., Zurich/St-Gall 2013, ad art. 322 (cité Trechsel/Jean-Richard-dit-Bressel, Praxiskommentar StGB)

Trechsel Stefan/Lieber Viktor, in: Trechsel Stefan/Pieth Mark (édit.), Schweizerisches Strafgesetzbuch, Praxiskommentar, 2e éd., Zurich/St-Gall 2013, ad art. 179octies (cité Trechsel/Lieber, Praxiskommentar StGB)

Umbricht Robert P./Rodriguez Rodrigo/Krüsi Melanie, in: Schnyder Anton K./Vogt Nedim Peter/Honsell Heinrich/Berti Stephen V. (édit.), Basler Kommentar Internationales Privatrecht, 3e éd., Bâle 2013, ad art. 129 (cité BSK IPRG-Umbricht/Rodriguez/Krüsi)

Verbiest Thibault/Spindler Gerald/Riccio Giovanni Maria/van der Perré Aurélie, Study on the Liability of Internet Intermediaries, 12 novembre 2007, disponible à l'adresse ec.europa.eu/internal_market/e-commerce/docs/study/liability/final_report_en.pdf

Volken Paul, in: Girsberger Daniel et al. (édit.), Zürcher Kommentar zum IPRG, 2e éd., Zurich 2004, ad art. 130 (cité ZK IRPG-Volken)

Von Büren Bruno, Kommentar zum Bundesgesetz über den unlauteren Wettbewerb, Zurich 1957

Weber Rolf H./Wolf Christoph A., Fragmentarische E-Commerce-Gesetzgebung, in: Jusletter du 18 juin 2012 (cité Weber/Wolf, Jusletter du 18.6.2012)

Weber, Rolf H., E-Commerce und Recht, 2e éd., Zurich/Bâle/Genève 2010 (cité Weber, E-Commerce)

Wullschleger Marc, Die Durchsetzung des Urheberrechts im Internet, Berne 2015

Zeller Franz, in: Niggli Marcel Alexander/Wiprächtiger Hans (édit.), Basler Kommentar Strafrecht II, 3e éd., Bâle 2013, ad art. 322 (cité BSK StGB II-Zeller)

Zeller Franz, Zugangssperren im Internet: keine Beschwerdebefugnis für Musikkonsumenten, medialex 2014, 209 ss. (cité Zeller, medialex 2014)

Zufferey Nathalie/Bacher Jean-Luc, in: Kuhn André/Jeanneret Yvan (édit.), Commentaire Romand. Code de procédure pénale suisse, Bâle 2010, ad art. 273 (cité Zufferey/Bacher, CR CPP)