# La responsabilité des prestataires intermédiaires sur les réseaux

Montero, Etienne

*Published in:*
Le commerce électronique européen sur les rails? : Analyse et propositions de mise en oeuvre de la directive sur le commerce électronique

*Publication date:*
2001

*Document Version*
le PDF de l'éditeur

CHAPITRE VI

# LA RESPONSABILITÉ DES PRESTATAIRES INTERMÉDIAIRES SUR LES RÉSEAUX*

Étienne MONTERO

## PROPOS LIMINAIRES

**516.** Les réseaux numériques – et singulièrement l'internet – peuvent être une source de préjudices économiques, moraux, voire corporels, liés à la diffusion de contenus illicites, lacunaires ou non conformes à l'attente légitime des usagers. Se trouve ainsi posée, de manière récurrente, la question de la responsabilité – pénale et civile – non seulement des producteurs et éditeurs de pareils contenus, mais aussi des prestataires intermédiaires, dont le rôle est soit de rendre ceux-ci accessibles, soit d'en assurer l'hébergement ou le transport à distance.

La dimension mondiale de l'internet rend souvent malaisée l'identification des auteurs de messages préjudiciables, d'autant qu'ils ont pu œuvrer à partir de l'étranger. En revanche, les fournisseurs d'accès et d'hébergement, notamment, sont connus, proches et à la portée de la victime. Souvent ils sont aussi plus solvables. Ces circonstances expliquent que l'attention se soit naturellement portée sur les prestataires intermédiaires.

Le contentieux relatif à la responsabilité des intermédiaires fait actuellement l'objet de vives controverses en jurisprudence, en doctrine et, naturellement, parmi les divers acteurs concernés (les intermédiaires eux-mêmes, les représentants des usagers de l'internet, des titulaires de droits de propriété intellectuelle, des consommateurs, etc.). Les hésitations et discussions portent sur la possibilité technique, la faisabilité économique et l'opportunité du contrôle et, au besoin, du filtrage des contenus diffusés par les soins des intermédiaires. Au-delà, l'âpreté du débat est due, logiquement, à la diversité des intérêts en présence et des

---

* Le présent commentaire reprend largement et, pour partie, complète ou actualise une étude antérieure de E. MONTERO, "La responsabilité des prestataires intermédiaires de l'internet", *Revue Ubiquité*, n° 5, juin 2000, pp. 99 à 117. Cette publication a été réalisée dans le cadre de l'intervention de l'auteur lors de l'Audition publique sur le thème "Le développement du commerce électronique en Europe : quelle politique de l'Union ?", organisée au Parlement Européen par la Commission juridique et du marché intérieur, à Bruxelles, le 28 mars 2000. Cet événement était préparatoire à la session du Parlement au cours de laquelle fut adoptée, en seconde lecture, la proposition de directive sur le commerce électronique (position commune).

"idéologies" ou politiques juridiques prônées. Il s'ensuit une grande incertitude juridique, qui se traduit par l'élaboration de solutions jurisprudentielles, et même législatives, divergentes au sein de l'Union européenne.

**517.** Ce constat explique que la Commission européenne ait souhaité intervenir pour fixer des principes et critères de responsabilité uniformes. Elle estime, en effet, que "les divergences existantes et émergentes entre les législations et les jurisprudences des États membres dans le domaine de la responsabilité des prestataires de services agissant en qualité d'intermédiaires empêchent le bon fonctionnement du marché intérieur, en particulier en gênant le développement des services transfrontaliers et en produisant des distorsions de concurrence (…)" (considérant n° 40)[610].

Outre la prétention de rapprocher les législations et les jurisprudences des États membres en ce domaine, la section 4 poursuit d'autres objectifs déclinés dans le considérant n° 40. On se borne ici à les énoncer :

1° elle prévoit que, dans des cas spécifiques, les prestataires intermédiaires aient le devoir d'agir pour éviter des activités illégales ou pour y mettre fin.

2° elle entend constituer la base adéquate pour l'élaboration de mécanismes rapides et fiables permettant de retirer les informations illicites et de rendre l'accès à celles-ci impossible.

3° enfin, il est à noter que la directive ne devrait pas faire obstacle au développement et à la mise en œuvre effective, par les différentes parties concernées, de systèmes techniques de protection et d'identification, ainsi que d'instruments techniques de surveillance rendus possibles par les techniques numériques, dans le respect des limites établies par les directives concernant la protection des personnes physiques à l'égard du traitement des données à caractère personnel[611].

---

[610] Voy. également l'exposé des motifs de la proposition de directive du Parlement européen et du Conseil relative à certains aspects juridiques du commerce électronique dans le marché intérieur présentée par la Commission le 18 novembre 1998, COM (1998) 586 final, p. 13, où est il est souligné, notamment, combien "la situation actuelle incite les prestataires à implanter leurs activités dans les États membres dotés de régimes favorables" (risque de "forum-shopping"). Ultérieurement, nous nous référerons exclusivement à cet exposé des motifs (cité, en abrégé, exposé des motifs ou commentaire article par article, avec indication de la page).

[611] Directive 95/46/CE du Parlement européen et du Conseil du 24 octobre 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, *J.O.C.E.*, L 281 du 23 novembre 1995 et directive 97/66/CE du Parlement européen et du Conseil du 15 décembre 1997 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des télécommunications, *J.O.C.E.*, L 30 janvier 1998, p. 24.

**518.** Après une succincte présentation d'ensemble de la section 4 (domaine d'application, nature des régimes de responsabilité institués et économie générale du dispositif), nous procéderons à une analyse, article par article, de la section, en formulant au passage nos suggestions en vue de la transposition. Sauf exceptions, il ne sera pas fait état des décisions rendues, par les cours et tribunaux des États membres de l'Union européenne, en référence aux régimes de droit commun de la responsabilité[612]. Pareille analyse jurisprudentielle serait hors de propos dans le cadre du présent commentaire.

## I. VUE D'ENSEMBLE DE LA SECTION 4

### A. Le domaine d'application

**519.** La section 4 s'inspire indubitablement de la législation américaine relative au droit d'auteur dans l'environnement numérique — le "*Digital Millenium Copyright Act"*, adopté le 28 octobre 1998, aux fins de ratifier les deux traités de l'OMPI du 20 décembre 1996[613].

Comme l'indique son intitulé, la section 4 traite exclusivement de la responsabilité des prestataires intermédiaires sur les réseaux de communication. Le rôle d'intermédiaire se caractérise par le fait que les informations sont non seulement fournies par les destinataires du service, mais aussi transmises ou stockées à la demande de ces derniers[614]. Pour rappel, par "destinataire du service", il faut entendre la personne, physique ou morale, qui, à titre privé ou professionnel, utilise un service de la société d'information, notamment pour rechercher des informations ou les rendre accessibles (cf. l'art. 2, d)[615].

**520.** Dans la directive européenne, comme dans la loi américaine, les régimes (d'exonération) de responsabilité diffèrent, plus précisément,

---

[612] Pour un tel examen de jurisprudence, voy. E. MONTERO, étude précitée; A. STROWEL et N. IDE, "Responsabilité des intermédiaires : actualités législatives et jurisprudentielles", disponible sur internet (www.droit-technologie.org).

[613] Pour une comparaison des deux textes, V. SEDALLIAN, "La responsabilité des prestataires techniques sur Internet dans le Digital Millenium Copyright Act américain et le projet de directive européen sur le commerce électronique", *Cahiers Lamy droit de l'informatique et des réseaux*, n° 110, 1999, pp. 1-4.

[614] Cf. Commentaire article par article, p. 28.

[615] Sauf indication contraire, les articles cités au texte sans autre précision renvoient toujours aux dispositions de la directive européenne sur le commerce électronique. Le même principe vaut pour les références aux considérants de la directive.

selon l'*activité* exercée, et non en fonction du type d'opérateur[616]. Cette distinction est capitale et constitue une clé d'interprétation décisive du dispositif de la section 4. En effet, une activité de nature apparemment technique, ou présentée comme telle, peut être "disqualifiée" en activité de production ou d'édition de contenu, en fonction du comportement du prestataire concerné ou de certains engagements contractuels souscrits par lui. En ce cas, pour cette activité, ce dernier sera soumis au droit commun de la responsabilité et ne pourra donc bénéficier d'un régime favorable prévu à la section 4. Le commentaire article par article de la proposition initiale de directive (p. 28) est très clair sur ce point : "la distinction en ce qui concerne la responsabilité n'est pas fondée sur le type d'opérateur, mais sur le type d'activité exercé. Le fait qu'un prestataire remplit les conditions pour être exonéré de responsabilité pour une activité donnée ne l'exonère pas de sa responsabilité pour toutes ses autres activités".

Ainsi, seules certaines *activités* exercées par les intermédiaires techniques sont couvertes par les exonérations de responsabilité des articles 12 à 15. Il s'agit des activités de transport, de fourniture d'accès aux réseaux, de stockage temporaire sous forme de "cache" et d'hébergement. Les activités de production et d'édition sur les réseaux, quant à elles, ne sont pas visées par ces dispositions. Elles ressortissent donc au droit commun de la responsabilité. Il en est de même pour les activités relatives aux moteurs de recherche et à l'établissement de liens hypertextes. A l'occasion de ses rapports relatifs à l'application de la directive, à présenter au Parlement européen, au Conseil et au Comité économique et social, avant le 17 juillet 2003 et ensuite tous les deux ans (art. 21, 1), la Commission devra analyser en particulier la nécessité de présenter des propositions relatives à la responsabilité des fournisseurs de liens hypertextes et de services de moteur de recherche… (art. 21, 2).

**521.** Contrairement à la loi américaine, dont le domaine d'application est limité au *copyright* et à la contrefaçon, à l'exclusion des autres activités illicites, la section 4 vise, de manière horizontale, tous les types de contenus illicites. Aussi le système de responsabilité a-t-il vocation à s'appliquer en matière de concurrence déloyale, de contrefaçon d'œuvres protégées par des droits intellectuels, de publicité trompeuse, d'atteinte à la vie privée, de diffamation, etc.

[616] Voy. le très explicite considérant n° 42.

Les règles établies dans la section 4 concernent tant la responsabilité pénale que civile[617]. Les exonérations de responsabilité couvrent "à la fois les cas où un prestataire de services pourrait être tenu directement responsable d'une infraction et ceux où il pourrait être jugé responsable à titre accessoire d'une infraction commise par une autre personne", notamment sur la base des règles de la participation criminelle (par exemple comme complice, pour avoir fourni, en connaissance de cause, une aide, une assistance ou tout autre moyen ayant facilité la réalisation de l'infraction) (cf. art. 67 et 68 C. pén.)[618].

Les travaux préparatoires de la directive soulignent, en des termes quelque peu maladroits, que "les dispositions de cette section n'affectent pas le droit matériel qui régit les différentes *infractions* qui peuvent être concernées. Cette section se borne à limiter la responsabilité"[619]. Autrement dit, la section 4 n'a pas d'incidence sur la substance du droit de la responsabilité tant pénale que civile des États membres. Elle n'entraîne pas que les États membres doivent modifier ici ou là les principes et dispositions qui gouvernent ces matières, se contentant de les écarter dans des cas déterminés et sous certaines conditions.

### B. La nature des régimes de responsabilité

**522.** Le législateur européen n'a pas opté pour l'instauration d'un régime spécifique d'imputation préalable et hiérarchique (c'est-à-dire par défaut) – communément désigné sous le nom de "responsabilité en cascade" –, en dépit du plaidoyer fait en ce sens par plusieurs auteurs[620].

Cette solution nous paraît heureuse pour de multiples motifs déjà exposés ailleurs[621].

---

[617] Cette interprétation ne peut s'autoriser ni d'une disposition expresse ni d'un considérant de la directive, mais s'appuie sur diverses indications claires et indiscutables dans le commentaire article par article de la proposition de directive (pp. 29 et 30).

[618] Commentaire article par article, p. 29. Bien qu'elle figure dans le commentaire de l'article 12, cette remarque vaut pour les trois cas d'exonération.

[619] Commentaire article par article de la proposition de directive, p. 28. Souligné par nous.

[620] Par exemple, F. OLIVIER et E. BARBRY, "Des réseaux aux autoroutes de l'information : révolution technique? Révolution juridique? 2. Du contenu informationnel sur les réseaux", *J.C.P.*, G, 1996, I, 3928, p. 185, n° 43 ; D. VOORHOOF, "De regel van de getrapte verantwoordelijkheid : van de 19de naar de 21ste eeuw ?", *Recente Arresten van het Hof van Cassatie*, 1996, pp. 387 et s.

[621] Cf., en particulier, E. MONTERO, "La responsabilité civile des médias", dans A . STROWEL et F. TULKENS (sous la direction de), *Prévention et réparation des préjudices causés par les médias*, Bruxelles, Larcier, 1998, pp. 95 et s. ; *Idem*, "Les responsabilités liées à la diffusion d'informations illicites ou inexactes sur Internet", in E. MONTERO (éd.), *Internet face au droit*, Cahiers du CRID, n° 12, Kluwer, 1997, spéc. pp. 127 et s.

Comme on sait, en droit belge, un régime de responsabilité en cascade est consacré, en matière de presse écrite, par l'article 25, alinéa 2, de la Constitution[622]. Divers arguments[623] conduisent à penser qu'en l'état actuel du texte, ce régime – forgé à une autre époque et dans un autre contexte, et techniquement mal adapté aux réseaux de communication numériques – ne trouve pas à s'appliquer à ces derniers. Par conséquent, il n'y a pas lieu, à notre avis, de modifier cette disposition constitutionnelle dans le cadre de la transposition en droit interne de la section 4.

Quant à la suggestion formulée par certains auteurs de créer un régime de responsabilité en cascade *spécifique* pour l'internet, elle ne nous paraît pas opportune et n'est, au demeurant, plus possible. Pour faire bref, il nous semble qu'un système visant à la désignation préalable et automatique des responsables, même par défaut, cadre mal avec un environnement ouvert comme l'internet, où les rôles sont peu définis, volatiles et les liens existants entre les acteurs parfois éphémères et peu transparents, au contraire de domaines tels que l'audiovisuel ou la presse écrite.

En refusant de s'engager dans cette voie, la Commission européenne a donc fait un choix judicieux à nos yeux.

**523.** Le système de responsabilité de la directive s'inscrit, en quelque sorte, dans l'orbite du droit commun. Concrètement, l'activité de simple transport (*"mere conduit"*) est pratiquement exonérée de toute responsabilité ; en revanche, pour l'hébergement et le stockage sous forme de "cache", la responsabilité du prestataire peut être recherchée, à certaines conditions précisées. Nous sommes d'avis que, ce faisant, le législateur s'évertue fondamentalement à lever les hésitations – porteuses de distorsions de concurrence au sein de l'Union européenne (cf. le considérant n° 40 déjà cité) – concernant le rôle et la diligence due par les intermédiaires techniques de l'internet. A cette fin, le législateur européen ne fait, en définitive, que circonscrire le devoir général de prudence et de diligence à charge des prestataires intermédiaires, en fixant un critère *raisonnable* destiné à guider le juge dans son appréciation.

---

[622] Pour rappel, un arrêt de la Cour de cassation en date du 31 mai 1996 a réaffirmé, en des termes particulièrement nets, que la responsabilité en cascade prévue par cette disposition s'applique non seulement à l'action publique, mais aussi à l'action civile en réparation. Cf. Cass., 31 mai 1996, *J.T.*, 1996, p. 597, avec les concl. conf. de M. l'avocat général LECLERCQ.

[623] Voy. E. MONTERO, "La responsabilité civile des médias", *op. cit.*, spéc. pp. 95-108.

## C. L'économie générale du dispositif

**524.** A notre avis, la directive, en sa mouture définitive, est parvenue à trouver un bon équilibre entre les différents intérêts en jeu[624]. A juste titre, elle opère une distinction fondamentale entre les activités dites de "simple transport", largement exonérées, et les autres activités intermédiaires (l'hébergement et le stockage sous forme de cache), soumises, elles, à une responsabilité limitée.

### *1. Absence d'obligation générale de surveillance*

**525.** L'absence d'obligation *générale* de surveillance à charge des prestataires est un principe essentiel que nous ne pouvons qu'approuver. Plus précisément, l'article 15, 1, invite les États membres à n'imposer aux prestataires, pour la fourniture des services de "simple transport", de stockage sous forme de "cache" et d'hébergement, aucune obligation générale de surveiller des informations qu'ils transmettent ou stockent, ni aucune obligation générale de rechercher activement des faits ou des circonstances révélant des activités illicites. Les prestataires intermédiaires se trouvent ainsi dispensés d'effectuer des contrôles *a priori* systématiques, techniquement malaisés, aléatoires quant à leur efficacité, difficilement supportables économiquement et toujours susceptibles de dégénérer vers des formes de censure préventive non souhaitée. Sans compter le risque de glissement vers une objectivation de la responsabilité tant pourrait être grande la tentation pour les juges, en présence d'une information illicite, de *supposer* l'insuffisance du contrôle et d'en *déduire* une faute dans le chef de l'intermédiaire mis en cause.

Il est à remarquer que ce principe n'empêchera pas les intermédiaires (on songe en particulier aux fournisseurs d'accès et prestataires d'hébergement) d'effectuer certains contrôles, comme ils l'ont toujours fait. Leur image de marque est en jeu et tout porte à croire que, demain, ils continueront d'y être sensibles. Ces contrôles *volontaires* sont les bienvenus et répondent, du reste, à un vœu exprimé en ce sens dans la directive (considérant n° 40, *in fine*).

---

[624] En ce sens également, voy. la position en seconde lecture de la Commission juridique et du marché intérieur du Parlement Européen (Recommandation pour la deuxième lecture relative à la position commune du Conseil en vue de l'adoption de la directive du Parlement européen et du Conseil relative à certains aspects juridiques des services de la société de l'information, et notamment du commerce électronique, dans le marché intérieur, rapport de A. PALACIO VALLELERSUNDI, au nom de la Commission juridique et du marché intérieur, 12 avril 2000, FINAL A5-0106/2000, p. 10).

### *2. Obligation de collaboration avec les autorités publiques compétentes*

**526.** En même temps, la directive permet aux États membres d'imposer aux prestataires "l'obligation d'informer promptement les autorités publiques compétentes d'activités illicites alléguées qu'exerceraient les destinataires de leurs services ou d'informations illicites alléguées que ces derniers fourniraient ou de communiquer aux autorités judiciaires compétentes, à leur demande, les informations permettant d'identifier les destinataires de leurs services avec lesquels ils ont conclu un accord d'hébergement" (art. 15, 2). Ainsi, les prestataires seraient tenus de se comporter de manière responsable, en faisant diligence dès l'instant où ils ont connaissance d'infractions et en collaborant avec les autorités judiciaires. Si ces obligations sont effectivement imposées dans les divers États membres, il nous paraît que le système ne peut alors s'analyser comme un encouragement à la passivité, au "laisser-faire" et à l'insouciance.

#### *a) Obligation d'information concernant les activités illicites*

**527.** L'obligation, à charge des prestataires de services, de porter à la connaissance des autorités publiques compétentes les activités supposées illicites est déjà de mise en Belgique. En effet, un protocole de collaboration a été signé le 28 mai 1999 entre l'ISPA (*Internet Service Provider Association*) et les ministres de la justice et des télécommunications[625]. Cet accord de collaboration élargit les compétences de l'ancien point "pornographie enfantine" de la police judiciaire à toutes les infractions commises via l'internet et le rebaptise "point de contact central de la *computer crime unit* nationale de la police judiciaire", dénommé aussi, en abrégé, "le point de contact judiciaire central". Les signataires de l'accord soulignent, dans l'exposé des motifs, qu'une bonne collaboration entre les ISP et les services judiciaires et policiers nécessite une communication rapide et efficace, qu'il est indiqué, à cet effet, d'utiliser le canal de l'internet comme moyen de communication et que la méthode la plus appropriée est l'instauration d'un point de contact central (considérant n° 9). L'article premier de l'accord précise, à juste titre, que la procédure de collaboration ne concerne que les communications publiques d'informations via l'internet. Il n'appartient donc pas aux ISP de s'informer du contenu d'une communication privée telle qu'un courrier électronique à caractère privé, un "chat" privé ou un site web dont l'accès est limité.

---

[625] Le "Protocole de collaboration pour lutter contre les actes illicites sur l'internet" est disponible sur le site de l'ISPA à l'adresse suivante : www.ispa.be/fr/c040202.html. Ce protocole d'accord s'ajoute au code de conduite de l'ISPA, disponible à l'adresse www.ispa.be/fr/c040201.html.

Par ailleurs, poursuit la même disposition, "l'objectif n'est pas que l'ISP passe activement internet au crible afin d'y repérer des éventuels contenus illicites. Il n'appartient pas aux ISP de vérifier et de qualifier tout contenu mis à disposition du public par l'internet, que ce soit par ses propres serveurs ou via les serveurs d'autres ISP. Ce n'est que si l'ISP constate un contenu présumé illicite ou qu'un utilisateur attire son attention sur un tel contenu, que l'ISP en informera le point de contact judiciaire central". Ce principe nous apparaît en parfaite conformité avec la règle déposée dans l'article 15, 1, de la directive sur le commerce électronique (absence d'obligation de surveillance), en même temps qu'il jette les bases pour une mise en œuvre de l'article 15, 2 (en son premier volet). Les articles 2 et suivants de l'accord précisent et détaillent les modalités de la procédure de collaboration.

L'article 2 s'intéresse à l'utilisateur de l'internet qui "*peut* [!] dénoncer le contenu présumé illicite via un courrier électronique (contact@gpj.be) adressé directement au point de contact judiciaire central ou s'adressant à son ISP". Pour que cette possibilité soit effective, ce dernier est tenu d'assurer, via son website, la publicité du point de contact central ainsi que de l'adresse électronique de l'ISP à laquelle des dénonciations peuvent être adressées (art. 2, *in fine*).

**528.** La disposition clé de l'accord est sans conteste l'article 3, qui fait *obligation* (!) à l'ISP d'informer le plus rapidement possible le point de contact judiciaire central du contenu présumé illicite dont il a connaissance via un courrier électronique (contact@gpj.be).

Comme le précise l'article 3, alinéa 2, "l'ISP, ainsi que l'utilisateur d'internet, peuvent utiliser le formulaire standardisé qui est proposé par le point de contact central et disponible sur son site (www.gpj.be)".

L'article 4, alinéa 1er, dispose que "l'utilisateur ou l'ISP, selon le cas, reçoivent dans les 24 H après réception un accusé de réception du point de contact judiciaire central, sauf si la dénonciation a été faite de manière anonyme"[626].

Il appartient au point de contact judiciaire central de décider de la prise en considération du contenu présumé illicite. S'il estime qu'il ne s'agit manifestement pas d'un contenu illicite, le contenu ne sera pas pris en

[626] "Cet accusé de réception est adressé par courrier électronique ou par télécopieur et indique uniquement que l'information a bien été reçue (avec indication de la date et de l'heure)" (art. 4, al. 2).

considération (art. 5) ; dans le cas contraire, il transmettra le dossier au parquet compétent (art. 6, al. 1er), auquel cas l'ISP ou l'utilisateur, selon le cas, et l'ISPA en sont informés dans les meilleurs délais (art. 6, al. 2).

Parmi les points essentiels de l'accord, l'article 7 mérite également d'être épinglé : "Les ISP s'engagent à collaborer avec les services judiciaires, à attendre leurs indications et à s'y conformer. Si le contenu visé est *présumé* constituer une infraction en matière de pornographie enfantine, dès qu'ils sont informés de la prise en considération du dossier par le point de contact judiciaire central, les ISP s'engagent à bloquer, par tous les moyens dont ils peuvent raisonnablement disposer, l'accès au contenu illicite, sauf indication contraire explicite des services judiciaires"[627].

**529.** Globalement, le protocole de collaboration – présenté ici dans les grandes lignes – paraît satisfaisant et anticipe la mise en œuvre du premier volet de l'article 15, 2, de la directive. Au titre de ses points forts, on relève le fait qu'il a été négocié sur une base volontaire entre les parties concernées, ce qui est de nature à favoriser son application loyale. Cela étant, nous sommes d'avis qu'il convient d'inscrire expressément dans la loi de transposition de la directive, cette obligation, pour les prestataires de services, d'informer promptement les autorités publiques compétentes des activités présumées illicites dont ils prennent connaissance par eux-mêmes ou qui leur sont renseignées. Mais rien n'empêche – tout au contraire (cf. le considérant n° 40 de la directive) – que les modalités de mise en œuvre de pareille obligation légale soient arrêtées dans le cadre d'un accord volontaire négocié (co-régulation).

Néanmoins, l'accord devrait être revu, selon nous, afin d'y intégrer une procédure, soigneusement formalisée, de notification, de retrait et de blocage[628]. L'élaboration de ce genre de mécanismes est explicitement recommandée par la directive sur le commerce électronique, qui plus est, de préférence, dans le cadre d'une auto- ou co-régulation (cf. considérants n° 40 et n° 46, *in fine*). Ainsi serait-il possible d'accroître les ambitions et la portée de l'article 7 du protocole d'accord. En effet, sur le plan des principes, on comprend mal pourquoi l'engagement de blocage de l'accès au contenu illicite devrait se limiter au cas des infractions en matière de pornographie enfantine. A bien y réfléchir, il paraît sage, pour l'heure, de se limiter à cette hypothèse où il est aisé pour un service de police

[627] Souligné par nous. Le libellé de cette disposition est maladroit en ce que celle-ci semble établir une présomption de culpabilité, alors que prévaut, en notre droit pénal, le principe inverse de la présomption d'innocence. Il eut mieux valu envisager le cas où le contenu apparaît *prima facie* constitutif d'une infraction…

[628] Il est prévu, du reste, que l'accord fasse l'objet d'une évaluation régulière par toutes les parties (art. 8).

judiciaire d'apprécier l'activité dénoncée comme illicite, à la différence d'autres situations (infraction à des droits intellectuels, diffamation…). Mais, enfin !, l'article 7 aurait déjà pu envisager d'autres cas pareillement faciles à traiter, tels que le blocage d'un site révisionniste renseigné comme tel !

Toujours est-il qu'il convient à présent de négocier des procédures plus ambitieuses et mieux élaborées de notification et de retrait, notamment afin d'assurer une transposition satisfaisante du nouveau régime de responsabilité (limitée) institué au profit de l'activité d'hébergement (art. 14 ; spéc. le § 3, *in fine*) et de rencontrer les difficultés pratiques que ce régime suscite (à ce propos et sur la teneur de ces procédures, voy. *infra*, n$^{os}$ 536 et s., notre commentaire de l'article 14).

**530.** L'accord de collaboration existant nous paraît être le cadre idéal pour arrêter ces procédures. A moins de prévoir une délégation au Roi pour définir celles-ci, sur proposition conjointe des ministres qui ont dans leurs attributions les Affaires économiques, la Justice et les Télécommunications. Dans ce cas, il convient que cet arrêté précise :

> 1° les mentions devant figurer dans la notification d'un plaignant et la forme que cette dernière doit revêtir ;
> 2° les modalités du droit reconnu au destinataire du service d'hébergement interpellé d'adresser une contre-notification au prestataire d'hébergement et les mentions devant figurer sur celle-ci ;
> 3° les délais de réaction laissés aux divers intervenants ;
> 4° les modalités de mise en œuvre des mécanismes, rapides et fiables, permettant le retrait des informations illicites ou le blocage des accès à ces dernières ;
> 5° les éventuelles sanctions civiles applicables en cas de notification manifestement intempestive et non fondée.

Si la voie de l'arrêté royal est choisie, il paraît souhaitable que le ministre le plus diligent consulte au préalable le Conseil de la Consommation, la Commission de protection de la vie privée et, au moins, une association représentative des prestataires intermédiaires. Ces consultations apparaissent comme le minimum qui puisse être fait en ce sens dès lors que la directive recommande, de manière particulièrement appuyée, que des mécanismes rapides et fiables de notification et de retrait soient "élaborés sur la base d'accords volontaires négociés entre toutes les parties concernées"! (Cf. l'art. 14, 3, *in fine*, et les considérants n° 40 et n° 46, *in fine*, de la directive).

*b) Obligation d'information concernant l'identité des clients*

**531.** Quant à l'obligation qui peut être imposée aux hébergeurs de communiquer aux autorités judiciaires l'identité de leurs clients, on signale que la récente loi du 28 novembre 2000 relative à la criminalité informatique établit, d'ores et déjà, les règles et délais de conservation, par les opérateurs et fournisseurs de services de télécommunications, des données d'identification d'utilisateurs de services de télécommunications, en vue de l'investigation et de la poursuite d'infractions pénales[629].

### *3. Obligation de surveillance dans des "cas spécifiques"*

**532.** Le considérant n° 47 apporte une précision importante concernant la portée de l'article 15, 1 : "l'interdiction pour les États membres d'imposer aux prestataires de services une obligation de surveillance ne vaut que pour les obligations à caractère *général*. Elle ne concerne pas les obligations de surveillance applicables à un cas *spécifique* et, notamment, elle ne fait pas obstacle aux décisions des autorités nationales prises conformément à la législation nationale". Nonobstant l'interdiction de l'article 15, 1, les "autorités nationales" peuvent donc enjoindre aux prestataires intermédiaires d'effectuer une surveillance et des contrôles dans des "cas spécifiques". Ainsi, le ministère public ou un service de police pourrait-il exiger qu'un intermédiaire surveille l'évolution d'un site web ou d'un groupe de discussions, voire même les faits et gestes d'un suspect particulier, à condition que cette dernière possibilité soit prévue par la loi (voy., notamment, la législation belge en matière d'écoutes téléphoniques)[630].

En toute hypothèse, à peine de contredire l'article 15, 1, le rôle de prévention des intermédiaires devrait être conçu de manière relativement étroite : seuls peuvent être imposés des contrôles ciblés et temporaires de sites, de groupes de discussion, etc., dûment identifiés, afin d'empêcher ou de combattre une activité illicite particulière[631].

---

[629] Loi du 28 novembre 2000 relative à la criminalité informatique (*M.B.*, 3 février 2001, p. 2909), article 14 complétant l'article 109*ter*, E, de la loi du 21 mars 1991 portant réforme de certaines entreprises publiques économiques.

[630] En ce sens, A. STROWEL, N. IDE et F. VERHOESTRAETE, "La directive du 8 juin 2000 sur le commerce électronique: un cadre juridique pour l'internet", *J.T.*, n° 6000, 2001, p. 142, n° 36. L'éventualité signalée au texte est à rapprocher de certaines dispositions (voy. not. les art. 9 et 12) de la loi du 28 novembre 2000 relative à la criminalité informatique (*M.B.*, 3 février 2001, p. 2909).

[631] Cf. le commentaire article par article, p. 31.

### *4. Mesures provisoires*

**533.** La directive précise très clairement que les exonérations prévues par les articles 12 à 14 "sont sans préjudice de la possibilité d'actions en cessation de différents types. Ces actions en cessation peuvent notamment revêtir la forme de décisions de tribunaux ou d'autorités administratives exigeant qu'il soit mis un terme à toute violation ou que l'on prévienne toute violation, y compris en retirant les informations illicites ou en rendant l'accès à ces dernières impossible" (considérant n° 45 et les art. 12, 3; 13, 2 et 14, 3). En d'autres termes, les régimes des articles 12 à 14 sont sans incidence sur les actions visant à obtenir des mesures de cessation ou d'interdiction. En Belgique, on songe aux actions en référé (les plus fréquentes à ce jour sur ces questions), ainsi qu'aux actions en cessation civiles[632] ou commerciales[633]. [634]

### *5. La charge de la preuve*

**534.** Qui doit établir que sont réunies les conditions de l'exonération des prestataires intermédiaires ? L'hésitation est permise. On peut soutenir que l'exonération pour les activités concernées est de principe et qu'il incombe dès lors au demandeur en justice d'administrer la preuve qu'une des conditions fait défaut. Par exemple, il aurait à prouver que le prestataire d'hébergement n'ignorait pas la présence sur ses machines d'un contenu litigieux et n'a rien fait pour le retirer ou rendre l'accès à celui-ci impossible. Mais on peut très bien raisonner à l'inverse et tenir que c'est au prestataire à démontrer qu'il satisfait aux conditions lui permettant de bénéficier d'un régime de faveur. Le dilemme est le suivant : "exonération de principe, sauf au demandeur à prouver que les conditions ne sont pas satisfaites" ou "exonération de principe si, et seulement si, le prestataire parvient à établir qu'il remplit les conditions". On ne trouve nulle part trace d'un commencement de réponse à cette question, capitale s'il en est.

**535.** Nous sommes portés à penser, pour notre part, que la première thèse est plus conforme à la volonté (probable) du législateur européen et plus satisfaisante sur le plan de la technique juridique. Cette opinion s'appuie sur deux arguments.

---

[632] Atteintes aux lois sur le droit d'auteur, sur la protection des programmes d'ordinateur ou sur la protection des bases de données.

[633] Atteintes à la loi du 14 juillet 1991 sur les pratiques du commerce et sur l'information et la protection du consommateur, *M.B.*, 29 août 1991.

[634] Sur ces diverses mesures provisoires, voir *infra*, le commentaire de l'art. 18.

Le premier est tiré du libellé des articles 12 à 14: tels que rédigés, ceux-ci semblent consacrer une "irresponsabilité, sauf si…", plutôt qu'une "responsabilité, sauf si…".

Le second argument est d'ordre technique: la thèse retenue fait peser sur la victime la charge de prouver que l'opérateur de réseau ou le fournisseur d'accès était à l'origine des informations transmises ou les a modifiées, ou encore que le prestataire d'hébergement savait qu'il hébergeait un contenu illicite. En toute hypothèse, cette preuve "positive" ne paraît pas insurmontable. Ainsi, le plaignant établira assez facilement que l'hébergeur *savait* car il avait formellement notifié à ce dernier la présence sur son serveur du contenu litigieux. Bien entendu, il aura pris soin de se ménager une preuve de son intervention (on voit, ici aussi, l'intérêt d'une procédure un tant soit peu formalisée "de notification et de retrait"). Par contre, en privilégiant la seconde thèse, on place le prestataire en situation de devoir administrer une *preuve négative* : il ne savait pas, il n'a pas modifié l'information transportée…, ce qui n'est jamais une solution heureuse en droit de la preuve.

## II. COMMENTAIRE ANALYTIQUE DES ARTICLES 12 À 14

### A. L'activité de "simple transport"

**536.** L'article 12 prévoit une exonération de responsabilité pour les activités de transport de l'information et de fourniture d'un accès au réseau de communication, *"à condition que le prestataire :*

> *a) ne soit pas à l'origine de la transmission ;*
> *b) ne sélectionne pas le destinataire de la transmission ; et*
> *c) ne sélectionne et ne modifie pas les informations faisant l'objet de la transmission".*

Les activités visées ici englobent le stockage automatique, intermédiaire et transitoire des informations transmises, pour autant que ce stockage serve exclusivement à l'exécution de la transmission sur le réseau de communication et que sa durée n'excède pas le temps raisonnablement nécessaire à la transmission (art. 12, 2). Autrement dit, est couvert par l'exonération le stockage furtif réalisé au cours et pour les besoins de la transmission, à ne pas confondre avec le stockage effectué à la demande et pour le compte d'un destinataire du service (art. 14), ni avec le stockage automatique, intermédiaire et temporaire de copies

d'informations (sur des sites dits "miroirs") aux seules fins de faciliter les consultations ultérieures (*system caching* visé à l'art. 13).

**537.** L'article 12 relatif aux services de transport et d'accès au réseau, à lire en combinaison avec l'article 15, consacre la thèse de la neutralité des prestataires concernés. Si ces derniers se limitent, respectivement, à l'activité de transport ou d'offre d'un accès au réseau, entendue *stricto sensu*[635], ils échappent à toute responsabilité du chef d'information illicite ou non conforme. Ces activités ne comportent aucune obligation *générale* de surveillance des informations circulant sur le réseau, ni aucune obligation de recherche active et systématique d'indices d'activités illicites, ni aucune obligation particulière de mettre en place des dispositifs de filtrage ou de faire diligence pour supprimer des informations renseignées comme illicites ou pour bloquer l'accès à des sites contraires à l'ordre public, ni aucune obligation de sensibilisation ou d'information des abonnés…

On peut affirmer que la directive exonère de toute responsabilité les opérateurs de réseau et fournisseurs d'accès agissant *qualitate qua*. Sans préjudice des possibilités d'actions au provisoire, leur responsabilité ne peut être mise en cause, ni au pénal, ni au civil, alors même, par exemple, qu'ayant connaissance de la présence d'informations illicites sur le réseau et ayant prise sur ces dernières, ils s'abstiennent d'intervenir. L'exonération pour le "simple transport" suppose que le prestataire n'est impliqué en aucune manière dans l'information transmise (considérant n° 43) ; elle ne bénéficie pas au prestataire qui collabore *délibérément* avec l'un des destinataires de son service (considérant n° 44). Cette solution procède manifestement d'un souci de prévenir toute forme de contrôle et de censure de leur part : les opérateurs de réseaux et fournisseurs d'accès se doivent d'être neutres à l'égard des contenus diffusés et de n'interférer en aucune manière. L'écart par rapport au droit commun est notable car on imagine sans difficulté des hypothèses où une responsabilité aurait pu être retenue par application des critères usuels[636].

---

[635] Cf. les conditions a), b) et c) de l'article 12, §, 1er, et le second paragraphe de l'article 12.

[636] A titre d'illustration, voy. Tribunal d'instance (*Amtsgericht*) de Munich, 28 mai 1998, 8340 Ds 465 ; Js 173158/95 ; *Bulletin d'actualité du Lamy droit de l'informatique et des réseaux*, n° 105, juillet 1998, p. 22 et le commentaire de R. VOGEL et S. DELAHAIE, "La décision allemande *'Compuserve'* : la première condamnation d'un fournisseur d'accès à l'Internet", in *Cahiers-Lamy droit de l'informatique et des réseaux*, n° 106, août-septembre 1998, p. 4. Ce jugement a été réformé en appel par la *Landgericht* de Munich, 8 décembre 1999, qui a acquitté le directeur de *Compuserve* (Allemagne), condamné à une peine de deux ans d'emprisonnement avec sursis en premier ressort pour avoir facilité l'accès à des *news groups* à contenu pédophile hébergés aux États-Unis par *Compuserve Inc.*

Les conditions de l'article 12 sont si strictes que la responsabilité des opérateurs de réseau et fournisseurs d'accès pourra rarement être mise en cause. Il n'est donc pas exagéré de considérer que l'on a affaire, en pratique, à une quasi immunité pour l'activité de "simple transport"… et à une quasi impunité sur le plan pénal.

### B. L'activité d'hébergement

**538.** La fonction d'hébergement concerne le stockage et le traitement d'informations à la demande du destinataire du service sur le système du prestataire. Aux termes de l'article 14, aucune responsabilité ne peut être engagée pour cette activité, *"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".*

L'article 14, loin d'instituer une exonération totale au profit du prestataire d'un service d'hébergement, se contente de limiter les causes de responsabilité. Ce faisant, il ne fait que préciser "à la baisse" la diligence due par ce prestataire, suivant un critère relativement raisonnable.

#### *1. Les conditions d'exonération*

**539.** Il résulte de la combinaison des articles 14 et 15 de la directive que la responsabilité du prestataire d'hébergement ne peut être engagée *que* s'il a une connaissance effective d'activités illicites *et* n'agit pas "promptement" pour retirer les informations ou rendre l'accès à celles-ci impossible.

Contrairement à l'exonération pour simple transport, qui est subordonnée à une exigence d'abstention dans la transmission de l'information, un devoir d'intervention incombe à l'hébergeur. Dès l'instant où celui-ci est informé de la présence d'informations illicites sur l'un de ses serveurs, il doit jouer un rôle actif: il est tenu de faire diligence, d'agir "promptement", pour retirer les informations illicites ou bloquer l'accès à celles-ci.

**540.** Remarquons que le degré de connaissance requis pour justifier un devoir d'intervention dans le chef de l'hébergeur n'est pas formulé de la même manière en matière d'action pénale (nécessité d'une "connaissance effective") et en matière d'action en responsabilité civile (il suffit que l'intermédiaire ait "connaissance de faits ou de circonstances selon lesquels l'activité ou l'information illicite est apparente"). La portée de cette distinction est toutefois relativement obscure. Selon une opinion, la connaissance pourrait résulter, dans la seconde hypothèse, d'une notification moins formelle que dans la première, ou naître de circonstances autres que la notification[637]. On reviendra sur ce point au moment de souligner l'intérêt des procédures de notification et de retrait (*infra*, n° 545).

**541.** Apparemment, aucune autre obligation positive n'est mise à charge du prestataire d'hébergement: ni obligation générale de surveillance, ni obligation d'effectuer un minimum de coups de sonde, ni obligation de mettre en place des procédures de sécurité ou de filtrage, ni obligation de conseil particulière…

Cependant cette interprétation paraît incertaine à la lecture du considérant n° 48, libellé comme suit : "*La présente directive n'affecte en rien la possibilité qu'ont les États membres d'exiger des prestataires de services qui stockent des informations fournies par des destinataires de leurs services qu'ils agissent avec les précautions que l'on peut raisonnablement attendre d'eux et qui sont définies dans la législation nationale, et ce, afin de détecter et empêcher certains types d'activités illicites*".

Par sa rédaction floue et imprécise, ce considérant sème une certaine confusion. En paraissant ouvrir la voie à l'instauration légale de contrôles *a priori*, nous pensons qu'il met à mal l'économie générale du régime institué par les articles 14 et 15.

A défaut de précisions supplémentaires, cette dernière éventualité porte en germe un risque de glissement vers la généralisation d'un contrôle *a priori*, d'une censure élargie, d'une part, et vers une objectivation de la responsabilité des hébergeurs, d'autre part.

En effet, pour éviter la mise en cause de leur responsabilité, ces derniers seront portés, en cas de doute, à supprimer les contenus apparemment

[637] Cf. A. STROWEL, N. IDE et F. VERHOESTRAETE, *op. cit.*, p. 143, n° 44.

illicites. Par ailleurs, en présence d'un contenu illicite non détecté, grande pourrait être la tentation des cours et tribunaux de "découvrir", le cas échéant, une faute dans le chef du prestataire : placement d'un filtre inefficace, recours à une technologie obsolète, choix contestable des mots clés retenus… Dès l'instant où la faute est supposée, plus que démontrée sur la base d'une appréciation effective du comportement du défendeur, force est d'admettre que la responsabilité s'objectivise.

En réalité, dans le mesure où ce considérant ne peut être interprété en un sens contraire à une disposition du corps de la directive, en l'occurrence l'article 14, il y a lieu d'estimer que la transgression des obligations qu'il permet d'imposer ne peut être sanctionnée au plan de la responsabilité. D'autres sanctions devraient être prévues, telles des amendes par exemple[638].

### *2. Difficultés d'interprétation*

**542.** Plus fondamentalement, le critère de responsabilité formulé par l'article 14 risque de susciter quelque difficulté d'appréciation. Comme tel, il suppose dans le chef du prestataire d'hébergement une compétence juridique qu'il n'a pas et ne doit pas avoir. On le somme pratiquement de se substituer au juge dans l'appréciation des contenus qui lui sont renseignés comme illicites. Il est piquant de constater qu'en prétendant manifestement lui épargner un rôle de *censeur*, le législateur européen n'a pas réussi à éviter de l'ériger en *juge*. Deux exemples peuvent suffire à illustrer la difficulté.

Supposons qu'un prestataire soit informé du fait qu'il héberge un site contenant des textes ou des images portant atteinte aux droits d'auteur du plaignant. Interpellé, l'éditeur du site fait valoir que les œuvres litigieuses sont évoquées dans le cadre du droit de citation. Si le juge saisi de l'affaire décide que la reproduction excédait effectivement les limites du droit de citation, la responsabilité du prestataire d'hébergement doit-elle être mise en cause au motif qu'il aurait eu tort de continuer d'héberger le site ? On pourrait multiplier des exemples similaires[639]. Ainsi, l'attention

[638] Selon un avis officieux recueilli auprès de la Commission européenne.

[639] Voir, par exemple, en jurisprudence belge, le jugement rendu par le tribunal de commerce de Bruxelles le 2 novembre 1999 dans une affaire opposant l'ASBL IFPI et la SA Polygram à la SA Belgacom Skynet. Il est reproché au défendeur de ne pas avoir supprimé les liens établis à partir de deux sites hébergés par ses soins vers des sites contenant des fichiers MP 3, alors qu'il "a été mis au courant d'activités suspectes". On s'interroge sur le bien-fondé de cette décision, dès lors que le défendeur ne pouvait être certain que le contenu du site lié était effectivement illicite. En ce sens, le commentaire de S. MALENGREAU à l'adresse http://www.droit-technologie.org (décision reproduite dans son intégralité).

d'un serveur peut être attirée sur la circonstance qu'il héberge des informations à caractère diffamatoire. Peut-il être reproché au serveur de s'être abstenu de les supprimer alors qu'il a pu estimer qu'elles ressortissaient à la liberté d'expression, qui inclut, dans une certaine mesure, un droit de critique, de polémique, etc. ?[640] Il faut remarquer combien la position du fournisseur d'hébergement peut être inconfortable : il peut lui être reproché par des tiers de ne pas avoir supprimé des informations litigieuses afin de limiter l'atteinte à leurs droits, mais il peut aussi lui être reproché par ses clients d'avoir effacé à tort des informations parfaitement licites. Il doit *agir vite*, au risque d'engager sa responsabilité extra-contractuelle envers les tiers lésés, *sans agir trop vite*, au risque d'engager sa responsabilité contractuelle envers ses clients.

**543.** À notre avis, il eut été préférable de distinguer les infractions *flagrantes* (ou *manifestement* illicites : images pédophiles, contrefaçon évidente, violation indiscutable d'un secret, propos incontestablement outrageants…), d'une part, et ce qui peut prêter à controverse ou à discussion, d'autre part. Ainsi, la responsabilité du fournisseur d'hébergement ne serait retenue qu'à la triple condition qu'il ait eu connaissance de la présence sur son serveur d'un contenu litigieux, que ce dernier ait été *manifestement* illicite et qu'il ait fait preuve d'inertie[641]. Tel est le cas, par exemple, d'un site à contenu révisionniste, qui est de toute évidence en défaut par rapport à la loi[642]. Une autre issue satisfaisante – et qui s'imposera vraisemblablement – serait d'interpréter le texte de l'article 14 de façon raisonnable. Concrètement, on considérerait qu'il ne prescrit pas au prestataire d'hébergement d'intervenir de façon *mécanique* – en procédant nécessairement et sans délai à la fermeture ou au blocage du site renseigné comme illicite –, mais lui enjoint de faire toutes diligences pour préserver les droits des tiers dans une mesure proportionnelle à la gravité de l'atteinte[643].

---

[640] Pour un exemple en jurisprudence belge, voy. Civ. Bruxelles (réf.), 2 mars 2000, inédit (propos injurieux, diffamatoires et calomnieux se référant à un homme politique et tenus dans le cadre d'un groupe de discussion hébergé par le second défendeur). Cette ordonnance illustre la difficulté d'appréciation pour le juge des référés, qui doit se borner à juger de l'apparence des droits, par une mise en balance des intérêts en présence, sans se prononcer définitivement sur le fond. On imagine *a fortiori* l'embarras d'un prestataire d'hébergement qui n'a pas la formation, ni la compétence, d'un magistrat, pour apprécier le bien-fondé des plaintes qui lui sont adressées.

[641] Rappr. V. SÉDALLIAN, *Droit de l'Internet*, Collection AUI, 1997, p. 120.

[642] Loi du 23 mars 1995 tendant à réprimer la négation, la minimisation, la justification ou l'approbation du génocide commis par le régime national-socialiste allemand pendant la Seconde Guerre mondiale, *M.B.*, 30 mars 1995, p. 7996. Une législation similaire existe aussi, notamment, en France, en Allemagne, en Autriche et en Suisse.

[643] Rappr. N. MALLET-POUJOL, note sous Paris, 10 février 1999, *op. cit.*, p. 392. On s'avise que la décision à prendre peut présenter, dans certains cas, une réelle difficulté d'appréciation.

Il est vraisemblable que l'article 14 sera transposé tel quel en droit interne. En ce cas, il serait utile que les critères d'interprétation suggérés ici figurent dans l'exposé des motifs de la loi de transposition.

**544.** L'insécurité juridique tient également à l'imprécision de l'article 14 quant au seuil de connaissance requis dans le chef de l'hébergeur : pour considérer qu'il savait (et devait donc agir, sous peine d'engager sa responsabilité), suffira-t-il d'une simple dénonciation anonyme (par exemple, auprès du prestataire et du Parquet, ou via le point de contact central) ou d'une information à caractère public (telle une mention dans la presse), ou faudra-t-il une réclamation plus formelle ? La notification d'un plaigant doit-elle contenir des informations déterminées et quels sont les délais de réaction laissés au prestataire d'hébergement?

Pour répondre à ces interrogations et apporter une meilleure sécurité juridique, il nous paraît indispensable d'arrêter des procédures de notification et de retrait (*notice and take down*), ainsi que le recommande avec insistance la directive (art. 14, 3, *in fine* ; art. 21, 2; considérants n$^{os}$ 40, 41 et 49)[644]. Pareilles procédures fixent les conditions auxquelles doit satisfaire une notification et les modalités du retrait du contenu à respecter par l'intermédiaire.

**545.** A titre d'illustration (et d'inspiration !), on peut mentionner l'exemple américain du *Digital Millenium Copyright Act* de 1998 évoqué précédemment. Pour rappel, ce texte légal prévoit, pour quatre activités intermédiaires, une exonération de responsabilité, sous certaines conditions et dans le seul cas de la violation de droits d'auteurs.

Ce qui nous intéresse ici, c'est que ce texte met en place une procédure de *"notice and take down"*[645]. Pour pouvoir bénéficier de l'exonération de responsabilité, l'ISP est tenu de désigner un agent chargé de recueillir les notifications des plaignants. Ceux-ci adressent à l'agent un document

---

[644] Voir aussi le commentaire article par article, pp. 30-31 : "Ce principe, énoncé au deuxième tiret du paragraphe [il s'agit de l'art. 14, 1, point b, dans la rédaction définitive de cette disposition], constitue une base adéquate sur laquelle différentes parties intéressées peuvent effectivement mettre en place des procédures permettant de notifier au prestataire de services des informations qui sont à l'origine d'une activité illicite, et d'obtenir le retrait de ces informations ou une interdiction d'accès (procédures parfois appelées "procédures de notification et de retrait" – "notice and take down procedures"). On soulignera néanmoins que ces procédures ne se substituent pas aux voies de recours judiciaires existantes et ne sauraient le faire. La Commission encourage activement des systèmes d'autoréglementation, y compris l'établissement de codes de conduite et de lignes directes".

[645] Pour une description de cette procédure, voir A. STROWEL et N. IDE, "Responsabilité des intermédiaires : actualités législatives et jurisprudentielles", disponible sur internet (www.droit-technologie.org), p. 20.

écrit et signé qui doit comporter diverses mentions : une identification de l'œuvre contrefaite et du contenu contrefaisant, sa localisation sur le réseau, une déclaration que l'usage du défendeur est illicite et une déclaration sous serment concernant la véracité des informations contenues dans la notification. Si, après avoir reçu cette déclaration, l'ISP ne réagit pas rapidement, il peut se voir condamné à des dommages et intérêts dans le cadre d'une procédure au fond. S'il conteste la validité de la mise en demeure, l'abonné interpellé peut adresser à l'ISP une contre-notification, soumise, elle aussi, à de strictes exigences légales. L'ISP transmet cette contre-notification au plaignant et l'avertit qu'il va replacer le contenu litigieux sur le site dans un délai de 10 jours. Durant ce laps de temps, le plaignant peut introduire une action en référé pour obtenir une mesure d'interdiction, à défaut de quoi l'ISP doit replacer le contenu sur le site (dans un délai de 10 à 14 jours à compter de la contre-notification).

Semblable procédure présente divers avantages et permet de rencontrer les préoccupations exposées plus haut : elle est de nature à inciter l'ISP à procéder rapidement au retrait du contenu renseigné comme contrefaisant car ainsi, il se trouve exonéré de toute responsabilité non seulement à l'égard de la victime de la contrefaçon, mais aussi à l'égard de son abonné (qui pourrait rechercher sa responsabilité pour mauvaise exécution du contrat d'hébergement).

### C. L'activité de stockage sous forme de "cache"

**546.** L'article 13 concerne le stockage temporaire des copies de sites et services souvent consultés sur des serveurs relais mis en place par les fournisseurs d'accès. Cette technique, dite de "cache", permet d'améliorer les temps de connexion à des sites éloignés, et ainsi de désengorger les réseaux et accroître leurs performances. Le prestataire est exonéré pour ce type d'activité, *"à condition que :*

> *a) [il] ne modifie pas l'information,*
> *b) [il] se conforme aux conditions d'accès à l'information,*
> *c) [il] se conforme aux règles concernant la mise à jour de l'information, indiquées d'une manière largement reconnue et utilisées par les entreprises,*
> *d) [il] n'entrave pas l'utilisation licite de la technologie, largement reconnue et utilisée par l'industrie, dans le but d'obtenir des données sur l'utilisation de l'information*
> *et*
> *e) [il] agisse promptement pour retirer l'information qu'il a stockée ou pour en rendre l'accès impossible dès qu'il a effecti-*

> *vement connaissance du fait que l'information à l'origine de la transmission a été retirée du réseau ou du fait que l'accès à l'information a été rendu impossible, ou du fait qu'un tribunal ou une autorité administrative a ordonné de retirer l'information ou d'en rendre l'accès impossible".*

Les observations formulées au point précédent peuvent être reprises, *mutatis mutandis*, en ce qui concerne la limitation de responsabilité prévue par l'article 13, 1, pour l'activité de stockage sous forme de cache. L'exonération est acquise pourvu que le prestataire s'en tienne strictement à son rôle et agisse promptement pour supprimer l'information ou bloquer l'accès à celle-ci dès que pareille mesure lui a été ordonnée par un tribunal ou une autorité administrative ou qu'il a une connaissance *effective* du caractère illicite de l'information (point e), sans préjudice des devoirs imposés sur pied de l'article 13, 2.

**547.** Outre cette obligation positive, certaines conditions additionnelles tiennent compte des particularités du *system caching*. Ainsi, les points a) et d) consacrent un devoir d'abstention dans le chef de l'intermédiaire : il ne peut influer sur les contenus transmis, ni entraver l'utilisation des systèmes techniques. Les points b) et c) l'oblige à respecter certaines règles, à savoir, respectivement, celles relatives aux conditions d'accès à l'information et celles concernant sa mise à jour régulière. Cette dernière exigence est particulièrement importante afin d'écarter le risque d'un préjudice supplémentaire pour la victime d'une atteinte à ses droits. Si cette dernière a obtenu que des informations lui portant préjudice (diffamatoires, attentatoires à sa vie privée…) soient retirées du site d'origine, il ne faudrait pas qu'elles demeurent accessibles sur des serveurs contenant des copies caches non mises à jour de ce site.

## CONSIDÉRATIONS FINALES

**548.** Sans doute convient-il de procéder à une transposition relativement littérale des articles 12 à 15, moyennant les aménagements formels qui s'imposent (cf. l'utilisation fréquente des expressions "Les États membres veillent à…", "Les États membres peuvent…", "conformément aux systèmes juridiques des États membres", etc.).

Néanmoins, afin de rencontrer les difficultés d'application soulevées ici et là et de favoriser la sécurité juridique, certains critères d'interprétation proposés pourraient figurer dans le commentaire article par article de la loi de transposition.

**549.** En ce qui concerne la responsabilité des fournisseurs de liens hypertextes et de services de moteur de recherche et d'annuaire, deux options sont possibles : soit l'on n'en souffle mot dans la loi de transposition (on sait que la directive n'en dit rien) de sorte que le droit commun s'y applique, en attendant une éventuelle future initiative en ce domaine (cf. art. 21, 2, de la directive), soit l'on choisit de déterminer, d'ores et déjà, un régime de responsabilité limitée pour ces activités (comparable à celui prévu pour l'activité d'hébergement) ? Le législateur espagnol s'oriente vers cette dernière solution (assez maladroitement, à vrai dire). Nous pensons, pour notre part, qu'il est préférable de ne pas régler ces questions dans la loi de transposition, afin d'éviter de se mettre en porte-à-faux par rapport à une intervention ultérieure du législateur européen. D'autant qu'entretemps, rien n'empêche les cours et tribunaux de raisonner par analogie avec le dispositif légal mis en place pour trancher les différends qui leur seraient soumis.

**550.** Nous pensons qu'il est souhaitable d'inscrire dans le texte de loi l'obligation pour les prestataires intermédiaires d'informer promptement les autorités compétentes d'activités ou d'informations illicites dont ils prennent connaissance (voy. la formulation de l'art. 15, 2).

Enfin, il paraît indispensable d'instaurer des mécanismes efficaces de notification et de retrait (*notice and take down*), destinés à faciliter la suppression rapide des contenus illicites sur les réseaux. Pareils mécanismes pourraient être négociés entre l'ISPA et les ministres concernés, par exemple dans le cadre d'une révision du protocole d'accord signé entre l'association et les ministres de la Justice et des Télécommunications. Mais ils pourraient aussi être arrêtés par le Roi, sur proposition des ministres concernés, et après que ceux-ci aient procédé à diverses consultations. Dans ce cas, il convient de prévoir une délégation au Roi dans la loi de transposition.