http : // www.droit-technologie.org

Présente :

La responsabilité délictuelle sur Internet en droit suisse

UNIVERSITÉ DE NEUCHÂTEL – FACULTÉ DE DROIT

These de licence
Sous la direction du Professeur Thomas Prosbt

Morgan Lavanchy

Session 2002

date de mise en ligne :10 mars 2003

UNIVERSITÉ DE NEUCHÂTEL - FACULTÉ DE DROIT

Thèse de licence

La responsabilité délictuelle sur Internet en droit suisse

Morgan Lavanchy

Sous la direction du Professeur Thomas Probst

Avant-propos

A travers le monde, la responsabilité relative à Internet est un sujet d'actualité brûlant. En témoignent les actes législatifs, les cas de jurisprudence mais aussi la doctrine, qui s'enrichit exponentiellement, les sites *web* des juristes férus d'Internet en apportant la preuve.
Comme trop souvent, la Suisse fait figure d'exception. Certes, suite à la motion Pfisterer, le Parlement devrait modifier notre Code pénal dans le but de clarifier la responsabilité des prestataires techniques d'Internet, mais cela ne concerne pas la responsabilité civile de ces derniers. En outre, le Tribunal fédéral n'a pas encore donné le moindre avis véritablement relevant concernant la responsabilité en ligne et la doctrine est peu abondante. La Suisse paraît être le pays occidental le plus vierge de contacts avec le sujet « interneto-juridique » qui a généré le plus d'effervescence médiatique. Quoiqu'il en soit, notre Helvétie rentrera dans les rangs tôt ou tard. En attendant ces jours, il nous semble intéressant de se lancer dans une tentative de détermination du régime juridique suisse de la responsabilité délictuelle sur Internet. Nous nous limiterons en effet à l'aspect civil de la responsabilité en ligne, même si le domaine pénal nous servira à certains égards de muse. Il nous permettra surtout de ressentir la « patte » suisse dans le domaine de la responsabilité sur Internet, la face pénale de celle-ci ayant été plus débattue par la doctrine suisse que la face civile. Les solutions échafaudées en droit pénal nous guideront aussi de par leurs analyses techniques d'Internet.

Si nous étudierons quelques cas de responsabilité extra-contractuelle plutôt marginaux, le cœur des développements touchera la responsabilité des prestataires techniques d'Internet pour les contenus illicites circulant sur ce vecteur de communication. En revanche, de manière générale, nous n'aborderons pas les questions, nombreuses, concernant la propriété intellectuelle et la concurrence déloyale.

Pour conclure cet avant-propos, je tiens à remercier les personnes qui m'ont apporté leur aide, même succincte, dans la rédaction de cette thèse de licence, notamment les Professeurs Jacques Savoy et Bertil Cottier.

Juin 2002 Morgan Lavanchy

Table des matières

Liste des abréviations

AG	Amtsgericht
al.	alinéa
AOL	America OnLine
art.	article
BGBl	Bundesgesetzblatt
c.	contre
CA	Cour d'appel
CDA	*Communications Decency Act*
cf.	se référer à (*confer*)
ch.	chambre
CCS	Code civil suisse
CEDH	Convention de sauvegarde des droits de l'homme et des libertés fondamentales du 4 novembre 1950
CO	Code des obligations du 30 mars 1911
CPS	Code pénal suisse
DMCA	*Digital Millenium Copyright Act*
éd.	édition
et al.	et autres
FAI	fournisseur d'accès à Internet
FDI	Forum des droits sur l'Internet
FF	francs français
GmbH	Gesellschaft mit Beschränkter Haftung
IETF	*Internet Engineering Task Force*
Inc.	Incorporated
JCP	Juris Classeur Périodique
LG	Landgericht
Lit.	littera
LSCPT	Loi fédérale sur la surveillance de la correspondance par poste et télécommunication du 6 octobre 2000
NJW	Neue Juristische Wochenschrift
OFJ	Office fédéral de la justice
op. cit.	dans l'ouvrage cité (*opus citatum*)
ord.	ordonnance
p.	page
par.	paragraphe
réf.	référé
RO	Recueil officiel
RS	Recueil systématique
RSN	Recueil systématique neuchâtelois
S.	Seite
TDG	Teledienstgesezt
TGI	Tribunal de grande instance
U.S.C.	United States Code
v.	versus
vol.	Volume

Partie 1 Introduction

A. Le « phénomène » Internet

Il est aujourd'hui presque inutile de présenter Internet, tant il est entré dans les mœurs planétaires. Ce réseau de communication international a enfanté des possibilités nouvelles d'expression et de création, d'éducation et de formation, d'échanges culturels et d'information, de jeu et de commerce. Il apporte un plus indéniable au bien-être de tout en chacun. Il semble incontestable qu'Internet a des conséquences autant importantes sur la vie sociale que le téléphone ou la révolution industrielle du 19e siècle, tant il a bouleversé les comportements de l'Homme. Cette mutation de la société est telle que l'on connaît déjà l'un des termes que les futurs historiens utiliseront pour désigner cette période charnière : révolution. Et les effets de cette révolution sont loin de se tarir. Internet conquiert des domaines toujours plus nombreux de notre quotidien. S'il est un phénomène, il n'est pas de mode et si personne ne saurait dire qu'il est entré à jamais dans nos vies, beaucoup pensent qu'il demeurera le point d'orgue des systèmes de télécommunication encore durant de nombreux siècles.
Mais toute chose a son mauvais pendant. Internet ne fait pas exception à la règle. Il n'est après tout qu'un instrument aux mains des individus et peut à cet effet être utilisé à mauvais escient. Les créateurs de cet outil n'ont songé qu'au bien qu'il pourrait amener et les techniciens qui gravitent aujourd'hui autour de la « toile » ne cherchent souvent qu'à en améliorer les performances. Par ce biais, ils encouragent bien involontairement les dérapages.
Dès le début des années 90, on a pu constater les risques d'abus liés à une utilisation incontrôlée du réseau des réseaux. Un sentiment de déresponsabilisation a entraîné une multiplication des dérives sur la « toile ». Nombre d'arnaques en tout genre s'y sont fait jour. L'inexpérience et l'excès de confiance de l'internaute lambda n'aident en rien. On sait qu'un homme averti en vaut deux ; sur le « net », un *hacker* en vaut mille. Mais les exemples les plus médiatisés touchent des domaines aussi scabreux que la pédophilie, le révisionnisme ou le terrorisme. Internet est devenu leur terrain de prédilection. Mais, ce qui rend Internet le plus dangereux, est l'inconscience des risques[1] que représente ce dernier. Inconscience du peuple et, plus fâcheux, des autorités. Or, une protection accrue des intérêts particuliers et de l'intérêt général est, non pas seulement la bienvenue, mais une nécessité. D'autant plus que tout en chacun peut être concerné par une atteinte découlant d'Internet. Nul besoin d'être un internaute. Les cas de diffamation en constituent un bon exemple.

Sur Internet, comme dans la vie réelle, la liberté est une notion fondamentale. Mais, on le sait, la liberté d'un individu s'arrête là où celle des autres commence. Et beaucoup outrepassent les limites du correct. Autant vertueux puissent devenir les citoyens du monde, l'enchaînement suivant trouvera toujours application : plus de « joueurs », plus d'atteintes. Ces dernières étant quasiment inévitables, la réparation du dommage n'en devient que plus importante. Et qui dit réparation, dit responsabilité.

---

[1] David ROSENTHAL, Les risques d'Internet - De la croyance à la réalité, résumé de l'étude TA « Internet – schöne neue Welt ? Der Report über die unsichtbaren Risiken », Conseil suisse de la science, Bern 1999, p. 18.

B. Les caractéristiques d'Internet

Afin de comprendre les développements qui suivront, il est nécessaire d'exposer quelques-unes des caractéristiques d'Internet, médium et moyen de communication unique en son genre. Ces singularités ont engendré le succès phénoménal que l'on connaît mais, depuis une dizaine d'années, génèrent des inquiétudes à foison.

1. Décentralisation

Les communications sur Internet sont décentralisées : elles ont lieu entre ordinateurs[2], propriétés de nombreux intervenants, et ne passent pas par un point unique[3]. Il n'y a pas d'administration centrale[4], qui contiendrait des centres d'archivage ou des organismes de contrôle des communications électroniques. Par ailleurs, de tels organismes seraient inefficaces, le volume de données échangées étant sans pareil. Seule la *National Security Agency*, le service de renseignements américain, a la prétention de contrôler tous les moyens de communication, y compris Internet, par l'entremise de son système « Echelon » : lors des attentats du 11 septembre 2001, les Etats-Unis ont pu malheureusement constater à leurs frais qu'une telle ambition était surréaliste.

2. Omniprésence

Internet a une dimension mondiale : il est un monde virtuel, qui dépasse les frontières géographiques et politiques. Il abolit la notion d'espace. On ne peut rattacher Internet à la notion de territoire, à l'inverse d'un journal publié dans tel pays. Les informations du *web* sont accessibles depuis n'importe quel endroit de la terre, tant évidemment qu'il y ait une connexion.
Le caractère global et transnational d'Internet constitue un défi pour toute la logique étatique, dont il met à mal les législations.

3. Anonymat

Il semblerait qu'Internet permette à quiconque de perpétrer anonymement les pires agissements. S'il est vrai qu'une certaine clandestinité prévaut sur Internet, nous aurons l'occasion de voir qu'il faut grandement relativiser cette idée, lorsque nous développerons le

---

2 Actuellement, il est aussi possible de « surfer » au moyen d'un téléphone mobile (grâce à la technologie WAP), d'un terminal Internet à peine plus grand qu'un agenda électronique ou d'une console de jeu. A quand Internet en arrière-fond de l'évier à vaisselle ?

3 Dans ce sens, Bruno GIUSSANI oppose les médias classiques de type « *broadcasting* », où il n'y a qu'un seul point d'émission, au « *networking* », médium dans lequel tout le monde est émetteur. Voir Bruno GIUSSANI, Pas de cybersexe sans capote, Webdo du 24 avril 2001, disponible à l'adresse suivante : http://www.webdo.ch/hebdo/hebdo_1996/hebdo_02/adf_02_ndi.html.

4 L'inverse est vrai pour un réseau fermé tel qu'un intranet. Un intranet est un réseau de télécommunication privé et local qui utilise les technologies d'Internet. Il est fermé parce qu'il est en général destiné à l'usage exclusif d'un organisme, une entreprise ou une université la plupart du temps. Il existe néanmoins parfois un passage entre l'intranet et Internet, contrôlé par un *firewall* : une personne de l'extérieur peut le cas échéant accéder à certaines ressources de l'intranet et inversement. Quoi qu'il en soit, la plupart des entreprises possédant un intranet ont un serveur qui stocke pendant un certains laps de temps les *e-mails* et autres mouvements relatifs à Internet.

thème des obligations à la charge du prestataire technique[5] et nous traiterons de la responsabilité du fournisseur de contenu[6].

4. Diversité et confusion des acteurs d'Internet

Le fonctionnement d'Internet nécessite la participation de nombreux « joueurs ». A priori, chacun a sa fonction, mais la réalité est tout autre : l'évolutivité du marché génère souvent un chevauchement des rôles. Un prestataire technique peut cumuler les rôles de prestataires de contenu, de transporteur, de fournisseur d'accès et d'hébergement[7] et un lecteur devient un auteur en plusieurs clics et tapotements sur son clavier, notamment par l'entremise des *newsgroups*[8].

5. Volatilité

En quelques instants et pour un coût risible, d'énormes quantités de données peuvent être transférées. S'il est repéré, le propriétaire d'un site hébergé sur un serveur basé dans un pays qui le tient pour illégal pourra le transférer sur un serveur situé dans un pays plus permissif.
Les injonctions des autorités judiciaires, même les mesures provisionnelles[9], se révèlent plus que souvent inutiles. En cas d'interdiction de diffuser un article ou des photos, quoi de plus simple que de les offrir sur un autre site ?

6. « *Effet multiplicateur* »[10]

Quelques caractéristiques techniques d'Internet vues ci-dessus sont telles, qu'elles accentuent la fréquence et l'intensité de nombreux comportements punissables et illicites. La fréquence, parce qu'Internet facilite la commission de certains actes, tout le monde pouvant s'adresser, presque sans coût, au monde entier par l'entremise de son site personnel par exemple : sur Internet, il est très difficile d'empêcher la divulgation d'une information[11]. L'intensité, parce que les atteintes sont quasi permanentes et le dommage d'autant plus grand, notamment en matière de droits de la personnalité. Une fois qu'une information illicite est sur le *web*[12], notamment une photo, elle ne le quitte généralement plus : sa dissémination subséquente et son accessibilité à des centaines de millions d'internautes est inévitable. On comprend que le dommage est démesuré.

---

5 Cf. Partie 3 B. 2.4.1 p. 49 et E. 2.3.3 ii p. 77.
6 Cf. Partie 3 I. 3 p. 111.
7 Tel est le cas de Sunrise.
8 Pour une définition, cf. Partie 3 H. 2.1 p. 103.
9 Charles PONCET, Intégration, p. 210.
10 Bertil COTTIER, Impact, p. 11.
11 Nous entendrons le terme « information » dans un sens large à l'instar de ce qui est préconisé dans l'exposé des motifs de la directive 2000/31/CE du 8 juin 2000 relative à certains aspects juridiques des services de la société de l'information, et notamment du commerce électronique, dans le marché intérieur, dite « directive sur le commerce électronique ». Cf. COM (1998) 586 final, p. 28.
12 Nous utiliserons parfois le terme « *web* », diminutif de *World Wide Web*, pour désigner Internet en général, même si le premier n'est qu'un des services offerts sur le second, au même titre que le courrier électronique par exemple.

7. Evolutivité

Internet se développe très rapidement et de façon quasi imprévisible. Arpanet[13], l'ancêtre d'Internet, a été conçu en 1969 pour des raisons militaires par des chercheurs de l'Université de Californie de Los Angeles sous le commandement du Ministère américain de la Défense. Il devait assurer les possibilités de communication de l'armée en cas de guerre nucléaire contre l'ennemi soviétique : la destruction d'une partie du réseau ne devait pas entraver la bonne circulation des informations. Dans les années 70 naquit Internet[14], grâce à la définition d'un protocole de communication commun : le TCP/IP[15]. Il gagna alors sa dénomination de « réseau des réseaux », ensemble de réseaux informatiques hétérogènes, privés et publics, interconnectés entre eux grâce à ce protocole commun. Dans les années 80, il fut principalement utilisé par des universitaires et des scientifiques. L'échange du savoir était alors la raison d'être d'Internet, devenu un outil civil.
Au début des années 90, le Centre Européen de Recherche Nucléaire (CERN), et plus particulièrement Tim Berners-Lee et Robert Caillau, délivre au monde le *World Wide Web*. La convivialité de ce service basé sur une interface graphique facile d'utilisation - « *Just click it* ! » - fit le succès d'Internet auprès du tout-public[16]. Le nombre de personnes connectées grandissant exponentiellement[17], Internet est de plus en plus utilisé à des fins commerciales : malgré ses balbutiements initiaux, le réseau des réseaux est la technique de commercialisation de l'avenir. C'est pourquoi aujourd'hui, on parle de la « Net-économie ».
Qui sait ce pourquoi nous utiliserons Internet dans quelques années ? Ce qui paraissait chimérique il y a quelques années, devient réalité grâce notamment à l'amélioration de la technologie de transfert des données. Petit à petit, les appareils mobiles remplaceront avantageusement les ordinateurs classiques. Les terminaux connectés au net le seront en permanence. Il paraît aussi certain que bien avant le 22^{e} siècle, nous ne regarderons plus la télévision qu'au moyen d'un système connecté à Internet[18]. La généralisation des hauts débits nous offrira encore de nombreuses surprises.
Le dynamisme du cyberespace amènera sans cesse de nouveaux défis pour de nombreuses professions, notamment pour les juristes. « *La loi ne peut suivre en temps réel les progrès technologiques* »[19]. L'essentiel est que le retard ne soit pas trop conséquent.

C. Internet n'est pas une zone de non-droit

Cette allégation est aujourd'hui un truisme mais il est intéressant et amusant d'aborder à nouveau succinctement le thème. Terra incognita, le réseau des réseaux a généré les fantasmes les plus fous. Parmi les chimères créées au début de sa formidable éclosion, il faut relever la théorie selon laquelle Internet aurait formé un « vide juridique », échappant aux lois de « notre monde ». Cette idée était partagée par nombre de libertaires[20] qui l'avait déduite des caractéristiques du *web*, que nous avons examinées ci-dessus.

---

13 *Advanced Research Projects Agency Network*.
14 *International Network*.
15 *Transmission Control Protocol over Internet Protocol*.
16 Pour plus de détails sur l'historique d'Internet, voir Arnaud Dufour, Internet, p. 25ss.
17 Le Journal du Net (http://www.journaldunet.com) donne régulièrement des chiffres très intéressants. Il y aurait actuellement plus de 500 millions d'internautes sur terre.
18 Ce passage est inspiré du contenu du site de la Fondation Internet Nouvelle Génération (FING), disponible à l'adresse http://www.fing.org.
19 Christian PAUL, Libertés, p. 80 (version Word).
20 Comme exemple actuel de défenseur de la liberté sur Internet, on peut citer l´association Agora (http://www.agora-fr.org), qui lutte contre les tentatives privées et publiques de contrôle d'Internet.

D'autres utilisateurs d'Internet penchaient pour l'application du droit conventionnel, à l'exclusion du droit national : Internet étant un univers virtuel, sans frontière, les conceptions juridiques nationales ne pouvaient y trouver place.
Ce qui liait ces deux courants était la foi en un système d'autorégulation, qui permettait aux acteurs de s'« autocontrôler » et de s'« auto-défendre ». En clair, ces nouveaux partisans de la liberté, ces « Lumières du 20e siècle », voyaient en Internet un monde virtuel tenant du Moyen-Âge ou du Far West, selon les choix de riposte. L'*e-bombing*[21] nous rappelle en effet étrangement une catapulte…
Tous les jugements touchant Internet ont supprimé le débat. Il ne faut pas oublier que derrière chaque action sur le *web*, il y a une personne réelle qui a utilisé du matériel réel. Et cette personne n'est rien d'autre qu'un justiciable comme les autres[22]. Internet n'est définitivement pas un *no man's land* juridique. Le droit, qu'il soit national ou international, s'y applique. Les *hackers* et autres cyberdélinquants n'ont qu'à bien se tenir. Il n'y a ni impunité, ni immunité sur les réseaux.

D. Le besoin général d'adaptation du droit

1. Le constat

Le droit se doit de refléter notre société. Internet ayant changé notre société, il est censé de songer qu'une modification de notre législation est nécessaire. Certes, le droit commun suisse s'applique pour une large part à Internet. Il suffit généralement pour ester en justice et permet de sanctionner la plupart des infractions commise par le biais d'Internet.
Mais, d'une part, Internet a généré des phénomènes nouveaux qui doivent être pris en compte par notre droit positif. D'autre part, les dispositions de quelques lois existantes sont parfois délicates à appliquer et à interpréter dans le contexte d'Internet. Il n'est pas toujours possible de procéder à une interprétation téléologique ou d'effectuer une analogie. On peut d'ailleurs se demander si cette dernière pratique, autant rassurante soit-elle, est judicieuse, tant il est vrai qu'appliquer une « *règle d'un autre âge, pensée pour une autre technique, dans un autre contexte* »[23] peut parfois apparaître absurde.

Quoiqu'il en soit, les principes fondamentaux de la sécurité et de la prévisibilité juridiques sont mis à mal par le phénomène Internet. Il faut assurer l'« *internetocompatibilité* »[24] de notre droit, afin qu'il puisse répondre aux questions de droit nouvelles que pose Internet. Il faut aussi rassurer au plus vite les investisseurs[25]. La place helvétique doit être concurrentielle au niveau du commerce électronique, si l'on veut éviter à moyen terme des conséquences néfastes sur l'économie suisse.

2. La prise en compte de phénomènes nouveaux

Le réseau des réseaux, et les nouvelles possibilités techniques qu'il offre, n'a généré que de rares nouveaux comportements illégaux mais ces exceptions mettent dans l'embarras les

---

21 L'*e-bombing* ou *mail bombing* est le « *bombardement d'une boîte de courrier électronique par l'envoi d'une quantité astronomique de messages* ». Cette définition est tirée de Eric LABBÉ, Pourriel, pollupostage et référencement abusif : le spamming dans tous ses états, Juriscom.net, avril 1999.

22 Voir le communiqué de l'Association des Utilisateurs d'Internet (AUI) concernant le référé UEJF c. Calvacom et autres, disponible sur le site http://www.aui.fr.

23 Michel VIVANT, Responsabilité, p. 2022.

24 Ce néologisme a été, à notre sens, inventé par Bertil COTTIER, Impact, p. 1.

25 Dans ce sens, Charles PONCET, Intégration, p. 217.

juges. Nous pensons notamment aux délits tels que le *spamming*[26], le *flooding*[27], l'*e-bombing*[28], le *craking*[29]et le *hacking*[30]. Si notre droit appréhende les deux dernières activités citées, les trois premières échappent la plupart du temps à toute incrimination pénale[31]. Notre droit pénal est en ce sens insuffisant. Quelques modifications législatives permettraient de garantir le respect des valeurs et des intérêts fondamentaux de notre société. Le principe de légalité, autant juste soit-il, empêche malheureusement de suivre l'évolution des nouveaux délits : aucun raisonnement par analogie n'est permis. Cette caractéristique du droit pénal peut avoir des incidences en droit civil, car la norme protectrice d'un intérêt patrimonial est souvent d'ordre pénal.
Dans le domaine de la propriété intellectuelle et de la concurrence déloyale, des pratiques telles que le *deep linking*, le *framing* ou l'*inline linking* posent des problèmes certains. Nous reviendrons sur ces procédés plus tard, dans le cadre de la responsabilité des fournisseurs de liens pour le contenu illicite vers lequel le lien renvoie[32].

3. La mise à mal de la législation actuelle

Clarifier les conditions d'application du droit positif dans le cyberespace semble indispensable, ne serait-ce que dans le domaine du commerce électronique.
Jusqu'à dernièrement, les art. 12 et suivants du Code des obligations empêchaient la conclusion sur Internet de contrats nécessitant la forme écrite. En Suisse, c'est par cette problématique que le processus d'adaptation du droit positif à la réalité technique a réellement débuté : le 1er mai 2000 est entrée en vigueur l'Ordonnance sur les services de certification électronique du 12 avril 2000[33]. Cette ordonnance ayant un « *caractère expérimental* »[34], une loi doit la remplacer : dans ce sens, le Conseil fédéral a adopté le 3 juillet 2001 le message relatif à la loi fédérale sur les services de certification dans le domaine de la signature électronique. L'avant-projet prévoit l'introduction dans le Code des obligations d'un art. 15a, qui met sur pied d'égalité la signature manuscrite et la signature numérique.

Toujours dans le domaine du commerce, le droit de la propriété intellectuelle, autant récent soit-il en grande partie, est un peu secoué par l'avènement d'Internet. Il est souvent difficile pour les juges de concilier les dispositions de la Loi sur le droit d'auteur[35] ou de la Loi sur la

---

26 Le *spamming*, ou publipostage électronique, est « *l'envoi massif de courriers électroniques non sollicités, le plus souvent à caractère commercial, à des personnes avec lesquelles l'expéditeur n'a jamais eu de contact et dont il a capté l'adresse électronique dans les espaces publics de l'Internet : forums de discussion, listes de diffusion, annuaires, sites web, etc.* ». Cette définition nous est donnée par la Commission nationale de l'informatique et des libertés (CNIL), dans Le Publipostage électronique et la protection des données personnelles, rapport adopté le 14 octobre 1999, disponible à l'adresse suivante : http://www.cnil.fr/thematic/them01.htm#publipostage.

27 De l'anglais signifiant « inondation », le *flooding* est surcharge intentionnelle d'un système informatique dans le but de le paralyser.

28 Pour une définition, cf. Partie 1 C p. 12.

29 Le *cracking* est l'intrusion d'une personne dans un système informatique dans un but d'altération, de soustraction ou de destruction des données stockées. Le cracker agit surtout par malveillance ou cupidité. Il ne faut donc pas le confondre avec le *hacker* (voir note suivante).

30 Le *hacking* est l'activité d'une « *personne passionnée d'informatique qui, par jeu, curiosité, défi personnel ou par souci de notoriété, sonde, au hasard plutôt qu'à l'aide de manuels techniques, les possibilités matérielles et logicielles des systèmes informatiques afin de pouvoir éventuellement s'y immiscer* ». (Source : Office de la langue française du Québec, http://www.olf.gouv.qc.ca).

31 Laurent MOREILLON, Délits, p. 21.

32 Cf. Partie 3 G. 2 p. 95.

33 RS 784.103.

34 Cf. l'art. 1 al. 1 de l'Ordonnance.

35 RS 231.1.

protection des marques[36] avec certains phénomènes découlant du net, par exemple les copies temporaires de données sur des serveurs *proxy*[37].

4. La solution

Au vu des développements précédents, on voit qu'une réforme juridique, mais non une révolution, est indispensable afin de cesser de vivre dans l'incertitude juridique totale, même si l'évolution technique de la société de l'information rend la quête de la certitude autant impossible que celle du Saint Graal. Reste à savoir comment légiférer en tenant compte des particularités du monde numérique, notamment étendre le champ d'application du droit commun au net. La question de l'intégration de cette nouvelle technologie dans nos systèmes juridiques traditionnels est délicate, mais à notre sens, la législation en question doit être à l'image d'Internet, soit « *dynamique, volatil, transfrontière* »[38].
Dynamique et volatil, car, comme vu plus haut, Internet peut encore nous surprendre par quelques mutations. Devant la difficulté d'appréhender le développement technologique de ce médium, la législation se doit d'être neutre techniquement, afin de ne pas être obsolète avant son entrée en vigueur et de résister quelque temps[39]. Cela oblige le législateur à éviter le détail, les précisions devant être apportées par une ordonnance, acte qui permet de promptes modifications. Lorsqu'il est question d'un domaine technique, les lois formelles se doivent de se limiter aux principes[40].
Transfrontière, car les difficultés d'application du droit actuel résident pour beaucoup dans le fait qu'il a été créé dans un contexte national, alors qu'Internet ignore les frontières des Etats et leurs ordres juridiques. Etant donné la petitesse géographique de la Suisse, créer un droit à caractère exclusivement national serait absurde. Il faut absolument s'inspirer des directives européennes et de la - malheureusement - peu abondante régulation mondiale. Jusqu'ici, le législateur a su regarder ce qui se passe outre frontières, à l'image de l'avant-projet de la Loi sur le commerce électronique[41]. Gageons qu'il en fera de même à l'avenir.
Dans tous les cas, le législateur ne doit pas se perdre en nouvelles législations de toutes sortes : d'une manière générale, il doit se limiter à la promotion d'Internet et du *e-commerce* et la création de la sécurité juridique[42]. Il faut seulement rendre le droit « *effektiv* »[43].

Au niveau de la forme globale de la législation relative à Internet, il semble judicieux de créer une loi générale spécifique au réseau des réseaux, soutenue par des modifications de lois existantes, notamment celles touchant la propriété intellectuelle. On pourrait aussi compléter la Loi sur les télécommunications (LTC)[44].

Il faut préciser que l'adaptation des législations nationales est un bien en attendant le meilleur, c'est-à-dire l'adoption de conventions internationales. Même un encadrement juridique européen semble quelque peu insuffisant. Le caractère transnational d'Internet oblige une

---

36 RS 232.11.
37 Pour des détails techniques, cf. Partie 3 B. 3 p. 52.
38 Bertil COTTIER, Impact, p. 2.
39 Contra André BERTRAND et Thierry PIETTE-COUDOL, Internet et le droit, Paris 1999, p. 6. Les auteurs estiment qu'une loi spécifique à Internet sera toujours prise en défaut par l'évolution de la technologie.
40 Michel VIVANT, Responsabilité, p. 2024.
41 Disponible sur le site de l'Office fédéral de la justice (http://www.ofj.admin.ch). Cet avant-projet s'inspire en particulier de la directive 97/7/CE du 20 mai 1997 concernant la protection des consommateurs en matière de contrats à distance (JOCE L 144 du 4.6.1997).
42 Markus BERNI, E-Commerce, p. 87.
43 Rolf H. WEBER, Haftung, p. 535.
44 RS 784.10.

approche mondiale des problèmes liés à ce médium, si l'on souhaite une efficacité optimale des solutions. La coopération des Etats passera sûrement par l'entremise d'organisations internationales, telles que l'Organisation mondiale du commerce (OMC) ou l'Organisation de coopération et de développement économique (OCDE).
D'une manière générale, il ne sera pas aisé de franchir l'obstacle de l'unanimité[45]. La diversité des législations nationales, due à la « *disparité des conceptions de la liberté* »[46], constitue un indice des difficultés futures dans la quête du consensus. On connaît l'appréhension diamétralement opposée du racisme aux Etats-Unis ou en Europe mais on sait aussi que les seuils de tolérance peuvent être très différents en Europe occidentale : si la pornographie est interdite en Irlande, elle est totalement libre en Suède.
En outre, beaucoup d'Etats trouvent leur intérêt dans les lacunes conventionnelles. Les Etats aux législations plus laxistes gagnent souvent à ce que les cyberdélinquants trouvent refuge sur un serveur situé sur leur territoire. Un exemple évident est constitué par les casinos virtuels : maintes îles exotiques n'ont aucune législation en la matière, alors que les pays occidentaux interdisent ou soumettent à autorisation ce genre d'activités. En se plaçant sur un serveur situé dans un tel paradis insulaire, le vil commerçant dispose pourtant d'un marché mondial. Les jeux d'argent sont dangereux mais pas assez, faut-il croire. Au final, seules de rares conduites illégales sont réprimées unanimement : la pornographie enfantine en fait inévitablement partie.

E. Le complément à la régulation traditionnelle : l'autorégulation

Face aux champions bafoués que forment la régulation étatique et la régulation conventionnelle, un outsider offre des solutions différentes : l'autorégulation.
L'autorégulation consiste en un système de réglementation consensuelle élaborée par les acteurs privés eux-mêmes, notamment les associations de professionnels ou de consommateurs. L'autorégulation a un sens proche des notions d'autodiscipline et de responsabilisation[47]. Elle est une alternative plus élastique et plus adaptée à Internet que les moyens législatifs traditionnels. L'autorégulation est d'autant plus malléable qu'on devrait en parler au pluriel. Il existe plusieurs formes d'autorégulation, celles-ci pouvant avoir des modalités et champs d'application très divers.
La forme la plus connue d'autorégulation est la « netiquette »[48]. La netiquette, qui varie considérablement selon son lieu d'adoption et son adoptant[49], est un code de conduite plus ou moins formalisé qui donne des usages, des pratiques et des règles de politesse et de savoir-vivre quant à l'utilisation correcte et harmonieuse d'Internet, notamment du courrier électronique et des *newsgroups*[50]. Ces normes de comportement non officielles poussent, en particulier, l'internaute à procéder à des communications qui ne soient ni trompeuses, ni offensantes. Chaque nouvel utilisateur devrait en prendre connaissance avant d'utiliser les services liés à Internet. Celui qui contrevient à ces règles est censé s'attirer les foudres de la « communauté ». Des moyens d'autocontrôle devaient ramener à la raison les moutons noirs[51].

---

45 Dans ce sens, Rolf H. WEBER, Haftung, p. 544.
46 FG Associés, Internet et les libertés publiques, Interview publiée dans le Monde Informatique, 7 juillet 2000, disponible sur Droitweb.com.
47 Arnaud HAMON, Expression, p. 127.
48 Le terme résulte de la contraction de l'expression anglaise « *network etiquette* »
49 La netiquette plus connue se trouve à l'adresse http://www.albion.com/netiquette.
50 A noter qu'il ne faut pas confondre la netiquette et la nethique. Cette seconde fait référence à des règles de conduite empreintes de moralité. Les « Ten Commandments for computer ethics » du Computer Ethics Institute en constituent un bon exemple. Ils sont disponibles sur le site http://www.cpsr.com.
51 Tous les moyens sont bons lorsque la communauté souhaite clouer au pilori une personne qui a trahi ses règles. Il peut s'agir de « publicité » de bonne aloi pour les traîtres qui jouissent d'une certaine notoriété.

L'espoir qu'un tel système fonctionne ne fit illusion que jusqu'au véritable essor d'Internet, c'est-à-dire jusqu'à la moitié des années 90. Tant qu'Internet n'était utilisé que par des scientifiques et des universitaires aux mêmes valeurs, la mécanique tournait rond. Mais la vague de nouveaux utilisateurs s'avéra plutôt irrespectueuse et les innombrables violations de la netiquette devinrent impossibles à endiguer.

Si l'autorégulation semble vaine chez l'internaute moyen, il n'en est peut-être pas de même parmi les professionnels d'Internet. En France, la première affaire touchant la responsabilité des prestataires a été favorable à une autorégulation des intermédiaires techniques[52]. Le 5 mars 1996, l'Union des Etudiants Juifs de France (UEJF) assigna en référé un certain nombre de fournisseurs d'accès et d'hébergement pour infraction à la loi réprimant les délits d'apologie et de provocation à la discrimination, à la haine et à la violence. L'UEJF souhaitait qu'il soit ordonné à ces prestataires Internet, sous astreinte, d'empêcher toute connexion à des sites *web* ou forums de discussion contenant des informations négationnistes. En l'absence de réglementation spécifique à l'époque et devant la complexité de l'affaire, le président du TGI proposa une médiation. La décision subséquente rejeta la demande, considérée comme trop générale et imprécise, mais fit part des bonnes intentions de chaque société, qui satisfirent l'UEJF. Le juge donna en effet acte des résolutions des intermédiaires techniques, dont les plus importantes consistaient en des « *moyens d'information et de sensibilisation* », des « *actions déontologiques* », la mise en place d'une charte auprès du cocontractant et la rupture immédiate du contrat avec l'hébergé en cas de violation répétée de la loi ou de la charte. Le plus important est que plusieurs des sociétés en question acceptèrent le principe d'être responsables des pages hébergées, l'éventuelle responsabilité devant certes « *être limitée aux seules pages web et forums de discussion dont elles sont les concepteurs, les animateurs, et/ou qu'elles hébergent volontairement pour les diffuser, soit pour leur propre compte, soit pour le compte de tiers, abonnés ou annonceurs, auxquels elles sont contractuellement liées* ». En revanche, les défendeurs firent valoir que leur responsabilité ne saurait être recherchée en leur qualité de fournisseurs d'accès.
Cette décision a été jugée timide par certains. Elle est pourtant « *la première pierre de l'édifice de la responsabilité des professionnels d'Internet* »[53]. Cette décision et les diverses bonnes idées que l'on peut voir ci et là nous font dire que l'autorégulation est incontestablement un plus. Il faut privilégier la mise en oeuvre des solutions et initiatives imaginées par les acteurs privés. Elles sensibilisent les prestataires et utilisateurs à certains problèmes et renforcent le développement de pratiques loyales.
D'ailleurs, la directive 2000/31/CE du 8 juin 2000 relative à certains aspects juridiques des services de la société de l'information, et notamment du commerce électronique, dans le marché intérieur[54], dite « directive sur le commerce électronique », oblige à son article 16 les Etats membres et la Commission à encourager « *l'élaboration, par les associations ou organisations d'entreprises, professionnelles ou de consommateurs, de codes de conduite au niveau communautaire* ». En Belgique, l'*Internet Service Provider Association* (ISPA) a déjà élaboré un code de conduite[55], qui oblige ses membres à collaborer autant que possible avec

---

Mais la sanction préférée est la paralysie du serveur de courrier du félon. Dans cette optique, un moyen original consiste à abonner la personne à des centaines de listes de diffusion. Mais le moyen classique est le *mail bombing*. D'une manière générale, les messages injurieux envoyés au traître ou postés sur un *newsgroup* sont appelés « *flames* ».

52 TGI Paris, ord. réf. 12 juin 1996, UEJF c. Calvacom et autres, disponible à l'adresse suivante : http://www.aui.fr/Affaires/UEJF/ordonnance.html.

53 Eric BARBRY et Frédérique OLIVIER, La responsabilité des professionnels de l'internet… une histoire sans fin, LEGICOM N° 21/22, 2000/1 et 2, p. 80.

54 JO n° L 178 du 17 juillet 2000, p. 1-16.

55 Disponible à l'adresse http://www.ispa.be/fr/c040203.html.

les instances judiciaires et à offrir aux internautes des possibilités de dénonciation pour avertir le prestataire en cas d'abus sur le net.

Après la netiquette et les codes de conduite, il faut encore examiner une autre forme d'autorégulation particulièrement intéressante : la régulation technique, plus précisément, la régulation de l'architecture technique d'Internet[56]. Intrinsèquement, le réseau des réseaux n'est rien d'autre qu'une infrastructure technique. En modifiant cette infrastructure, on modifie les comportements possibles. Certaines contraintes techniques, « *difficilement évitables ou carrément incontournables* »[57], pourraient s'avérer très efficaces dans la lutte contre l'illégalité. L'exemple le plus avéré aujourd'hui concerne les *cookies*. Un *cookie* est une espèce d'agent intelligent « mouchard » qui enregistre les pages *web* visitées par l'internaute et les opérations effectuées sur ces pages[58]. Techniquement, ce mouchard s'implante, soit dans le disque dur de l'ordinateur du cybernaute, soit dans la mémoire vive de cet ordinateur. Si l'internaute retourne sur le site qui a placé le *cookie*, celui-ci renvoie des informations au site. Les *cookies* permettent ainsi de déterminer le comportement d'un utilisateur particulier et de constituer une base de données sur l'utilisateur. Ils ont donc rapidement été utilisés à des fins commerciales pour déterminer les habitudes comportementales des internautes. Comment faire respecter la protection des données personnelles de ces internautes ? La question revient à se demander comment l'usager peut intervenir sur les données qu'il délivre involontairement. Par le droit, difficilement. Par la technique, bien plus facilement. La norme P3P[59] est une solution. Elle permet à l'usager de définir ses préférences dans les « échanges » avec le site *web*, de gagner en contrôle dans le domaine des *cookies*[60]. Une véritable régulation personnelle est alors offerte à l'utilisateur. Encore faut-il que la norme P3P soit utilisée par les concepteurs de sites. C'est là qu'intervient l'*Internet Engineering Task Force* (IETF)[61], l'organisme chargé de créer les standards techniques d'Internet. L'IETF produit toujours un travail intéressant, malgré la croissance des enjeux liés à Internet et par là, la baisse de sa neutralité du fait de l'aide intéressée de grosses écuries technologiques.
Devant l'efficacité de la régulation technique, on peut penser qu'il serait profitable que le droit s'intéresse à réglementer la technique et non seulement les comportements humains. Le problème est qu'une législation nationale ne serait pas adéquate devant le caractère ubiquiste d'Internet et que les mécanismes de création des conventions internationales ne sont pas assez rapides pour suivre l'évolution technologique.

Quoiqu'il en soit, au contraire de ce que demande certains professionnels d'Internet, on ne peut uniquement se satisfaire de l'autorégulation. Si elle porte encore ses fruits quant à la détermination des standards techniques, elle ressemble globalement d'ores et déjà à un rêve envolé. Le pouvoir et l'argent mènent le bal sur Internet comme ailleurs. Tout comportement est question d'intérêt. Internet n'a bien évidemment pas pu faire converger les intérêts de chaque entité. Un individu ou une société ne respectera un code de conduite relatif au net que tant qu'il ou qu'elle y aura intérêt. Et la communauté ne contre-attaquera que si elle y trouve

---

56 Ce passage est largement inspiré de l'article de Pierre TRUDEL, Architecture.
57 Pierre TRUDEL, Architecture, p. 188.
58 Arian MOLE, Cookies : des mouchards sur Internet, les Echos, 15 janvier 1998.
59 Platform for Privacy Preferences. Des informations sont disponibles à l'adresse suivante : http://www.w3.org/P3P. Pour un résumé, voir Christian PAUL, Libertés, p. 73.
60 Relevons seulement qu'actuellement, le système d'exploitation Windows XP permet de bloquer ou de restreindre, à des degrés différents, l'acceptation des *cookies* sur l'ordinateur personnel de l'internaute. Microsoft a agi de lui-même pour protéger ses clients contre les *cookies* mais n'a autrefois pas hésité à introduire un identificateur global unique dans son processeur Intel Pentium III ou dans les logiciels du pack Office97…
61 http://www.ietf.org.

un intérêt… Les promesses sont vites bafouées dans ce monde de loups. On ne peut contraindre efficacement une personne à un certain comportement que par la loi. Cette dernière reste indispensable pour encadrer Internet, notamment pour réprimer certains crimes et protéger le consommateur ou le créateur d'une œuvre.

Mais un concept nouveau pourrait redorer le blason de l'autorégulation en la liant à la régulation publique. Plus haut, nous avons opposé par le verbe la régulation traditionnelle à l'autorégulation. Il faut plutôt admettre que deux types de régulation devraient être fédérés. Cette « corégulation » offrirait une palette intéressante de solutions aux problèmes complexes découlant d'Internet : deux solutions valent mieux qu'une, surtout lorsqu'elles sont combinées habilement.
Cette idée de régulation plurielle d'Internet se retrouve actuellement en France. Si les Etats-Unis se contentent souvent de l'autorégulation et le reste de l'Europe se satisfait principalement de la régulation traditionnelle, un mouvement souhaitant la coexistence de la régulation des acteurs publics et de l'autorégulation des acteurs privés a émergé dans l'Hexagone. C'est ainsi qu'en 1998, le rapport du Conseil d'Etat sur les réseaux parlait pour la première fois de « corégulation »[62]. Il s'en suivit la création du « Forum des droits sur l'Internet (FDI)[63] », « *espace d'échanges et de coopération entre les acteurs de la régulation* »[64]. Formellement constitué en association, le FDI doit amener divers acteurs – de l'internaute moyen à la Commission européenne - à réfléchir sur les questions de droit générées par Internet, afin de construire intelligemment le cadre juridique de ce dernier. Le FDI doit se comporter en haut-parleur de tous les avis, dont il doit en extraire la moelle, expression du point de vue général. Au mieux, il obtient un consensus. Dans ses activités, cet organisme spécifique est indépendant et neutre. Toute solution dégagée doit être immaculée de traces de lobbying, sans quoi elle perdrait grandement de sa valeur.
En parlant de valeur, Arnaud HAMON met en avant, à juste titre, le point faible de cet organisme a priori très intéressant : il n'est actuellement pas consacré par la loi[65]. Le FDI n'a pas de réelle légitimité et l'efficacité de ses actes risque d'en pâtir. Peut-être n'est-ce qu'une question de temps. Temps qui nous confirmera sûrement qu'un instrument autant flexible que la « plurirégulation » mérite toute l'attention des Etats qui s'intéressent de près à la régulation d'Internet. L'approche inédite de régulation française devrait en inspirer plus d'un.

---

62 Conseil d'Etat (français), Etude Internet et les réseaux numériques, 2 juillet 1998, disponible à l'adresse suivante : http://www.internet.gouv.fr/francais/textesref/rapce98/sommaire.htm.
63 A visiter à l'adresse http://www.foruminternet.org.
64 Christian PAUL, Libertés, p. 102. L'auteur consacre toute la seconde partie de son rapport à cet organisme.
65 Arnaud HAMON, Expression, p. 146.

Partie 2 La problématique de la responsabilité délictuelle relative à Internet

A. Généralités

On l'a dit, Internet est aussi un espace d'abus et par conséquent, une source de dommages. Qui doit réparer ces dommages ? C'est la question de la responsabilité extra-contractuelle. La plupart du temps, les relations entre l'auteur de l'acte illicite et le lésé ne sont en effet pas contractuelles. Il sera d'autant plus difficile pour la victime de trouver réparation, tant on sait que le régime de la responsabilité contractuelle est plus avantageux en raison, notamment, de la présomption de la faute.

1. La recherche d'un responsable par substitution

Comme dit dans l'avant-propos, le cœur des développements touchera la responsabilité des intermédiaires techniques pour les contenus illicites circulant sur Internet. Les fournisseurs d'hébergement, fournisseurs d'accès et autres outils de recherche sont en effet les soldats de première ligne dans la guerre des actions en dommages et intérêts des victimes d'Internet, et ce pour plusieurs motifs.
Tout d'abord, nous avons déjà relevé que l'auteur de l'information illicite n'est parfois pas identifiable. Ensuite, il peut être hors de portée, par exemple s'il habite aux Iles Galápagos : dans ce genre de pays, le droit n'est que peu répressif et l'exécution d'un jugement civil rendu en Suisse ne sera pas chose aisée, la collaboration internationale n'étant pas une priorité. En plus, l'auteur peut être sans le sou. Il peut même s'agir d'une société fantôme qui disparaîtra plus vite que son ombre. Outre ces obstacles difficilement surmontables, des complications au niveau de la preuve des actes illicites commis sont à attendre. Les résultats probants sont rares.
Mieux vaut se retourner contre un autre « participant » à la diffusion du message illicite ayant pignon sur rue, géographiquement proche, solvable et redoutant les effets d'un contentieux sur sa réputation. Il ne fallait donc pas s'étonner lorsque plusieurs affaires, notamment américaines et françaises, ont soulevé la question de la responsabilité des prestataires techniques, parties stables du réseau. Depuis lors, les décisions et les législations se sont enchaînées. Après tout, il n'y a, a priori, aucune raison valable de laisser tranquille ces intervenants sans approfondissement de la question.

2. La contestation de ce rôle

Le prestataire technique d'Internet semble être le bon numéro pour le lésé, content de voir l'existence d'un grand nombre de responsables potentiels. Mais il est évident que les professionnels d'Internet n'allaient pas se laisser imputer une telle charge sans batailler. Dès les premières affaires, s'est dressé un mouvement visant à exonérer les intermédiaires de toute responsabilité. Les arguments des défenseurs de la non-responsabilité des prestataires sont simples : ils n'auraient que des fonctions purement techniques et il leur serait tout bonnement impossible d'opérer un contrôle des informations hébergées, transportées ou indiquées.
Un mouvement antithétique s'est évidemment rapidement dessiné. Devant les maintes dérives émanant du net, la société civile représentée par certains politiques a très vite montré du doigt

les prestataires, en exigeant leur responsabilité systématique. Après tout, pas de prestataires, pas d'atteintes aux droits des tiers, soutiennent les zélateurs de cette tendance. Nous ajouterons, pas de prestataire, pas d'Internet. Il n'empêche qu'un relent de cette position se lit dans l'affaire Estelle Hallyday[66], la Cour d'appel ayant jugé qu'un fournisseur d'hébergement se doit d'assumer les risques que son activité comporte.

Aucune de ses approches n'est juridiquement, ni moralement acceptable : il faut chercher « *non point un improbable juste milieu, mais une réponse de raison* »[67]. D'un côté, si aucune menace ne pesait sur les intermédiaires techniques, les actes illicites seraient favorisés par l'anonymat de l'auteur, entre autres ; de plus, une irresponsabilité totale de principe serait contraire à l'égalité des citoyens devant la responsabilité personnelle. De l'autre côté, les prestataires techniques participent certes à la propagation d'informations illicites, mais « *participer est une chose, être responsable en est une autre* »[68]. Et on ne peut simplement déclarer un participant responsable sous prétexte qu'il faut un remplaçant au premier responsable ou pour des questions d'éthique : cela serait anti-préventif, les auteurs potentiels d'actes illicites étant encouragés par la certitude que le lésé s'attaquerait au prestataire. Il faut se détacher de la personne dont on traite l'éventuelle responsabilité, des lobbies et même de la morale. Il faut se demander ce qui peut légitimement fonder la responsabilité civile d'un prestataire.

3. Quel type de fondement juridique ?

La responsabilité civile peut reposer sur deux types de titres qui fondent l'obligation de réparer.
Dans les pays de droit écrit, la faute est le chef de responsabilité par excellence. Néanmoins, parallèlement à l'évolution de la technologie et les risques inhérents qui en découlent, les responsabilités objectives ont fleuri et prennent aujourd'hui une place d'importance dans le droit de la responsabilité délictuelle européen. Dans l'affaire Estelle Hallyday, l'application de la théorie du risque, qui amène une responsabilité causale, est perceptible pour certains auteurs[69].
Un système fondé sur le risque serait excellent au niveau de la sécurité juridique. Mais une telle approche du problème semble à présent avoir disparue pour diverses raisons, en particulier parce qu'elle contrevient à la liberté d'expression et au développement du net. Les juges s'essaient désormais à définir les comportements fautifs des professionnels d'Internet et les législateurs donnent les conditions d'exonération de responsabilité d'une responsabilité aquilienne. L'idée de base est qu'un reproche doit pouvoir être formulé à l'égard de l'opérateur technique. Dans ce sens, Michel VIVANT met en avant ce qu'il appelle « le triptyque pouvoir - savoir - inertie », selon lequel ne peut être fautif que celui qui peut techniquement agir, sait qu'il doit agir, mais n'agit pas[70].

A l'échelon mondial, se dégage à l'heure actuelle un consensus en faveur de la responsabilité pour faute. A juste titre.

---

66 Voir Partie 3 E. 2.2.1 p. 66.
67 Michel VIVANT, Responsabilité, p. 2022.
68 Michel VIVANT, Responsabilité, p. 2021.
69 Par exemple, FG Associés, A propos de la décision Estelle Hallyday, Expertises, avril 1999, disponible sur Droitweb.com.
70 Michel VIVANT, Responsabilité, p. 2023.

4. Conclusion

Nul choix. Le droit *de lege lata* suisse est le socle sur lequel nous nous baserons pour déterminer la responsabilité extra-contractuelle des intervenants d'Internet. Mais les œillères devront être mises de côté, car la globalité du phénomène Internet nous amène tout naturellement à s'inspirer du vécu et de l'acquis étrangers. D'autres guides devront également nous diriger dans notre quête : les concepts de la technique, de la liberté d'expression et du développement d'Internet.

B. Le droit suisse applicable

1. Généralités

« *En l'état actuel des choses, caractérisé par une absence de régulation étatique et une autorégulation balbutiante, le régime de cette responsabilité doit de rechercher par référence au droit commun* ». Autant cette déclaration du président du Tribunal de grande instance de Nanterre, du 8 décembre 1999[71], n'est plus valable pour la France, autant elle trouve toute sa force en Suisse, car aucune disposition législative suisse ne traite actuellement de la responsabilité en ligne. A l'instar des pays ayant déjà connu une période de gros doutes quant à la responsabilité délictuelle sur Internet, l'application du droit commun n'ira pas sans générer un certain nombre de problèmes.

Le droit commun suisse de la responsabilité délictuelle est composé du Code des obligations (CO)[72], du Code civil[73] et d'abondantes lois spéciales. Les règles en question instituent des responsabilités pour faute ou des responsabilités objectives. Il faut, a priori, et se référer à la responsabilité aquilienne et écarter du débat les responsabilités causales, ces dernières nécessitant une base légale. Mais il ne faut pas oublier que le droit de la responsabilité civile fait actuellement l'objet d'une révision : parmi les nouveautés, il faut relever l'art. 50 de l'avant-projet de la Loi fédérale sur la révision et l'unification du droit de la responsabilité civile[74] (ci-après : avant-projet de révision), qui instaure une responsabilité pour risque.

2. La responsabilité pour faute en Suisse

2.1 Notions

Les art. 41 et suivants du Code des obligations forment le droit général de la responsabilité pour faute ou responsabilité aquilienne. Le principe général est posé par l'art. 41 al. 1 du CO : « *celui qui cause, d'une manière illicite, un dommage à autrui, soit intentionnellement, soit par négligence ou imprudence, est tenu de le réparer* ». Il y a l'idée que l'auteur aurait pu empêcher le fait dommageable de survenir. L'obligation de réparer se fonde sur un reproche fait à l'auteur.

Il existe des dispositions spéciales instituant une responsabilité pour faute. Nous pensons en particulier aux lois sur la propriété intellectuelle. Mais ces règles spéciales renvoient aux

---

71 TGI Nanterre, 1ère ch. A, 8 décembre 1999, Lynda Lacoste c. Multimania et autres, disponible à l'adresse suivante : http://www.juriscom.net/txt/jurisfr/img/tginanterre19991208.htm.

72 RS 220.

73 RS 210.

74 Disponible sur le site de l'Office fédéral de la Justice (http://www.ofj.admin.ch).

dispositions générales du droit des obligations quant à l'action en dommages-intérêts et à la réparation du tort moral[75].

2.2 Les conditions d'application

Il convient de rappeler brièvement les conditions d'application de la responsabilité aquilienne, en insistant sur la notion de faute, décisive dans le débat.

2.2.1 Le préjudice

Le préjudice est une diminution involontaire des biens d'une personne, qu'il s'agisse de son patrimoine, auquel cas l'on parle de dommage[76], ou de son bien-être, auquel cas l'on parle de tort moral.
Le tort moral est aussi défini comme les « *souffrances physiques et psychiques ressenties par la victime à la suite d'une atteinte à sa personnalité* »[77]. Selon l'art. 49 du CO, le lésé trouvera réparation lors d'une atteinte à la personnalité d'une certaine gravité. Il faut notamment penser à une information touchant à l'honneur ou à la vie privée d'une personne, chose fréquente sur Internet.

2.2.2 L'illicéité

L'illicéité est la violation d'une règle protectrice des intérêts d'autrui ou d'un droit absolu de la personne lésée, en l'absence de motifs justificatifs. Selon l'art. 46 de l'avant-projet de révision, « *est illicite le fait dommageable qui porte atteinte à un droit protégé par l'ordre juridique* ».
Les droits subjectifs absolus sont protégés sans disposition prévoyant expressément une protection : sur Internet, les droits absolus pouvant être violés sont les droits de la personnalité[78] et les droits de propriété intellectuelle. Ces droits sont tellement fondamentaux que toute atteinte est illicite, sauf motif justificatif. Peu importe le comportement de l'auteur. C'est pourquoi on parle alors d'illicéité de résultat.
La violation d'une norme protectrice est en revanche nécessaire pour qu'une atteinte à un intérêt autre qu'un droit absolu trouve réparation. On parle d'illicéité par le comportement, car l'illicéité découle d'un certain agissement interdit par l'ordre juridique[79]. On aura compris qu'en cas d'infraction pénale, la responsabilité civile de l'auteur est automatiquement engagée lorsque la victime a subi un dommage. En revanche, le patrimoine en soi n'est pas protégé : l'individu n'a pas un droit subjectif au maintien et à l'accroissement de son patrimoine. Ainsi, lorsque la victime d'un dommage patrimonial ne peut invoquer une règle protectrice, elle n'obtiendra pas d'indemnisation.
On remarquera que les motifs d'exclusion de l'illicéité ne trouveront que rarement application en cas de responsabilité en ligne. On pourrait néanmoins imaginer un cas de légitime défense en cas d'attaque par un pirate informatique.

---

75 L'art. 62 al. 2 de la Loi sur le droit d'auteur et l'art. 9 al. 3 de la Loi contre la concurrence déloyale en constituent deux exemples.

76 On utilisera parfois le terme « dommage » en lieu et place de préjudice, tant il est vrai que le TF a assimilé la réparation du tort moral à celle du dommage dans les ATF 87 II 143 et 102 II 18. D'ailleurs, selon l'art. 45 de l'avant-projet de révision, « *le dommage comprend le dommage patrimonial et le tort moral* ».

77 Henri DESCHENAUX et Pierre TERCIER, La responsabilité civile, Berne 1975, 1ère éd., p. 54.

78 Surtout le droit à l'honneur et à l'intimité de sa vie privée.

79 Comme exemple, on peut citer certaines infractions instituées par le Code pénal, telles que l'escroquerie ou la gestion déloyale. On peut aussi évoquer les actes de concurrence déloyale institués par la loi y relative.

2.2.3 Le rapport de causalité adéquat

Le préjudice doit être le résultat logique de l'acte illicite. Pour ce faire, le fait imputable à l'auteur doit être une cause naturelle - la condition *sine qua non* - et adéquate du préjudice. Selon la jurisprudence constante du Tribunal fédéral, « *constitue la cause adéquate d'un dommage tout fait qui, d'après le cours ordinaire des choses et l'expérience générale de la vie, était propre en soi à entraîner un effet du genre de celui qui s'est produit, en sorte que la survenance de ce résultat apparaît d'une manière générale favorisée par le fait en question* »[80]. Cette problématique n'étant en rien modifiée par le fait que l'acte illicite soit causé par le biais d'Internet, nous en resterons là[81].

2.2.4 La faute

La faute est un manquement individuel à un devoir imposé par l'ordre juridique[82]. Cette notion est liée à celle de reproche. On distingue l'élément subjectif de l'élément objectif de la faute.
L'élément subjectif de la faute est la capacité de discernement de l'auteur, plus précisément sa capacité délictuelle. Il faut qu'il ait eu la faculté de renoncer à l'acte dommageable. Cet élément ne pose évidemment aucun problème dans la problématique de la responsabilité des prestataires techniques.
L'élément objectif de la faute correspond au manquement individuel de l'auteur. Actuellement, pour déterminer si un tel manquement a eu lieu, l'acte de l'auteur est comparé a un comportement standard qu'aurait une personne diligente et raisonnable dans les mêmes circonstances. On ne tient compte que des critères objectifs, soit des circonstances concrètes, telles que l'âge ou la formation de l'auteur et on détermine si l'auteur s'est éloigné du parcours qu'une personne avisée aurait suivi. S'il s'en est éloigné, il a généralement commis une faute. Mais l'avant-projet de révision vise à « resubjectiviser » la notion de faute. Ainsi, agirait par négligence « *la personne qui n'observe pas la diligence commandée par les circonstances et par sa situation individuelle* »[83]. La responsabilité pour faute a comme caractéristique qu'un reproche puisse être fait à la personne en cause : elle aurait raisonnablement pu et dû faire quelque chose pour éviter la survenance du dommage. Or, un reproche est surtout individuel, d'où l'idée de « resubjectiviser » la faute. En ce qui concerne la responsabilité des intermédiaires techniques, les motifs d'excusabilité subjective n'interviendront pas. Par contre, ils pourraient avoir de l'importance dans l'examen des certains cas marginaux de responsabilité.

Il convient encore brièvement de distinguer les deux espèces de fautes : le dol et la négligence.
La faute intentionnelle ou dol est liée à la problématique de la connaissance du caractère illicite d'un contenu. Afin d'établir la responsabilité de l'auteur, il faudra préciser quel fait entraîne connaissance. Si la notification d'une autorité judiciaire amène connaissance, qu'en est-il de la notification du lésé, voire d'un tiers ? On tentera d'y donner une réponse plus loin. En tous les cas, le dol est de façon générale moins problématique que la négligence, même s'il ne sera pas toujours chose aisée de prouver la connaissance de l'auteur.
Il y a négligence lorsque l'auteur ne veut pas le résultat illicite mais n'accomplit pas les efforts nécessaires pour l'éviter. La négligence sera souvent au centre du débat de la

---

80 Cf. RO ATF 102 II 237 par exemple.
81 Pour un développement de la question, voir Pierre Engel, Traité de droit des obligations, 2ème éd., Bern 1997, p. 482ss.
82 Pierre WIDMER et Pierre WESSNER, Rapport, p. 118.
83 Cf. art. 48a al. 1 de l'avant-projet de révision.

responsabilité des intermédiaires techniques : on se demandera si le prestataire technique aurait pu ou dû prévoir le résultat illicite, en faisant preuve de l'attention commandée par les circonstances. Cela reviendra à se demander quels moyens il devra mettre en œuvre, afin d'éviter au mieux tout dommage. La diligence étant une notion à géométrie variable, elle permettra au juge suisse de tenir compte, s'il le souhaite, de la législation européenne.

3. L'avant-projet de la Loi fédérale sur la révision et l'unification du droit de la responsabilité civile

Evidemment, nulle n'est notre volonté de présenter cet avant-projet dans son ensemble. Mais en ce qui concerne la responsabilité des prestataires techniques, il est intéressant d'examiner l'art. 50 de cet avant-projet, qui instaure une clause générale de responsabilité pour risque. L'art. 50 est subsidiaire aux responsabilités pour risque actuellement prévues par les lois spéciales. Il vise les activités spécifiquement dangereuses. Selon le second alinéa de cette disposition, « *est réputée spécifiquement dangereuse l'activité qui, par sa nature ou par celle des substances, instruments ou énergies utilisés, est susceptible, en dépit de toute la diligence qu'on peut exiger d'une personne spécialisée en la matière, de causer de fréquents ou de graves dommages…*». Malgré toute la diligence raisonnablement exigible, notamment l'adoption des mesures les plus perfectionnées, le risque zéro ne peut exister pour ce type d'activité[84].

Par leur nature, les activités d'hébergement de sites et de fourniture d'accès à Internet participent inévitablement et fréquemment à la création de dommages. Il est incontestable qu'aucune diligence de la part des professionnels d'Internet ne pourrait empêcher de tels dommages de subvenir. Un tel risque est inhérent à Internet. De telles activités doivent-elles alors être définies comme spécifiquement dangereuses au sens de l'art. 50 ?

Il est clair que l'avant-projet de la révision n'a pas été prévu pour la responsabilité des prestataires techniques. Il vise plutôt des activités « *de transport créant un danger similaire à celui des véhicules à moteur ou des chemins de fer* »[85], l'utilisation de chaudières, le tir dans un stand, etc[86]. Le rapport explicatif précise que cette clause générale de responsabilité pour risque est introduite pour la raison qu'une législation spéciale « *ne sera* […] *jamais à même de s'adapter à l'évolution scientifique et technique avec une rapidité suffisante…* »[87]. Est-ce une ouverture vers les problématiques d'Internet ? Le Tribunal fédéral nous réservera-t-il une surprise en appliquant cette clause à la responsabilité des professionnels d'Internet ? Seul l'avenir nous le dira, mais une telle jurisprudence nous étonnerait fort. On répétera que la responsabilité causale n'a pas la cote en matière de responsabilité en ligne. De plus, il faut peut-être se rappeler de l'échec d'un avant-projet de loi fédérale modifiant le Code Civil suisse et le Code des obligations, qui proposait l'introduction dans un art. 49^{bis} dans le CO d'une responsabilité sans faute pour les entreprises de presse, de radio et de télévision. Cette proposition avait été sèchement écartée, pour la raison qu'il était inacceptable d'assimiler l'activité d'une entreprise de presse à celles d'exploitants créant des risques caractérisés, à l'image d'une société de chemins de fer[88]. Or, il n'est pas si étrange de tirer un parallèle entre les professionnels d'Internet et les gens de la presse, de la radio et de la télévision, tant il est

---

84 Pierre WIDMER et Pierre WESSNER, Rapport, p. 142.

85 Pierre WIDMER et Pierre WESSNER, Révision et unification du droit de la responsabilité civile, commentaire abrégé, 1999, p. 6.

86 Pierre WIDMER et Pierre WESSNER, Rapport, p. 118.

87 Pierre WIDMER et Pierre WESSNER, Rapport, p. 144.

88 Pierre-Ami CHEVALIER, Les rapports éditeur-rédacteur et les tiers, in Aspects du droit des médias, tome I, Fribourg 1983, p. 180 et 181.

vrai que les activités de ces entités tendent, ou du moins participent, à la diffusion d'informations.

C. Les guides

1. Le vécu et l'acquis étrangers

1.1 La jurisprudence

Les pays qui entourent la Suisse ont connu ses cinq dernières années de nombreuses affaires dans le domaine de la responsabilité relative à Internet. Nous étudierons quelques décisions étrangères tout au long des développements. Si elles nous suggéreront les solutions valables en Suisse, il ne faudra néanmoins pas leur accorder une importance démesurée, car il s'agira souvent de jugements en référé. Les juges du fond n'ont en effet que peu l'occasion de s'exprimer, les parties interrompant la procédure avant. On connaît l'adage: « un mauvais arrangement vaut mieux qu'un bon procès ».

1.2 Le droit étranger

Le caractère omniprésent d'Internet nous encourage aussi fortement à considérer le droit étranger, notamment le droit communautaire. L'harmonisation des solutions, même officieuse, est indispensable pour appréhender efficacement les problèmes liés à Internet.

1.2.1 Le *Communications Decency Act*

La première législation mondiale à traiter de la responsabilité délictuelle relative à Internet fut à notre connaissance la loi américaine dite *Communications Decency Act* (CDA), partie V du *Telecommunications Act*[89]. Rien d'étonnant de voir les Etats-Unis avec quelques longueurs d'avance sur le reste du monde : il ne faut perdre d'esprit qu'ils ont été le berceau d'Internet et que les premières affaires relatives à la responsabilité des prestataires techniques se sont déroulées dans le « pays de la liberté ». Adopté le 8 février 1996, le *Communications Decency Act* vise à réglementer, dans un but de protection des mineurs, l'« *offensive material* »[90] véhiculé en particulier par les services d'Internet. La loi a, a priori, une étendue limitée à ce qui touche aux contenus offensants mais son champ d'application est plus large : elle a ainsi été récemment utilisée dans une affaire de fausse information boursière[91]. En revanche, elle ne règle pas des domaines tels que la propriété intellectuelle[92].
Le CDA fut en partie invalidé en juin 1997 par la Cour Suprême des Etats-Unis[93] pour violation de la Constitution américaine et notamment de son 1[er] Amendement[94], qui protège le « *free speech* ». La section 230 de cette loi est restée intact. Son titre (c), intitulé « *Protection*

---

89 Public Law 104-104, 110 Stat. 56 (codified at 47 U.S.C. § 230).

90 Par « *offensive material* », il faut comprendre les contenus « *obscene, lewd, lascivious, filthy, excessively violent, harassing, or otherwise objectionable* ». Cf. l'art. 230 (c) ch.1 (A).

91 US Court of Appeals, Tenth Circuit, Ben Ezra, et al., v. AOL, 14 mars 2000, disponible à l'adresse suivante: http://laws.findlaw.com/10th/992068.html.

92 Jérôme BENEDICT, Responsabilité, p. 22.

93 Reno, Attorney General of the United States, et al. v. American Civil Liberties Union (ACLU) et al., 117 S.Ct. 2329, 138 L.Ed.2d 874 (1997), disponible à l'adresse suivante : http://supct.law.cornell.edu/supct/html/96-511.ZO.html.

94 « *Congress shall make no law… abridging the freedom of speech or of the press*. »

for good samaritan blocking and screening of offensive material », dispose que « *no provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider* ». Les intermédiaires techniques sont par conséquent vierges de toute responsabilité pour les informations procurées par un autre fournisseur de contenu. La section 230 prévoit aussi qu'un prestataire technique ne peut être tenu responsable d'avoir agi de bonne foi pour restreindre l'accès a des contenus offensants. Cette règle a pour but d'éviter qu'un *provider* voit sa responsabilité engagée en tant qu'éditeur (*publisher* en droit américain[95]) pour avoir exercé un contrôle sur le contenu offensant. Telle mésaventure avait enduré Prodigy, fournisseur de services américain, qui fut condamné pour avoir filtré le contenu d'un forum de discussion[96].
Au final, l'exonération de responsabilité en faveur des fournisseurs techniques, qui vaut pour tous les types d'atteintes à l'exclusion de celles concernant le droit d'auteur, est sans limite et très générale : sauf le respect aux Messieurs du Congrès américain, qui visaient surtout à éviter tout *chilling effect* sur le *free speech*, le texte n'est pas construit « intelligemment ».

1.2.2 Le *Teledienstgesetz*

Le *Teledienstgesetz* (TDG)[97] du 22 juillet 1997, partie du *Multimediagesetz*, est la première réglementation véritablement détaillée sur la responsabilité en ligne. Entrée en vigueur le 1er août 1997, cette loi donne, selon une approche horizontale[98], une série d'exemptions qui constitue une sorte de filtre[99] préalable à l'application du droit commun allemand, civil ou pénal. Ce régime conditionnel d'immunité est la grande trouvaille du législateur allemand. Comme l'explique Cyril ROJINSKY[100], ce régime repose sur trois composantes : l'identification précise des certaines activités offertes par les prestataires techniques, la mise en place d'un principe de non-responsabilité pour ces mêmes activités à certaines conditions et le renvoi au droit commun, si le prestataire ne remplit pas les conditions. Le même auteur relève que le législateur allemand aurait pu imaginer « *une responsabilité de principe associée à des exclusions de responsabilité* […] *ou un régime spécifique de responsabilité* ».

1.2.3 Le *Digital Millenium Copyright Act*

La loi allemande relative aux « téléservices » a sûrement inspiré le *Digital Millenium Copyright Act* (DMCA)[101], adopté le 28 octobre 1998. Ce texte ratifie les deux traités de l'OMPI du 20 décembre 1996 sur le droit d'auteur et sur les interprétations et exécutions et sur les phonogrammes. Il contient surtout des règles spécifiques sur la responsabilité des prestataires techniques en matière de violation du droit d'auteur[102], sous le titre de *Online Copyright Infringement Liability Limitation Act*. Ce titre ajoute au *Copyright Act* de 1976 un paragraphe 512, qui donne des exonérations en distinguant les conditions d'application selon

---

95 Pour plus de détails, voir Jérôme BENEDICT, Responsabilité, p. 18.
96 Stratton Oakmont, Inc. v. Prodigy, 23 Media Law Report 1794 (1995).
97 BGBl. I S. 1870.
98 Dans le sens que la loi s'applique à tous les types d'atteintes à des droits subjectifs. A l'inverse, une législation verticale ou spécifique s'attache à régler les problèmes en cas d'atteinte à un droit particulier, tel que le droit d'auteur.
99 Uwe WALDNER, Internet-Nutzung, p. 361.
100 Cyril ROJINSKY, Approche, par. 5.
101 Public Law N°. 105-304, 112 Stat. 2860 (28 octobre 1998) (codified at 17 U.S.C. § 512).
102 Une partie de la doctrine américaine s'accorde à prétendre que les principes extraits du DMCA pourraient trouver application lors d'autres activités illicites, et non seulement en cas de violation de *copyright*, rapporte Valérie SÉDALLIAN (Responsabilité).

quatre types d'activités[103] : le simple transport, le *caching*, l'hébergement et la fourniture d'« *information location tools* »[104]. A l'instar du TDG, ces « havres de sécurité » (*safe harbours*) jouent un rôle de filtre avant l'application des règles générales de responsabilité.
La loi prévoit des procédures précises de « *notice and take down* » et « *counter-notice and put back* ». Ce système, que nous étudierons plus tard[105], permet au *service provider*, s'il agit conformément aux procédures, d'éviter toute responsabilité, autant vis-à-vis du plaignant que vis-à-vis de l'abonné, si le « *service provider* »[106] est par exemple un fournisseur d'hébergement[107]. Si ce dernier résilie à tort l'abonnement de son client et donc supprime le contenu, il doit en effet s'attendre à une action contractuelle de la part de l'hébergé.

1.2.4 La directive sur le commerce électronique

Le *Teledienstgesetz* et le *Digital Millenium Copyright Act* ont largement inspiré la directive 2000/31/CE du 8 juin 2000 relative à certains aspects juridiques des services de la société de l'information, et notamment du commerce électronique, dans le marché intérieur, dite « directive sur le commerce électronique »[108]. Ce texte est fondamental de part la vocation de la section 4 de son chapitre II à constituer un socle commun de règles de responsabilité pour l'ensemble des acteurs du réseau en Europe. Cette section, nommée « responsabilité des prestataires intermédiaires », donne des principes généraux qui s'appliquent à tout type de responsabilité, civile et pénale[109], selon une approche horizontale : à l'instar du TDG, les dispositions de la directive sont applicables pour tous types d'activités illicites exercées en ligne par des tiers, indépendamment des droits touchés.
A l'image du DMCA, la directive sur le commerce électronique explicite les conditions d'exonération de responsabilité des intermédiaires techniques d'Internet selon certaines activités : le simple transport, le stockage sous forme de « *caching* » et le fourniture d'hébergement. On remarque par contre que la directive ne détermine pas la responsabilité des exploitants de moteurs de recherche et d'annuaires et des « créateurs » d'hyperliens, ce qui est regrettable[110].
Pour chaque type d'activité, le prestataire doit remplir certaines conditions pour bénéficier de l'exemption prévue[111]. Le fait qu'un prestataire remplit les conditions de l'exonération pour une activité donnée ne l'exonère pas de sa responsabilité pour une autre activité.
La directive constitue seulement un filtre à l'application des principes de responsabilité : elle ne donne donc pas les conditions de responsabilité, reprenant l'idée du législateur allemand. Si le prestataire est en dehors du champ d'application des exemptions, la nature et l'étendue de sa responsabilité sont pesées selon le droit de la responsabilité de l'Etat membre en

---

[103] Et non en fonction du statut ou du métier des prestataires techniques, celui-ci se confondant avec celui-là. Ainsi, une université peut invoquer les dispositions du DMCA.
[104] Cette expression désigne en particulier les moteurs de recherche, les annuaires et les liens hypertextes.
[105] Les « *information location tools* » regroupent notamment les moteurs de recherches et les fournisseurs de liens hypertextes.
[106] Ce terme est utilisé pour parler des exploitants des quatre activités ci-avant citées.
[107] Alain STROWEL et Nicolas IDE, Responsabilité, p. 20.
[108] JO n° L 178 du 17 juillet 2000, p. 1-16. Il faut noter que le nom de « directive sur le commerce électronique » n'est pas vraiment descriptif de son contenu.
[109] Cela est mentionné dans l'exposé des motifs. Cf. COM (1998) 586 final, p. 29ss.
[110] Dans ce sens, entre autres, Cyril ROJINSKY, Approche, par. 22. ; Thibault VERBIEST et Etienne WÉRY, Responsabilité.
[111] Notons que dans le TDG, le DMCA ou la directive sur le commerce électronique, la cessation du trouble peut être demandée par le lésé même si le prestataire jouit de l'exonération de responsabilité. Celle-ci ne concerne que les demandes d'indemnité. Le succès de la demande de cessation n'est pas subordonné à la preuve d'une faute du prestataire mais uniquement à la preuve de la violation du droit du lésé. Dans le DMCA, les ayants droit voient néanmoins la cessation du trouble être limitée (cf. l'art. 512j).

question[112]. L'article 15 est primordial en ce sens qu'il prône, à l'instar du DMCA, l'absence d'obligation générale en matière de surveillance, mettant un terme, pour l'Union Européenne, au débat provoqué par l'affaire Estelle Hallyday.
La responsabilité des prestataires est traitée sur quatre articles uniquement. L'harmonisation est volontairement minimaliste[113] : la directive ne souhaite réglementer que ce qui est strictement nécessaire au bon fonctionnement du marché intérieur[114] et au développement du commerce électronique. L'objectif du cadre juridique créé est seulement d'offrir une certaine sécurité juridique, en évitant d'énormes disparités législatives ou jurisprudentielles entre les Etats membres[115], voire au sein d'un seul Etat, à l'image de la France.
On peut se demander si cet objectif sera atteint. Le minimalisme du législateur européen laisse beaucoup de questions ouvertes, auxquelles devront répondre les droits nationaux. Trop, selon certains, qui jugent tout bonnement la directive imprécise[116]. La marge de manœuvre des Etats membres est telle, que le risque est grand de voir se développer des divergences non négligeables, pouvant ainsi créer une distorsion de concurrence et freiner l'essor de la « société de l'information »[117]. On peut particulièrement craindre des disparités conséquentes dans l'appréciation de la notion de « *connaissance de l'activité ou de l'information illicites* » de l'art. 14 qui touche les prestataires d'hébergement.
Il existe heureusement la soupape de sécurité de l'art. 21 de la directive, qui permet de relancer la machine de l'harmonisation en cas de besoin.

Il faut encore noter l'existence de la directive 2001/29/CE du 22 mai 2001 sur l'harmonisation de certains aspects du droit d'auteur et des droits voisins dans la société de l'information[118]. Un peu à l'image des Etats-Unis et de leurs CDA et DMCA, l'Europe a choisi une approche horizontale, complétée par une approche verticale en ce qui concerne le droit d'auteur. En cas de violation de ce droit de propriété intellectuelle, les deux directives devront être lues simultanément.

1.2.5 Les lois de transposition des Etats membres de l'Union Européenne

Les Etats membres avaient jusqu'au 17 janvier 2002 pour transposer la directive sur le commerce électronique. Le Luxembourg est le premier Etat à avoir agir par une loi du 14 août 2000[119]. Le texte est sans surprise, comme le sont l'avant-projet belge[120] et la loi allemande[121]. Aucun de ces textes ne définit la notion de connaissance des contenus illicites, ni ne parlent des outils de recherche et autres fournisseurs de liens. En ce qui concerne ces derniers, le projet espagnol du 30 avril 2001 et l'*E-Commerce-Gesetz* (ECG)[122] d'Autriche sont plus « bavards ». Nous en reparlerons plus loin. La France a, quant à elle, d'abord adopté une

112 Cf. COM (1998) 586 final, p. 28.
113 Lors d'une conférence donnée à l'Université de Neuchâtel le 12 juin 200 sur la responsabilité des intermédiaires (cité ci-après : Conférence non publiée), Bertil COTTIER rapporte que cette volonté a largement été dessinée par les branches professionnelles touchant à Internet, qui ont amené le Parlement européen, qui souhaitait un régime strict, à revoir ses prétentions à la baisse.
114 Cf. considérant (10) de la directive et COM (1998) 586 final, p. 15.
115 Thibault VERBIEST, La Directive européenne sur le commerce électronique, Juriscom.net, 15 juin 2000. Cf. aussi considérant (40) de la directive.
116 Thibault VERBIEST et Etienne WÉRY, Responsabilité.
117 N'atteignant ainsi qu'imparfaitement les objectifs des considérants (7) et (8) de la directive.
118 JO n° L 167 du 22 juin 2001, p. 10-19.
119 Le texte est disponible sur le site http://www.droit-technologie.org.
120 L'avant-projet - non officiel - belge de loi sur certains aspects juridiques des services de la société de l'information du 30 novembre 2001 est disponible sur le site http://www.droit-technologie.org.
121 Gesetz über rechtliche Rahmenbedingungen für den elektronischen Geschäftsverkehr (Elektronischer Geschäftsverkehr-Gesetz, EGG), Bundesgeseztblatt du 20 décembre 2001, p. 3721ss.
122 BGBl. I Nr. 152/2001.

première loi[123] qui suivait la jurisprudence française, pour finalement ne transposer que très imparfaitement la directive sur le commerce électronique. Mais la Loi sur la société de l'information (LSI) devrait bientôt permettre à la France de rattraper son retard abyssal en matière de transposition[124]. Retard, dont font preuve la plupart des Etats membres non cités. Pour ces Etats, se pose la question de l'applicabilité directe de la directive sur le commerce électronique, à laquelle les juges ne tarderont pas à donner réponse[125].

2. Les concepts centraux

Un journaliste suisse a exprimé en une seule phrase tous les concepts à prendre en compte lors de l'appréhension des dérives du net : « *entendons-nous bien : il n'est pas question de protéger les pornographes, pédophiles, racistes et autres extrémistes qui se baladent dans le cyberspace - et qu'il faut au contraire dénoncer et frapper - mais de favoriser le développement d'Internet et du web et d'y préserver la liberté d'expression, en imaginant une réglementation politiquement raisonnable, socialement acceptable et techniquement réaliste des réseaux globaux* »[126].
Nous développerons trois de ces concepts capitaux : la technique, la liberté d'expression et le développement d'Internet.

2.1 La technique

Le chemin menant à la réponse à toute question juridique liée à Internet est entravé par les aspects techniques alambiqués de celui-ci, par la diversité des services qu'il offre et par ses mutations incessantes. La réponse n'est donc jamais définitive. C'est le propre d'Internet, infrastructure de communication sans pareil.
Le domaine de la responsabilité délictuelle n'échappe pas à la règle : les causes de responsabilités doivent être examinées à la lumière de la technique. On a vu plus haut le triptyque « pouvoir - savoir - inertie ». Qui dit pouvoir, dit capacité technique d'intervenir. A l'impossible, nul n'est tenu. On ne pourra tenir un intervenant pour responsable s'il n'a aucun pouvoir d'intervention sur le contenu illicite.
La question de la responsabilité est souvent liée à la connaissance des informations illicites et aux possibilités de contrôle de celles-ci[127]. Il faut se demander si l'acteur d'Internet les connaissait ou aurait dû les connaître. La plupart du temps, il n'aura qu'une connaissance limitée, voire nulle des informations. La question de la négligence entrera alors en compte.
La diffusion d'informations sur Internet nécessitant la participation de nombreux intervenants, il est indispensable de savoir quels sont les rôles respectifs de chacun au niveau technique. D'une manière générale, l'environnement technique doit être défini au mieux à chaque examen de responsabilité. A cet effet, la coopération avec des spécialistes de l'informatique et des réseaux semble indispensable. Aujourd'hui, une cour ne peut pas se permettre d'ignorer la technique et encore moins de montrer son ignorance. Pour l'anecdote, en 1996, la Cour suprême suédoise avait refusé de juger une affaire où l'exploitant d'un BBS était incriminé pour violation du droit d'auteur. Ainsi, la première haute cour d'un pays européen à s'être

[123] Loi n° 2000-719 du 1er août 2000 modifiant la loi n° 86-1067 du 30 septembre 1986 relative à la liberté de communication, *J.O.*, n° 177, 2 août 2000.
[124] Le projet de loi sur la société de l'information établi à l'issue du conseil des ministres du 13 juin 2001 est disponible sur le site de Legifrance, http://www.legifrance.gouv.fr.
[125] Etienne WÉRY, La directive e-commerce devrait être transposée pour aujourd'hui au plus tard !, http://www.droit-technologie.org , 17 janvier 2002.
[126] Bruno GIUSSANI, article paru dans l'Hebdo au courant de 1995, des dires de l'auteur.
[127] Thomas PROBST, Quelles responsabilités pour les fournisseurs d'accès et d'hébergement, p. 3 et 12.

penchée sur un problème de prestataire avait prétexté qu'il n'appartenait qu'au législateur de combler les lacunes législatives dans une matière aussi complexe[128].
Les lacunes scientifiques des juges les amènent souvent à apposer à Internet des raisonnements inadéquats. Le 28 janvier 1999[129], la 17e Chambre Correctionnelle du TGI de Paris a qualifié d'infraction instantanée un délit de presse perpétré sur Internet ! Et on ne parle pas des analogies plus que douteuses trouvées dans maintes décisions ici et là.
La compréhension du fonctionnement d'Internet est un passage forcé dans la détermination des responsabilités de ses intervenants.

2.2 La liberté d'expression

La protection des libertés est primordiale, qu'il soit question d'Internet ou pas. Mais le réseau mondial est le royaume des excès. Ses spécificités accentuent la problématique de la protection de la liberté d'expression, comme elles accentuent le bien et le mal qui découlent de ce vecteur de communication.
Internet est l'outil générateur de liberté d'expression par excellence. Il offre à quiconque la même autonomie que les magnats des média : les individus, associations et sociétés peuvent ainsi profiter de la diffusion mondiale de leurs opinions et d'informations propres[130]. Dans les pays favorisés, avoir un site personnel est en effet devenu une banalité : les coûts sont faibles, la création aisée. Il est encore plus facile de faire passer des idées par le biais des *newsgroups*. Instantanément et librement, les militants et les oppressés peuvent s'adresser au monde entier pour faire part de leurs soucis.
Mais si la liberté d'expression est toujours le pilier fondamental du réseau mondial, elle n'est pourtant pas à l'abri de menaces. Tout d'abord, une forte demande puritaine de sécurité pointe le bout de son nez : l'opinion publique, créé principalement par des non-internautes, demande la tête des auteurs de certaines pratiques, pornographiques, violentes ou racistes en particulier. Ensuite, les pays totalitaires mettent en œuvre des moyens énormes afin d'empêcher certaines opinions politiques et autres informations gênantes de franchir les frontières intérieures[131]. Finalement et c'est ce qui nous intéresse, l'insécurité juridique dans laquelle se trouvent les prestataires Internet risquent de conduire tout droit à la censure privée.

A vrai dire, il est normal que la liberté d'expression trouve des limites sur Internet, comme elle en trouve ailleurs. Cette liberté individuelle ne peut couvrir des atrocités telles que la haine raciale ou la pornographie enfantine. C'est toujours l'idée que la liberté de chacun doit s'arrêter là où commence celle des autres. C'est en tout cas l'optique des pays de tradition romano-germanique. On sait qu'aux Etats-Unis, le Premier Amendement de la Constitution confère une portée maximale au concept de liberté d'expression. La Cour Suprême des Etats-Unis n'accepte que de rares exceptions au « *free speech* ». Le CDA et le *Child Online Protection Act* de 1998 avaient un but plus qu'honorable : protéger les mineurs contre certains contenus choquants. Ces lois ont pourtant déclenché un tollé parmi les groupes de défense des

---

128 Bertil COTTIER, Conférence non publiée.
129 Voir à ce propos Alexandre BRAUN, Prescription des délits commis sur l'Internet : une impunité qui ne dit pas son nom ?, Juriscom.net, mars 1999.
130 Avec toutes les conséquences qu'une telle possibilité peut amener. Voir Philippe VANHOOLANDT, La désinformation sur Internet, octobre 1997, disponible à l'adresse http://www.vanho.com/articles/1229.htm.
131 La Chine ne restreint pas l'accès à Internet mais, à l'instar des autres technologies de l'information et des communications, contrôle le contenu transitant par ce biais. Les autorités chinoises ont ainsi mis en œuvre des technologies de filtrage d'accès aux contenus. Voir à ce propos, Shanti KALATHIL et Taylor C. BOAS, The Internet and State Control in Authoritarian Regimes : China, Cuba and the Counterrevolution, First Monday, volume 6, number 8 (August 2001) disponible à l'adresse http://firstmonday.org/issues/issue6_8/kalathil/index.html.

libertés individuelles et n'ont pas échappé au couperet des tribunaux étasuniens. Dans la décision de la *District Court for the eastern district of Pennsylvania* qui a précédé la décision de la Cour Suprême de juin 1997, un juge avait utilisé l'expression « *conversation mondiale sans fin* » pour désigner Internet et avait jugé qu'en tant que telle, elle méritait « *la plus haute protection contre l'ingérence de l'Etat* »[132]. La Cour Suprême a refusé la censure officielle qu'introduisaient les deux lois ci-dessus citées, en arguant entre autres que la protection des mineurs ne devait pas avoir un *chilling effect* sur la liberté d'expression des adultes. En effet, pour les personnes majeures, beaucoup des contenus visés par les deux lois ne sont pas illégaux : les adultes y ont d'ailleurs accès par l'intermédiaire de revues ou vidéocassettes coquines. La Cour Suprême s'est donc refusée de criminaliser l'expression sur Internet[133].
En Europe, la liberté d'expression, plus particulièrement la liberté d'information, est garantie par l'art. 10 al. 1 de la Convention de sauvegarde des droits de l'homme et des libertés fondamentales du 4 novembre 1950 (CEDH)[134]. En Suisse, l'art. 16 de la Constitution fédérale du 18 avril 1999[135] proclame les libertés d'opinion et d'information. La liberté d'expression est tellement fondamentale, dans un ordre juridique démocratique, que le Tribunal fédéral l'a en 1961 érigée en droit constitutionnel non écrit en se basant sur l'art. 55 de l'ancienne Constitution fédérale, qui ne consacrait que la liberté de la presse[136].

Mais autant fondamentale qu'elle puisse être, la liberté d'expression a des limites. A l'instar de nombreuses autres libertés : elle n'est pas absolue. D'ailleurs, « *la liberté d'expression est une liberté qui suppose des exceptions pour son exercice* »[137]. Ainsi, le second alinéa de l'art. 10 de la CEDH permet des restrictions « *prévues par la loi, qui constituent des mesures nécessaires, dans une société démocratique, à la sécurité nationale, à l'intégrité territoriale ou à la sûreté publique, à la défense de l'ordre et à la prévention du crime, à la protection de la santé ou de la morale, à la protection de la réputation ou des droits d'autrui, pour empêcher la divulgation d'informations confidentielles ou pour garantir l'autorité et l'impartialité du pouvoir judiciaire* »[138]. Internet est facilement susceptible d'atteindre à la plupart des intérêts généraux ou particuliers cités. En matière civile, les droits d'autrui seront le plus souvent invoqués pour contrer la circulation de contenus illicites. On pense notamment aux droits de la personnalité et aux droits de propriété intellectuelle. Il faut encore que l'invocation du droit justifiant une limitation de la liberté d'expression passe le test de la proportionnalité, conformément à la jurisprudence de la Cour européenne des droits de l'homme de Strasbourg[139]. En Suisse, les conditions de restriction aux droits fondamentaux sont en grande partie semblables à celles instaurées par la CEDH[140].

---

132 ACLU v. Reno, 929F. Supp. 824 (E.D. Pa. 1996). Traduction libre d'Arnaud HAMON, op. cit. (47), p. 57.
133 Arnaud HAMON, Expression, p. 70.
134 RS 0.101.
135 RS 101.
136 RO ATF 87 I 117.
137 Arnaud HAMON, Expression, p. 50.
138 A ce propos, Pierre-François DOCQUIR (Contrôle des contenus sur Internet et liberté d'expression au sens de la Convention européenne des droits de l'homme, http://www.droit-technologie.org, mai 2002) souhaite que « *la Cour européenne des droits de l'homme* [consacre] *le principe d'une interprétation restrictive des exceptions à la liberté d'expression sur Internet* ». Selon l'auteur, la protection de la liberté d'expression est encore plus importante sur Internet que dans la vie réelle.
139 Alain STROWEL et Nicolas IDE, Responsabilité, p. 15.
140 La nouvelle Constitution fédérale du 18 avril 1999 parle aussi de légalité et de proportionnalité. Entre aussi en compte la notion d'inviolabilité de l'essence du droit fondamental, condition rarement en question. Dans les termes, on peut noter une différence avec la CEDH : l'art. 36 al. 2 de la Constitution dit que la « *restriction d'un droit fondamental doit être justifiée par un intérêt public ou par la protection d'un droit fondamental d'autrui* ». Notre Constitution ne parle donc pas seulement de « droit d'autrui », mais de « droit fondamental d'autrui ». Dans un entretien électronique, Pascal MAHON, Professeur à l'Université de

Internet étant un espace juridique, les conditions de restriction susmentionnées s'y appliquent aussi et peuvent légitimement limiter la liberté d'expression y régnant. Mais on peut craindre que ces conditions ne soient pas respectées. On revient là aux inquiétudes qui pèsent sur la liberté d'expression. Cette valeur fondamentale est en effet liée à la délicate problématique de l'intervention du prestataire technique. Ce dernier ne doit pas contrevenir à la liberté d'expression en se couronnant d'un pouvoir de censure privé. En même temps, il doit veiller dans une certaine mesure - il faudra déterminer laquelle - aux droits légitimes des tiers, qui, on le rappelle, comptent parmi les limites de la liberté d'expression. Cette ambivalence amène beaucoup de problèmes.

Il faut tout de même préciser que l'intervention du prestataire ne signifie par forcément censure. L'hébergeur n'a pas que la simple suppression du site comme moyen de faire respecter les droits d'autrui. Il devrait agir proportionnellement à la faute. En ce sens, la médiation peut s'avérer efficace lorsque la faute est légère et apparemment involontaire : un *e-mail* et le tour peut être joué. Mais peut-on raisonnablement imposer au prestataire de se comporter comme un chaperon ?

Il est clair qu'un site totalement hors-la-loi devra être supprimé du serveur du fournisseur d'hébergement. Les complications apparaissent dans les cas limite. Il peut s'avérer difficile de distinguer le licite de l'illicite. C'est dans ce genre de cas qu'il faudra clarifier les moyens à mettre en place par le prestataire, afin que sa responsabilité ne puisse être engagée. Afin d'éviter une censure préjudiciable, on pourrait penser qu'il ne faudrait donner à l'intermédiaire technique le pouvoir d'agir que lorsqu'il y a manifestement violation de la loi ou qu'en cas de doute, une injonction d'une autorité judiciaire est nécessaire. Mais ne serait-ce pas être trop laxiste vis-à-vis des cyberdélinquants ?

La question du filtrage des contenus est tout autant délicate. Techniquement, les moyens de filtrage sont actuellement loin d'être convaincants et on doute fort que l'évolution de la technologie amènera un jour une solution véritablement probante. Les logiciels[141] utilisés de nos jours, surtout par les Américains il faut le dire, sont peu efficaces. Ils interdisent l'accès à certains sites traitant du cancer du sein ou de la lutte contre le SIDA, ou encore au site de la *National Organization for Women*[142], organisme américain de défense des droits de la femme. A l'inverse, le site du Ku Klux Klan n'est pas censuré et son horrible croisade peut se perpétuer par le biais du net[143]. Si la non-censure de ce site s'explique par la protection accordée par le Premier Amendement aux racistes les plus véhéments, il n'est pas acceptable que des sites d'utilité publique fassent les frais d'un dégrossissement inadéquat. Les limites techniques des programmes rendent le filtrage arbitraire et par là, juridiquement très contestable au vu de la liberté d'expression. Le juge de la Cour Suprême des Etats-Unis John Paul Stevens, statuant sur l'opportunité du CDA vis-à-vis du « *free speech* », déclara : « *dans une société démocratique, la sauvegarde de la liberté d'expression prime sur tout avantage théorique mais non prouvé d'imposer une censure* ».

La notion de connaissance du contenu illicite risque aussi indirectement d'atteindre illégitimement à la liberté d'expression. Cette notion n'est définie ni par la directive sur le commerce électronique, ni par les lois de transposition de cette directive. Tant que les prestataires ne sauront pas ce que signifie le terme « connaissance », notamment si cette connaissance est réalisée lors de la notification du lésé et non de l'autorité judiciaire, ils auront tendance à supprimer tout site faisant l'objet d'une plainte. La directive sur le

---

Neuchâtel, nous signale toutefois que cette distinction n'est que peu significative, car l'expression « droit d'autrui » de la CEDH vise surtout les droits fondamentaux.

141 Par exemple, CYBERsitter, NetNanny et CyberPatrol.

142 http://www.now.org.

143 Jean-Pierre CLOUTIER, Censure et liberté d'expression : recherche d'une solution politiquement raisonnable, socialement acceptable et techniquement réaliste, disponible à l'adresse suivante : http://www.risq.qc.ca/enquete/3/analyses/libexpre.html.

commerce électronique entendait pourtant ne pas « *porter atteinte aux règles et principes fondamentaux nationaux en matière de liberté d'expression* »[144].

Le conflit entre liberté d'expression et respect des droits des tiers génère de nombreuses questions. Nous essayerons plus loin d'y donner des réponses, tiraillées qu'elles seront entre la reconnaissance de la primauté des libertés et la sauvegarde des droits d'autrui qui passe par un certain contrôle.

2.3 Le développement d'Internet

Nous avons vu l'importance d'Internet dans notre société. Importance sociale, économique, culturelle, politique et démocratique. A ses considérants (1) et (2), la directive sur le commerce électronique relève plus spécifiquement que le développement des services de la société de l'information et donc d'Internet rapproche les peuples européens et que le développement du commerce électronique créera un nombre d'emplois conséquent.
L'importance d'Internet nous amène à dire qu'il faut éviter de rendre responsables les personnes indispensables à son fonctionnement, à un tel point qu'elles ne puissent plus assumer leur rôle et qu'un poste de la grande « entreprise » Internet ne puisse plus être repourvu. C'est surtout en rapport avec le concept de développement d'Internet que l'application d'une responsabilité fondée sur le risque paraît très contestable. Elle n'encouragerait évidemment pas de nouveaux professionnels à gagner le domaine. Beaucoup d'entreprises établies verraient vite se pointer la faillite à l'horizon. En prévision des futures dommages et intérêts ou en conséquence du paiement de primes d'assurances ruineuses, les « survivantes », en feraient payer le prix à leurs clients.
Internet est un outil fabuleux : il faut le préserver et encourager son développement. Le monde a tout à y gagner.

[144] Cf. considérant (9) de la directive sur le commerce électronique.

Partie 3 La responsabilité délictuelle des acteurs d'Internet

Le fonctionnement d'Internet induit la participation de nombreux intervenants. Plusieurs auteurs se sont essayés à l'élaboration d'une typologie logique de ces acteurs d'Internet[145]. Il ne nous semble pas obligatoire de classer de façon systématique ces divers intervenants puisque l'on traitera de leur responsabilité au cas par cas, même si plusieurs d'entre eux feront l'objet d'une réflexion analogue. Il existe tellement de doutes quant à la définition de ces protagonistes qu'un classement logique tient assurément de l'aléatoire : l'important est de savoir de quel acteur il est question. C'est pourquoi nous nous contenterons de lister les intervenants de façon intuitive.
Il faut encore préciser que lorsque nous examinerons la responsabilité du fait de contenus illicites, ne comptera pas le métier de la personne susceptible de responsabilité, mais bien « *sa fonction au regard des contenus diffusés* »[146]. La versatilité de la notion de « métier » du net la rend inutile dans notre réflexion.

A. L'internaute

1. Notion

L'internaute, ou moins communément cybernaute, est l'utilisateur d'Internet. La plupart du temps grâce à un ordinateur, il « navigue » sur la toile, se sert de sa messagerie électronique, consulte des *newsgroups*, etc. L'usager est principalement lecteur, spectateur ou auditeur, en un mot, consommateur d'informations. Mais le caractère interactif d'Internet permet à l'internaute d'avoir un comportement contributif. C'est surtout lorsqu'il interférera dans le grand jeu d'Internet qu'il risquera de voir sa responsabilité engagée, même si la simple consommation d'informations pourrait théoriquement engager sa responsabilité.
La question de la responsabilité de l'internaute a été jusqu'alors peu discutée. Elle sera tôt ou tard d'importance. Afin d'éviter au mieux les dérapages, des mesures doivent être prises à tous les niveaux du processus illégal. Comme exemple, le cybernaute qui fréquente les casinos virtuels pourrait dans le futur se voir sanctionné pénalement. Une loi américaine a déjà introduit ce principe[147].

2. La responsabilité du fait de la consommation d'informations

La question de la responsabilité de l'internaute en tant que consommateur d'information peut paraître pour le moins surprenante en matière civile. Mais on peut sérieusement y songer dans un cas de figure au moins. Celui qui verrait un adulte télécharger[148] (*download*) des images de pornographie dure depuis un site *web* et les stocker sur son disque dur, et ne pas prendre les

[145] Bertil COTTIER (Conférence non publiée) distingue les fournisseurs de contenants (transporteurs, fournisseurs d'accès, fournisseurs d'hébergement) des fournisseurs de contenu (auteurs et éditeurs, fournisseurs de valeur ajoutée, internaute) en plaçant les relayeurs d'informations (exploitants d'un moteur de recherche, fournisseur de liens, exploitants de forum de discussion) dans une troisième catégorie.
[146] Frédérique OLIVIER et Eric BARBRY, Hébergement.
[147] André BERTRAND et Thierry PIETTE-COUDOL, Internet et le droit, Paris 1999, 1e éd., p. 121.
[148] Une nouvelle vague souhaiterait que le verbe anglais « *download* » soit traduit par les termes « télédécharger » ou « décharger ». Nous nous en tiendrons néanmoins à « télécharger ».

mesures pour éviter qu'une personne sous sa garde - par exemple l'enfant du voisin - les découvre. Ce manque de diligence pourrait attenter à l'intégrité psychique de l'enfant. En l'espèce, les conditions d'une action en dommages-intérêts seraient remplies. En matière pénale, un tel agissement pourrait tomber sous le coup de l'art. 197 du CPS.
Il faut relever que d'une manière générale, la responsabilité pénale du fait de la consommation d'informations sera bien plus sollicitée que la responsabilité civile. Ce principe devrait être introduit à l'échelon mondial, grâce à l'art. 9 al. 1 lit. e de la Convention sur la cybercriminalité, qui condamne la possession de pornographie enfantine dans un système informatique.

3. La responsabilité du fait d'une déclaration dans un *newsgroups* ou dans un forum de discussion non fermé

Internet est un médium conversationnel. Il donne à l'internaute l'occasion de devenir un auteur « publié », notamment par l'entremise des forums de discussion et des *newsgroups*. Or, ces services sont souvent utilisés pour invectiver les personnalités les plus diverses. Demandez à Bill Gates… En tant qu'auteur, le cybernaute supporte envers les tiers la responsabilité civile des informations qu'il diffuse. Cette problématique est identique à celle de la responsabilité du fournisseur de contenu étudiée plus loin[149]. Il faut seulement indiquer que la faute de l'internaute, en tant qu'amateur, devra le cas échéant être appréciée moins sévèrement par les tribunaux que celle des professionnels de l'information.

4. La responsabilité du fait de l'utilisation du courrier électronique

4.1 Notions

La messagerie électronique est, avec le *World Wide Web*, le service le plus connu et utilisé du réseau Internet. Il s'agit d'un système de transmission de messages par voie électronique sur un réseau de communication local ou global. Les messages en question sont nommés courriers électroniques ou *e-mails*[150]. L'expéditeur, identifié par son adresse électronique[151], envoie son message à un ou plusieurs destinataires, identifiés de la même façon. Chaque adresse électronique est associée à une boîte aux lettres électronique, située sur le serveur du gérant du service de messagerie électronique ; les messages sont reçus dans cette boîte et y résident jusqu'à ce que l'usager les télécharge sur son propre ordinateur.

Si ce service est si répandu, c'est qu'il est très pratique, rapide et presque gratuit. Tout fournisseur d'accès digne de ce nom offre ce service à ses abonnés.

4.2 La responsabilité au travers d'une déclaration

L'expéditeur d'un message électronique peut-il voir sa responsabilité civile engagée vis-à-vis de personnes tierces pour le contenu illicite que renfermerait l'*e-mail* ? D'une manière générale, non[152]. La réponse dépend en fait de la qualification donnée au courrier électronique.

---

[149] Cf. Partie 3 I. 2 p. 110.
[150] Contraction de « *electronic mail* ». La Délégation générale à la langue française recommande le terme « courriel »…
[151] Sauf usage d'un « *anonymizer* ». Pour une définition de l'*anonymizer*, cf. Partie 3 I. 3 p. 111.
[152] En matière pénale, la question est autre. Certaines dispositions, à l'image de l'art. 197 al. 3 du CPS, permettent d'engager la responsabilité pénale de l'auteur d'un courrier électronique. C'est ainsi qu'une

Il est admis que le courrier électronique est un support de communication privée. L'analogie avec le courrier postal sous enveloppe saute aux yeux. Celle, avec les conversations téléphoniques, aurait déjà largement suffi. Dans un arrêt canadien[153], le juge s'est amusé à tracer tous les parallèles existants entre l'*e-mail*, d'une part, le courrier traditionnel et les appels téléphoniques d'autre part. La liste est longue.
Ce caractère de communication privée et individuelle rend l'*e-mail* protégé par le secret des télécommunications, garanti qu'il est par l'art. 13 al. 1 de la nouvelle Constitution du 18 avril 1999 et plus spécifiquement par l'art. 43 de la loi fédérale sur les télécommunications (LTC)[154] et les art. 179[bis] et suivants du Code pénal. Dans l'ATF 126 I 50, le Tribunal fédéral a logiquement confirmé que le courrier électronique était protégé par le secret des télécommunications.
Mais admettre que l'*e-mail* est toujours une communication privée, c'est aller un peu vite en besogne. En France, la circulaire relative aux services télématiques du 17 février 1988 prévoit qu'une communication est privée lorsque le message est strictement destiné à une ou plusieurs personnes déterminées ou individualisées. Quid d'un *e-mail* envoyé à une liste de diffusion (*mailing list*) ? « *Il faut distinguer selon le type de liste et selon ses modalités de fonctionnement* »[155] mais le nombre d'abonnés à la liste, qui peut être minuscule comme considérable, n'est pas le critère le plus pertinent. Si la liste de diffusion et les archives y liées ne sont destinées qu'à des personnes identifiées - par exemple les membres d'un syndicat ou un groupe d'amis -, il s'agit d'une correspondance privée. François-Régis LEVOL rapporte l'avis d'un conférencier qui va dans ce sens[156]. L'orateur, qui se base sur un arrêt de 1954, met en avant le concept de « communauté d'intérêts ». S'il y a une communauté d'intérêts entre les abonnés de la *mailing list*, la communication est privée. La condition de la communauté d'intérêts est par exemple remplie lorsque la liste est exclusivement adressée au personnel d'une entreprise ou aux membres d'une société ou d'une association. A l'inverse, si les abonnés ne sont pas liés par une communauté d'intérêts, la communication est publique. C'est le cas lorsque quiconque peut sans autre s'inscrire à la liste. Or, la plupart des *mailing lists* sont ouvertes à tous.
Il faut s'inspirer de ces théories, mais la qualification juridique d'une liste de diffusion, et le régime de responsabilité y découlant, jouera au cas par cas.

La même réflexion vaut pour les forums, groupes de discussion, *chats*[157] ou sites *web* selon que ces lieux d'expression sont privés ou fermés. Si la participation au forum ou l'entrée au site ne nécessite qu'une demande d'abonnement toujours acceptée ou seulement l'introduction d'un mot de passe toujours donné, les communications au sein du forum ou les informations du site doivent être considérées comme publiques. A l'inverse, si les participants et internautes sont triés sur le volet, on peut admettre que le secret des télécommunications prévaudra. Ce même secret vaut bien évidemment aussi pour la téléphonie via Internet.

Pour conclure ce passage sur l'*e-mail*, rappelons que « *le caractère privé du mail ne couvre pas ce que le droit interdit* »[158]. Pour exemples, l'art. 10 al. 2 lit. b de la Loi sur le droit

---

Américaine a été condamnée à 15 mois de prison avec sursis pour avoir envoyé à un Suisse des photographies à caractère pédophile, rapporte Bernard DUMAS sur droit-net@cru.fr, le vendredi 11 juillet 1997 à 10h58.

153 R. v. Weir (1998), A.J. 155, 59 Alta. L. R. (3d) 319, (1998) W.W.W. 228.

154 RS 784.10.

155 Sébastien CANEVET, FAQ sur le courrier électronique, www.canevet.com.

156 François-Régis LEVOL, Liste Droit droit-net@cru.fr, Mardi 15 mai 1997, 1h04.

157 Le *chat* (traduction française : petite conversation, causette) est un mode d'utilisation d'Internet qui permet à deux ou plusieurs personnes de « bavarder » par écrit et en temps réel. Appelé aussi « bavardoir » en France, un tel service nécessite l'emploi du protocole IRC (*Internet Relay Chat*).

158 Eric BARBRY, Le droit du mail, 31 octobre 2000, journaldunet.com.

d'auteur interdit l'envoi par message électronique d'une œuvre protégée sans l'autorisation de son ayant droit et, comme cité dans la note de bas de page (152), l'envoi d'images pédophiles est tout aussi réprimé.

4.3 Au travers de l'*e-bombing*

On a déjà parlé plus haut de l'*e-bombing,* ou *mail bombing*, en tant que moyen de justice propre. On répétera qu'on parle ici d'un « *bombardement d'une boîte de courrier électronique par l'envoi d'une quantité astronomique de messages* ». En imaginant que les messages peuvent être de grosse taille, l'usage de la boîte *e-mail* de la victime peut se révéler impossible pendant quelque temps. Cette boîte étant limitée dans sa taille par l'entité la mettant à disposition, généralement un fournisseur d'accès à Internet, il est fort possible que *des e-mails* légitimes ne puissent arriver dans la *mailbox* de l'internaute pour la raison suivante : « *User quota exceeded* ». Selon les circonstances, la non réception d'un *e-mail* peut s'avérer préjudiciable, notamment pour une société commerciale. Afin de supprimer l'engorgement de sa boîte, la victime peut télécharger tous les messages, ce qui verrait le cas échéant sa facture de connexion devenir salée. Mais il devrait plutôt utiliser un logiciel tel que Spambuster, qui permet de supprimer des *e-mails* dans le serveur du gérant de service de messagerie électronique, sans les télécharger. Une autre solution consiste à supprimer son compte *e-mail* et donc à changer d'adresse. Cette dernière solution amène le risque de perdre des messages électroniques importants.
Si le *mail bombing* peut à l'évidence créer un dommage chez la victime, il ne sera pas chose aisée de trouver la norme protectrice nécessaire à la condition de l'illicéité de l'agissement. On pourrait imaginer l'application de l'art. 144bis du CPS, qui ne semble pas exiger une mise hors d'usage définitive de la *mailbox*[159]. Dans son message, le Conseil fédéral a en effet exprimé que l'art. 144bis du CPS ne condamne pas seulement les formes d'atteinte qui aboutissent à la détérioration des données, mais aussi celles « *dont les effets sont comparables, dans la mesure où l'ayant droit est empêché d'accéder aux données et les utiliser* »[160]. David ROSENTHAL[161] propose, avec prudence, de punir le *spamming* par l'application de l'art. 179^{septies} du CPS. Cette disposition pourrait encore mieux s'appliquer au *mail bombing*, car on retrouve dans cet acte la méchanceté exigée par l'article en question. Il n'empêche qu'une interprétation téléologique est nécessaire à l'application de ces normes pénales, qui n'ont pas été pensées pour l'*e-bombing*.

4.4 Au travers du *spamming*

Le *spamming* est une technique de prospection de masse visant à adresser, grâce à un robot de gestion d'adresses électroniques, un même message, souvent publicitaire, à une multitude de personnes, voire de *newsgroups*. Généralement, cette pratique ne crée que de simples désagréments à l'internaute : il doit effacer les *spams*, messages qui lui sont inutiles. La survenance d'un véritable dommage est rare. Même si dommage il y avait, la réparation n'aurait sûrement pas lieu car, comme l'explique Laurent MOREILLON[162], aucune disposition pénale actuelle ne se prête réellement à la condamnation du *spamming* et la norme protectrice nécessaire sera souvent introuvable. Dans tous les cas, les questions découlant de cet agissement tiennent surtout de la protection des données et de la concurrence déloyale. Nous n'aborderons pas cette problématique.

---

[159] Laurent MOREILLON, Délits, p. 23.
[160] FF 1991 II 982.
[161] David ROSENTHAL, Unverlangte Weber-E-Mail ohne Rechtsfolgen ?, Medialex 4/1999 p. 204.
[162] Laurent MOREILLON, Délits, p. 24.

B. Le fournisseur d'accès à Internet (*access provider*)

1. Notions

Le fournisseur d'accès à Internet[163] offre à ses abonnés, particuliers ou entreprises, une connexion au réseau Internet. En mettant son serveur, connecté en permanence à Internet, à la disposition de ses abonnés, le fournisseur leur permet l'accès à l'ensemble des informations disponibles sur Internet.
Le contrat d'abonnement, peut être payant ou non[164]. L'accès à Internet n'est généralement pas le seul service compris dans le contrat d'abonnement. Tout fournisseur d'accès digne de ce nom procure en effet un compte *e-mail* à son client. De plus, nombreux sont les fournisseurs d'accès qui exploitent un *news server* et permettent ainsi à l'abonné l'accès à un choix de *newsgroups*.

En tant qu'il fournit un service de télécommunication, le fournisseur d'accès doit, conformément à l'art. 4 al. 2 de la loi fédérale sur les télécommunications (LTC), annoncer son activité à l'Office fédéral de la communication. En Suisse, c'est l'unique formalité pour offrir un tel service.

Il faut noter que pour accroître leurs performances, les fournisseurs d'accès à Internet posent et utilisent des *proxy servers*. L'installation de relais est aussi nécessaire. Nous verrons plus tard si de telles pratiques peuvent amener la responsabilité du fournisseur[165].

Il faut encore préciser que le fournisseur d'accès traditionnel est lui-même client de plus grands fournisseurs d'accès, propriétaires de *backbones*[166] et mentionner que les universités et entreprises qui offrent des postes de connexion, respectivement à leurs étudiants et employés, ne sont pas des *access providers*. Ces dernières entités disposent elles-mêmes d'un accès à Internet, dont elles font profiter les personnes qui lui sont affiliées.

2. La responsabilité pour les contenus illicites auxquels le fournisseur a donné accès

Les fournisseurs d'accès à Internet se décrivent souvent comme de « simples tuyaux » ou des « tronçons de route ». Or, on ne peut généralement pas rendre responsable des accidents le propriétaire des routes sur lesquelles ils ont eu lieu. En tant que pur intermédiaire, les *access providers* demandent leur totale irresponsabilité, assurant qu'ils n'ont aucun lien avec les informations par eux transférées.
Mais, le fournisseur d'accès est un élément obligatoire dans le processus de visualisation des contenus d'Internet. Par conséquent, on ne peut pas, a priori, écarter sa responsabilité. La

---

163 Comme exemple suisse, on peut citer Bluewin.

164 Concernant l'accès à un réseau téléphonique traditionnel, la tendance est à la gratuité de l'abonnement. Mais ce mode de connexion disparaîtra prochainement au profit des déjà très utilisées connexions par câble TV et surtout des connexions à large bande telles que l'ADSL (*Asymmetric Digital Subscriber Line*). La gratuité s'évanouira alors, en tout cas pendant quelques temps.

165 Cf. Partie 3 B. 3 p. 52 et D. 2 p. 59.

166 Un *backbone* (en français, colonne vertébrale) est un « *réseau central très rapide qui connecte une multitude de petits réseaux* », selon le site http://www.dicofr.com. Pour plus de détails, voir Arnaud DUFOUR, Internet, p. 8ss.

question de la responsabilité du fournisseur d'accès est d'autant plus importante que le lésé serait bienheureux de pouvoir actionner avec succès ce prestataire technique. Il ne faut pas perdre de vue que, même si cela s'avère possible, poursuivre l'auteur est souvent inutile et que beaucoup d'hébergeurs sont intouchables, en particulier lorsqu'ils sont domiciliés aux Etats-Unis et protégés par le Premier Amendement.
Examinons tout d'abord quelques cas de jurisprudence, ainsi que la législation relative à la responsabilité des fournisseurs d'accès.

2.1 La jurisprudence

En Suisse, aucune décision ne touche directement les fournisseurs d'accès à Internet. Le jugement qui mit un terme à l'affaire dite du « 156 » ou du « téléphone rose » pourrait néanmoins servir de guide.
A l'étranger, la jurisprudence en matière de fourniture d'accès est de manière générale moins riche que celle concernant les prestataires d'hébergement. L'affaire CompuServe a, à l'époque, défrayé la chronique et mis le monde d'Internet en émoi.
Globalement, les différents parquets ont été très prudents quand à l'éventuel engagement de responsabilité des fournisseurs d'accès.

2.1.1 La jurisprudence suisse : l'affaire dite du 156[167]

Le 7 mai 1991, Monsieur Rosenberg, le directeur général du département des télécommunications des PTT de l'époque, décida l'introduction du télékiosque 156 à titre d'essai, essai qui débuta le 1er octobre 1991. Le système du télékiosque permet à un exploitant de faire écouter des enregistrements sonores. A l'époque en tout cas, il suffisait d'un raccordement téléphonique pour y accéder. Suite à la lettre du Procureur général du canton de Vaud du 11 octobre 1991, le responsable des PTT a su que des publications à caractère pornographique étaient disponibles sur le télékiosque 156, chose dont il devait d'ailleurs se douter. Mais pour les PTT, « *des mesures ne pourraient être prises que lorsqu'un jugement pénal définitif et exécutoire rendu contre les abonnés concernés aurait été notifié* ». Les PTT ajoutèrent qu'ils « *n'ont ni le devoir, ni le droit de soumettre les conversations téléphoniques à des contrôles et que l'abonné est seul responsable de ses messages* » : les fournisseurs d'un télékiosque ne pourraient pas être tenus pour responsables des contenus qu'ils véhiculent.
Le TF n'a pas été de cet avis. Il a jugé qu'en continuant à mettre à disposition ce télékiosque, afin de le rentabiliser, Monsieur Rosenberg s'est rendu coupable, au sens de l'art. 25 du CPS, de complicité de publications obscènes, respectivement de pornographie, car les enregistrements pornographiques étaient accessibles à des jeunes de moins de 16 ans.
La condamnation pénale a surtout tenu au fait que les PTT avaient créé une infrastructure qui rendait les agissements prévisibles et l'avaient maintenue après avoir été « *informés et mis au pied du mur par la lettre du Procureur vaudois* ». Il y a donc eu inertie alors qu'il y avait pouvoir et savoir.

L'Office fédéral de la justice a considéré que cette jurisprudence est applicable aux fournisseurs d'accès[168]. Nous ne partageons pas ce point de vue. Bertil COTTIER admet la possible analogie avec les hébergeurs, mais exprime de très gros doutes concernant les fournisseurs d'accès[169]. Il faut dire qu'un fournisseur d'accès ne met pas à disposition des installations propres à commettre des infractions, mais offre seulement l'accès à Internet, outil

[167] Rosenberg c. Procureur général du canton de Vaud, RO ATF 121 IV 109.
[168] OFJ, Internet. Le nouveau média interroge le droit, Bern 1996, ch. II. 2. b.
[169] Bertil COTTIER, Conférence non publiée.

qui permet ce genre d'agissements. De plus, le fournisseur d'accès n'a généralement aucun intérêt - économique - à ce que transitent par son système des contenus illicites. Surtout, le fournisseur de télékiosque peut mettre fin, sans problème, à tout agissement illicite. Ce n'est pas le cas du fournisseur d'accès, comme nous le verrons plus tard[170].

2.1.2 La jurisprudence étrangère : l'affaire CompuServe[171]

En 1995, constatant que CompuServe Information Services GmbH - ci-après CompuServe GmbH - permettait d'accéder à des *newsgroups* à caractère illicite, le Ministère public munichois assigna Felix Somm, le directeur de CompuServe GmbH de l'époque, à couper l'accès à ces groupes de discussion. En fait, Felix Somm n'avait aucun moyen technique de supprimer cet accès. En effet, c'est la maison-mère de CompuServe GmbH, CompuServe Inc., qui hébergeaient les groupes de discussion sur son *news server* et les mettait à disposition de tous les clients de CompuServe des *newsgroups* au moyen d'un *frame relay*[172]. Felix Somm répercuta donc la demande à CompuServe Inc., qui bloqua l'accès à quelque 282 *newsgroups*. Leur fermeture déclencha une levée de boucliers parmi les abonnés de CompuServe, ce qui amena une vague de résiliation d'abonnements. Il est vrai que si ces groupes de discussion étaient illégaux en Allemagne, la plupart étaient tout à fait licites aux Etats-Unis : dans le lot, il y avait même un *newsgroup* qui traitait de la vie sexuelle des handicapés. En 1996, la firme américaine réouvrit les *newsgroups* litigieux - à l'exception des rares groupes au nom manifestement explicite -. Elle estimait qu'elle prenait les mesures qu'on pouvait attendre d'elle en mettant à disposition de chaque abonné le logiciel CyberPatrol, qui permet à l'internaute de censurer les *newsgroups* de son choix.
Conséquemment à la nouvelle attitude de CompuServe, les autorités pénales bavaroises inculpèrent, en février 1997, Felix Somm pour propagation de messages à caractère pédophile, zoophile et violent.
En mai 1998, contre toute attente et même à l'encontre du réquisitoire du Procureur, l'Amtsgericht de Munich[173] condamna à deux ans de prison avec sursis et à 100.000 Deutschmark d'amende le dirigeant de la filiale germanique pour avoir en connaissance de cause diffusé des contenus pornographiques en donnant accès à certains *newsgroups* et sites *web*. Selon le tribunal, CompuServe GmbH avait connaissance des contenus illégaux et le blocage de ceux-ci était techniquement possible et raisonnable, considérant qu'il était possible pour CompuServe Inc. de bloquer l'accès aux contenus illicites uniquement pour les abonnés allemands[174]. Si CompuServe n'a pas agi, ce serait uniquement par peur de perte de profits. En raisonnant sur la base l'art. 2 al. 3 du *Strafgesetzbuch* interprété selon l'art. 5 al. 2 du *Teledienstgesetz* (TDG), la cour a donc jugé le dirigeant coauteur de l'infraction.

Ce jugement a provoqué un tollé parmi les professionnels d'Internet. Il est vrai qu'il avait pour conséquence de rendre responsable un fournisseur d'accès à Internet de tout contenu illicite présent sur Internet et d'obliger le fournisseur à des contrôles et filtrages techniquement impossibles. En cas de confirmation, une telle jurisprudence aurait presque

---

[170] Cf. Partie 3 B. 2.3.2 p. 44.
[171] Pour une foultitude d'informations sur cette affaire, voir le site « The Somm Case », disponible à l'adresse http://www.digital-law.net/somm.
[172] Un *frame relay* est « *protocole de communication utilisé sur les longues distances* », selon le site http://www.dicofr.com.
[173] AG Munich, arrêt du 28 mai 1998, NJW 1998, p. 2836ss.
[174] Ce qui était faux, en tout cas à l'époque, chose confirmée par un expert de l'Office fédéral - allemand - pour la sécurité des techniques d'informations.

sonné le glas des prestataires techniques[175] et donc d'Internet. Si l'intention du juge n'était pas mauvaise[176], elle montre néanmoins son incompréhension du cyberespace.

Heureusement, dans son arrêt du 17 novembre 1999[177], la Cour d'appel de Munich a annulé cette décision de non-sens et acquitté Felix Somm. De l'avis de ce tribunal, il n'y avait tout d'abord ni « *Tatherrschaft* », ni intention de la part de CompuServe GmbH de violer la loi afin d'obtenir un profit et on ne pouvait donc pas qualifier la filiale allemande de coauteur. Ensuite, l'Amtsgericht avait confondu à tort CompuServe Inc. et CompuServe GmbH[178] : même très liées, elles ne constituent pas moins deux entités juridiques différentes. Et si CompuServe Inc. tenait à disposition de ses abonnés les *newsgroups* et aurait pu se voir appliquer l'art. 5 al. 2 du TDG, il n'en était rien de CompuServe GmbH, qui ne pouvait être défini que comme un simple fournisseur d'accès. L'art. 5 al. 3 du TDG trouvait donc application. Et selon cette disposition, le prestataire de services qui ne donne que l'accès à des contenus illicites ne peut être tenu pour responsable. Même en application de l'art. 5 al. 2 du TDG, le dirigeant n'aurait d'ailleurs pas dû être condamné, car « *le blocage par un fournisseur d'accès allemand d'informations de nature pornographique provenant des Etats-Unis n'était pas raisonnablement possible* »[179].

2.2 La législation étrangère

2.2.1 Le *Teledienstgesetz*

La première phrase de l'art. 5 al. 3 du TDG a le contenu suivant : « *Dienstanbieter sind für fremde Inhalte, zu denen sie lediglich Zugang zur Nutzung vermitteln, nicht verantwortlich* ».

2.2.2 La directive sur le commerce électronique

L'art. 12 de la directive, nommé « Simple transport (« Mere conduit ») », dit :

1. Les Etats membres veillent à ce que, en cas de fourniture d'un service de la société de l'information consistant à transmettre, sur un réseau de communication, des informations fournies par le destinataire du service[180] *ou à fournir un accès au réseau de communication, le prestataire de services ne soit pas responsable des informations transmises, 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.

---

[175] Quelques intermédiaires techniques, à l'image d'AOL, ont ainsi déclaré que ce jugement mettait en péril leurs activités commerciales en Allemagne.

[176] La décision était « *essentiellement motivée par des raisons d'ordre public et de protection de la jeunesse* », selon Lionel THOUMYRE, Réglementation.

[177] LG Munich I, arrêt du 17 novembre 1999, NJW 2000, p. 1051ss.

[178] Uwe WALDNER, Internet-Nutzung, p. 363 ; Markus BERNI, E-Commerce, p. 86.

[179] Francis SEGOND, Affaire CompuServe Allemagne, résumé de la décision en appel, disponible sur le site http://www.canevet.com.

[180] L'art. 2 lit. d de la directive sur le commerce électronique définit le « destinataire du service » comme « *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* ». Cette expression désigne donc autant le consommateur de l'information que le fournisseur de l'information, professionnel ou non.

2. Les activités de transmission et de fourniture d'accès visées au paragraphe 1 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.

3. Le présent article n'affecte pas la possibilité, pour une juridiction ou une autorité administrative, conformément aux systèmes juridiques des Etats membres, d'exiger du prestataire qu'il mette un terme à une violation ou qu'il prévienne une violation.

La directive vise à restreindre la responsabilité du fournisseur d'accès, en tant qu'il se limite au transport de données. S'il n'a qu'un rôle passif, s'il reste neutre, il n'encourra pas le risque de voir sa responsabilité engagée.

2.3 Développements

2.3.1 Le contrôle de la licéité des informations qui transitent par les installations du fournisseur d'accès

L'accès fourni vaut pour Internet et ses services dans leur ensemble et non pour des services ou informations spécifiques : le fournisseur d'accès est une « *porte qui ouvre sur Internet* »[181]. Le fournisseur connaît les protocoles techniques utilisés par ses abonnés - HTTP[182] pour le *web*, par exemple - mais pas le contenu de leurs échanges[183]. La quantité de données transitant par la « porte » est telle que tout contrôle systématique de leur licéité est impossible, à plus forte raison que l'information est découpée en paquets[184].
Les techniques de filtrage de contenu, dont on reparlera encore, sont techniquement très limitées et peuvent être facilement contournées[185]. Les critères de licéité et d'illicéité sont trop nombreux pour les incorporer correctement dans un logiciel et aucun programme ne pourrait les utiliser de façon idoine. Au niveau juridique, séparer le bon grain de l'ivraie est une opération délicate. N'est pas juge qui veut, en compétence et en légitimité. Actuellement, le filtrage est à un point inefficace qu'il ne peut raisonnablement être exigible. De plus, c'est à coup sûr qu'il contreviendrait illégitimement à la liberté d'expression[186] : comme le dit si bien Jérôme BENEDICT, « *il s'agit de ne pas ériger le fournisseur d'accès, qui n'ouvre qu'une passerelle, en censeur des données qui transitent sur Internet* »[187]. En outre, dans un monde où l'instantanéité prime, peut-on se permettre de réduire grandement la vitesse de transfert des données pour un résultat minçolet ? On en revient au concept du développement d'Internet.

---

[181] Meryem MARZOUKI, Quelques définitions, Après-Demain, revue de la Ligue des droits de l'homme, n° 430-431, janvier-février 2001, disponible à l'adresse suivante : http://www-asim.lip6.fr/~marzouki/perso/publi/apresdemain2.html.

[182] L'HTTP (*HyperText Transfer Protocol*) est la méthode utilisée pour transporter des pages *web* sur le réseau.

[183] Christian PAUL, Libertés, p. 30.

[184] Cf. Partie 3 D. 1 p. 59.

[185] La cryptographie, l'usage de codes même simplistes ou la non-utilisation de certains mots douteux constituent des solutions simples et peu chères pour les cyberdélinquants.

[186] Thibault VERBIEST et Etienne WÉRY (Responsabilité, p. 170) pensent que, en sus de la liberté d'expression, la censure privée contrevient sûrement à des principes tels que la présomption d'innocence ou la compétence du pouvoir judiciaire pour rendre la justice.

[187] Jérôme BENEDICT, Responsabilité, p. 41. L'auteur nous fait part d'une théorie intéressante. Selon lui, les dispositions protégeant le secret des télécommunications, notamment l'art. 13 al. 1 de la Constitution fédérale, « *interdisent toute forme de filtrage systématique des données circulant sur les canaux télématiques ordinaires* » (Jérôme BENEDICT, Responsabilité, p. 32). Si cet avis s'avérait juste, on pourrait alors ne plus se poser la question du contrôle de la licéité des informations transitant par le service du fournisseur d'accès.

La doctrine est unanime[188] : on ne peut imposer au fournisseur d'accès une obligation de contrôle des millions d'informations qui transitent par ses installations. L'inverse ne serait « *ni raisonnable sur le plan technique, ni satisfaisant sur le plan démocratique* »[189], ni juridiquement acceptable, compte tenu de la protection nécessaire de la liberté d'expression. Cette opinion est conforme à l'art. 15 al. 1 de la directive sur le commerce électronique, qui prévoit que « *les Etats 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* ». Il y a consensus ! Que ce mot est doux dans le monde d'incertitude que forme Internet…

2.3.2 L'intervention du fournisseur d'accès en cas de connaissance

Si le fournisseur d'accès à Internet n'a, a priori, pas à connaître les informations se trouvant sur le réseau, qu'en est-il de son pouvoir d'intervention, s'il est averti de l'existence de tel ou tel contenu illicite ? A la différence du fournisseur d'hébergement, l'*access provider* n'est pas lié contractuellement avec l'auteur du contenu illicite, qu'il ne connaît en principe pas. Il ne peut supprimer un contenu à la source. Quoiqu'il fera, le site au contenu illicite pourra être visité par l'entremise d'un autre fournisseur d'accès. Si des procédés de blocage d'accès à un site sont techniquement possibles à mettre en place, la controverse est vive quant à savoir si de telles mesures sont raisonnablement exigibles du fournisseur d'accès. La Police fédérale y est allée de son avis[190].
Techniquement, le fournisseur d'accès peut tout d'abord bloquer l'adresse IP[191] du serveur *web*[192] au niveau du routeur ou exclure certains noms de domaine - par exemple aryanbooks.com - au niveau du *domain name server* (DNS). Tout le serveur en question devient alors inaccessible. Cette technique de blocage ne convient donc pas, lorsque le contenu illicite est faible en proportion de tous les contenus bloqués[193]. Elle ne conviendrait en tout cas pas lorsque sont en jeu des prestataires d'hébergement. On voit mal tous les sites hébergés par Geocities devenir inaccessibles, à cause d'un seul propriétaire de site malintentionné. Par contre, la mesure est efficace lorsque l'auteur a son propre serveur.
Au travers de son serveur *proxy*, le fournisseur peut bloquer une page précise. Encore faut-il que ce serveur ne soit pas contourné, volontairement ou non, par l'internaute. Un serveur *proxy* « transparent » serait alors une possibilité, car ce serveur est automatiquement et invisiblement utilisé par le client, de sorte que ce dernier ne peut pas directement visiter le site voulu.
Toutes ces méthodes ont des inconvénients. Elles diminuent les performances du fournisseur d'accès, lui prennent du temps « administratif » et peuvent lui coûter bonbon. De plus, elles

---

188 Pour exemples, Robert G. BRINER, Die Rechtsstellung des Access Providers, in Information Highway, Bern 1996, p. 521 ; Police fédérale suisse, Responsabilité pénale, p. 13 : « *Il n'est pas concevable, ni rationnel de rechercher activement et individuellement des contenus répréhensibles sur Internet en raison du changement et de l'augmentation que subissent quotidiennement les données ; une telle mesure ne peut donc être exigée* ».

189 Gérard HAAS et Olivier DE TISSOT, Atteintes.

190 Police fédérale suisse, Responsabilité pénale. Elle s'est à cet égard inspirée de l'ouvrage de David ROSENTHAL, Current Problems and Possible Strategies for Combating Racism on the Internet, disponible à l'adresse http://www.rvo.ch/docs/unracism.pdf, ainsi que de l'ouvrage d'Ulrich SIEBER, Verantwortlichkeit im Internet – Technische Kontrollmöglichkeiten und multimediarechtliche Regelungen, Munich 1999.

191 L'adresse IP (*Internet Protocol*) ou adresse Internet est un numéro unique qui identifie chaque ordinateur sur Internet.

192 Il faut noter que les remarques faites pour les serveur *web* valent, globalement, aussi pour les serveurs FTP.

193 Dirk SCHUHMACHER, Sperrungsverpflichtungen.

peuvent être évitées par l'usage d'un « *anonymizer*[194] », qui cache l'adresse IP du contenu litigieux. Les sites miroirs doivent aussi faire l'objet de mesures. Finalement, il ne faut pas oublier que rien ne vaut une intervention à la source. L'*access provider* n'est qu'un chemin, parmi d'autres, pour accéder au contenu. Même si tous les fournisseurs d'accès nationaux bloquent l'accès à un site, une personne domiciliée en Suisse peut toujours s'abonner auprès d'un *access provider* étranger. On revient au problème de l'absence de solution internationale.

En résumé, pour la Police fédérale, « *si le fournisseur d'accès est en possession d'indices concrets émanant d'une autorité de poursuite pénale et liés à de présumés contenus illicites circulant sur le réseau, il est invité à procéder à des blocages, pour autant que ceux-ci soient raisonnables* »[195]. Ces mesures doivent être considérées comme raisonnables s'il s'agit du blocage de l'adresse IP ou du nom de domaine si le contenu répréhensible « *est stocké sur un site ayant sa propre adresse IP* », et du blocage de l'URL[196] des pages litigieuses dans le serveur *proxy*[197]. Il s'agit là de l'attitude exigée du fournisseur d'accès sous l'angle de la responsabilité pénale. Comment transposer une telle analyse en matière civile ? Peut-on aussi exiger un tel comportement du fournisseur sous l'angle de la responsabilité civile ? La faute civile peut être examinée indépendamment de la faute pénale[198]. Ce qui est raisonnable en pénal ne l'est pas forcément en civil.

Avant d'aller plus avant, examinons encore deux cas réels touchant des mesures de blocage.

En Suisse, la Commission fédérale des jeux a assigné, le 1er novembre 2000, plus de 200 fournisseurs d'accès suisses à bloquer l'accès à quelque 700 casinos virtuels, sous peine d'une amende pénale pouvant s'élever à un million de francs, pour complicité d'exploitation de ces maisons de jeu virtuel. Cette décision, qui était basée sur la Loi sur les maisons de jeu[199], le Code pénal suisse et la jurisprudence de l'arrêt Rosenberg, semblait légalement justifiée. Mais, par l'entremise du *Verband Inside Telecom* (VIT), les *access providers* suisses ont clairement refusé de s'exécuter. Devant une telle opposition, la Commission fédérale des jeux s'est résignée.

En Allemagne, en février 2002, la *Bezirksregierung* de Düsseldorf a ordonné à plus de 80 fournisseurs d'accès la mise en place de mesures de blocage sur la base des paragraphes 8 et 18 du *Mediendienstestaatsvertrag*. C'est la première fois que de telles mesures étaient imposées en Allemagne. Un de leur buts est de protéger la jeunesse, en empêchant l'accès à des sites racistes et révisionnistes situés sur des serveurs américains[200]. La *Bezirksregierung* de Düsseldorf tient pour raisonnables et proportionnelles au but, des mesures telles que l'exclusion du domaine du serveur de nom de domaine et la non prise en considération d'adresses IP dans le routeur ou dans le serveur *proxy* du fournisseur d'accès.
Les réactions ne se sont pas faites attendre. Pour le site http://www.netzzensur.de, ces mesures de filtrage constituent clairement une censure interdite par les principes démocratiques. Le

---

194 Un *anonymizer* est un tiers de confiance qui substituent son adresse IP à celle de l'internaute. Pour plus de détails, cf. Partie 3 I. 3 p. 111.

195 Police fédérale suisse, Responsabilité pénale, p. 13. Selon Bertil COTTIER (Conférence non publiée), la notification par l'autorité de poursuite pénale est le cas idéal mais la Police fédérale n'exclut pas un certain devoir d'action de la part du fournisseur d'accès en cas de notification d'une autre autorité - par exemple un tribunal civil -, voire d'un tiers. L'auteur fait par contre remarquer qu'un article de presse n'est pas suffisant.

196 L'abréviation URL signifie *Uniform (ou Universal) Resource Locator*. Il s'agit simplement de l'adresse d'un site sur le Réseau. Comme exemple, l'URL du site de la Migros est : http://www.migros.ch.

197 Police fédérale suisse, Responsabilité pénale, p. 12.

198 Cf. l'art. 53 du CO.

199 RS 935.52.

200 Tel que le tristement célèbre http://www.stormfront.org.

site est même allé jusqu'à comparer la situation du Nordrhein-Westfalen avec celle de l'Iran ou de la Chine. Les juristes allemands se posent aussi la question délicate de la compatibilité de ces mesures de blocage vis-à-vis de la liberté d'information. Andreas NEUMANN[201] doute de l'aptitude des mesures à atteindre leur but et se demande si la *Bezirksregierung* de Düsseldorf a bien pesé les droits en question, c'est-à-dire la protection de la jeunesse et le droit à l'information, tel qu'il est exprimé dans l'art. 5 al. 1 de la *Grundgesetz für die Bundesrepublik Deutschland* (GG) du 23 mai 1949[202]. En réfléchissant sur la base de liberté de la presse, Thomas STADLER arrive à la conclusion que le paragraphe 18 du *Mediendienstestaatsvertrag* est contraire à la Constitution allemande et que les « *Sperrungsverfügungen* » sont illégales ; il ajoute qu'il ne faut ordonner la prise de mesures à un fournisseur d'accès que si le propriétaire du site et l'hébergeur de ce site ne peuvent être recherchés, en précisant que l'*access provider* ne bloque jamais un contenu, mais le cache seulement à ses clients[203].

La *Bezirksregierung* de Düsseldorf annonçant, à la fin de l'année 2001, la future assignation, le *provider* ISIS avait anticipé la mise en place des mesures de blocage de sites[204]. Il a notamment bloqué les adresses litigieuses dans son serveur de nom de domaine (*domain name server* ou DNS). Un technicien d'ISIS fait remarquer qu'il suffit, pour l'internaute, de modifier les options Internet du système d'exploitation de son ordinateur personnel, plus précisément, les propriétés touchant au protocole Internet - TCP/IP -, pour que la mesure devienne inutile. La plupart des « surfeurs » ne paramètrent pas le DNS, si bien qu'ils utilisent automatiquement celui de leur fournisseur d'accès. Mais c'est un jeu d'enfant que d'entrer l'adresse IP d'un serveur de nom de domaine sans « *Web-Blockaden* ». Apprenant la nouvelle, le Chaos Computer Club[205] a d'ailleurs communiqué l'adresse Internet de plusieurs serveurs de domaine utilisables. Des dires du même technicien d'ISIS, la solution liée au DNS est « *schwachsinning* ». Il ajoute que le blocage de l'adresse IP au niveau du routeur toucherait des milliers de serveurs *web*. La *Fachhochschule* de Cologne a expérimenté quelques techniques liées à l'adresse IP, mais les tests ont été arrêtés lorsque les étudiants ne purent plus accéder à certains sites tels que celui de Yahoo... En fait, toujours selon l'expert informaticien, même un système à plusieurs millions de francs ne pourrait pas garantir des blocages efficaces. 99% des gens ne vont jamais sur les sites racistes et les personnes vraiment intéressées à se nourrir de tels contenus trouveront toujours un moyen de contourner les barrières mises en place.

Au final, l'avis que porte la doctrine majoritaire sur les mesures de blocage que connaissent les fournisseurs d'accès du Nordrhein-Westfalen est plutôt négatif. Ces mesures n'auraient principalement qu'un effet placebo et violeraient la *Grundgesetz*. Si des mesures de blocage contre des sites autant atroces que ceux qui étaient visés en Allemagne suscitent une telle polémique, on peut se demander ce qu'il adviendra de décisions qui viseraient à supprimer l'accès à un site exposant des photos de femmes dénudées sans leur autorisation. En fait, dans le cas présent, nous ne pensons pas que ces mesures soient autant inutiles que certains peuvent le croire. Si le but des mesures en question était d'empêcher même les plus malins d'accéder à ces sites litigieux, on comprendrait l'hilarité de certains. Mais le but était ici de diminuer la

---

201 Andreas NEUMANN, Ordnungsrechtliche Sperrungsverfügungen und die Informationsfreiheit nach Art. 5 Abs. 1 S. 1 2. Alt. GG, disponible à l'adresse suivante : http://www.artikel5.de/artikel/sperrunginffreiheit.html.

202 BGBl. I S. 1, disponible à l'adresse suivante : http://www.artikel5.de/gesetze/art5.

203 Thomas STADLER, Sperrungsanordnungen gegenüber Access-Providern, 2002, www.afs-rechtsanwaelte.de.

204 Ce passage est largement inspiré de Stefan KREMPL, Netzsperre für Fritzchen Doof, heise.de, 22.11.2001, disponible à l'adresse suivante : http://www.heise.de/tp/deutsch/inhalt/te/11175/1.html.

205 http://www.ccc.de.

possibilité pour de jeunes enfants de tomber par hasard sur des sites qui pourraient les choquer. Il ne faut pas sans cesse avancer l'argument du tout ou rien. Si les mesures de blocage sont bénéfiques, tout en étant raisonnablement exigibles, il y a lieu le cas échéant de les imposer.

En matière civile, on peut penser que les mesures de blocage examinées ne seront généralement pas raisonnablement exigibles. Cela dépendra bien évidemment du cas d'espèce, mais les effets bénéfiques de telles mesures seront trop souvent presque nuls. Devant le désespoir d'une personne diffamée, le juge devra garder ouverts les yeux sur la réalité technique et constater que les mesures de blocage impliquent de nombreux inconvénients pour le fournisseur d'accès et risquent de limiter gravement la liberté d'expression. Au contraire du domaine pénal, il ne faut pas oublier que, sur le plan civil, c'est souvent l'intérêt d'une seule personne qui est en jeu et non celui de la société. L'intérêt de la victime mérite certes d'être protégé, mais cette protection trouve plus facilement des limites que celle de l'intérêt de la société.
Mais attendons de voir les prochaines avancées technologiques en matière de techniques de filtrages et de blocage. Les mesures imposées par la *Bezirksregierung* de Düsseldorf ont eu le mérite d'amener les scientifiques à s'intéresser sérieusement à ce problème. L'Université de Dortmund s'est en effet lancée dans le test d'un nouveau produit qui devrait permettre, à moindre prix, de bloquer l'accès à certaines pages et de compliquer considérablement son contournement[206]. Le programme en question ne pourra pas chercher les contenus illicites mais, en cas de connaissance de l'illicéité de tel site, il empêchera la circulation vers le numéro IP du serveur suspect. Les contenus interdits seraient alors impossibles à appeler, les contenus légaux restant lisibles. Ce logiciel miracle est à l'heure actuelle loin d'être commercialisé mais, on le répète, lorsque l'état de la technique permettra un blocage précis de site illégaux inatteignables, on ne voit pas pourquoi un juge se priverait d'imposer la mise en place d'une telle mesure. Dirk SCHUHMACHER dit que pour juger du caractère raisonnable d'une mesure de blocage, il faut prendre en compte l'infrastructure technique concrète du *provider*[207]. Le jour où un logiciel de blocage de contenus peu cher et efficace sera sur le marché, plus personne ne pourra se retrancher derrière l'éventuel caractère irraisonnable de la mesure.

Si, dès mars 1996, un tribunal néerlandais laissait la porte ouverte à l'intervention du fournisseur d'accès, en précisant que la responsabilité de ce prestataire pouvait être engagée si la situation illicite lui était connue[208], il reste à déterminer ce que l'on entend par connaissance. Cette condition de connaissance est en tout cas remplie, en cas de notification d'une autorité judiciaire. Mais la notification du juge est-elle le seul moyen amenant juridiquement connaissance ? Selon David ROSENTHAL, il est évident que le fournisseur ne doit pas attendre un jugement pour agir : il se doit de prendre des mesures dès qu'il apprend par notification ou par hasard l'existence d'éléments concrets illicites, voire seulement probablement illicites. « *Ein vager oder allgemeiner Hinweis eines Kunden genügt dagegen nicht* »[209]. Il faut néanmoins relever que l'auteur ne semble pas différencier l'*access* et l'*host provider* dans son écrit.
En revanche, l'ancien art. 5 du TDG était interprété de telle façon qu'il n'obligeait pas le fournisseur d'accès à « *donner suite à une éventuelle mise en demeure qui lui serait adressée*

[206] Annecke WARDENBACH, Nazi-Propaganda : Forscher suchen Filter, WDR, 14.02.02, disponible à l'adresse suivante : http://online.wdr.de/online/computer/internet_aufraeumen/index.phtml.
[207] Dirk SCHUHMACHER, Sperrungsverpflichtungen.
[208] Thibault VERBIEST, Acteurs.
[209] David ROSENTHAL, Projekt, p. 111.

par un particulier »[210]. Au sujet du protocole de collaboration avec la justice que l'*Internet Service Provider Association* (ISPA) de Belgique a signé, son président, Eric PIETERS, a affirmé que les fournisseurs d'accès ne voulaient en aucun cas échapper à leur responsabilité, mais qu'ils ne devaient agir que s'ils étaient notifiés par une instance habilitée[211]. Le paragraphe 3 de l'art. 12 de la directive sur le commerce électronique semble exprimer la même opinion, puisqu'il permet aux Etats membres de prévoir qu'une autorité judiciaire ou administrative puisse demander au fournisseur d'accès de faire cesser la violation ou de la prévenir[212].

Aux USA, dans le cadre du CDA, dont on sait qu'il exonère les prestataires techniques de toute responsabilité pour le contenu de tiers et cela sans conditions, seul le juge peut légitimement demander à un *provider* de supprimer ou de restreindre l'accès à un message illicite. Ainsi, même si le fournisseur a une parfaite connaissance d'un contenu illicite, il n'a pas à réagir tant que le juge ne le lui a pas ordonné. C'est ainsi qu'en 1997, dans l'affaire Zeran v. America OnLine (AOL)[213], le demandeur s'était plusieurs fois plaint auprès d'AOL de messages diffamatoires postés sur un de ses forums de discussion par un internaute anonyme. Le plus grand fournisseur de services au monde n'avait pas supprimé les messages litigieux. La cause alla jusqu'à la Cour Suprême. Zeran reprochait à AOL sa non-réaction, notamment le fait ne pas avoir prévenu les usages de ses services que les *postings* étaient erronés. Mais, la Cour confirma les avis des cours inférieures et AOL échappa à toute responsabilité. Les cours concernées se sont basées sur l'idée que le *provider* risquerait de voir sa responsabilité engagée, s'il ne traitait pas le cas avec une grande attention. Or, les plaintes des usagers d'Internet seraient tellement fréquentes - par rapport à celles qui peuvent arriver sur le bureau d'un rédacteur de magazine - que le *provider* serait vite submergé et deviendrait une cible trop facile ou alors supprimerait sans autres tout message douteux, contrevenant ainsi au « *free speech* »[214]. Si AOL avait décidé d'agir, il aurait été considéré comme un « *good samaritan* ».
Cet arrêt, valable pour n'importe quel *provider*, instaure un régime d'immunité quasi totale qui est tout bonnement inacceptable vis-à-vis du mode de pensée juridique européen. Les principes s'y dégageant peuvent certes se justifier pour les fournisseurs d'accès, mais en aucune cas pour l'hébergeur, comme on le verra[215]. D'ailleurs, les décisions des tribunaux américains ont été fort critiquées par la doctrine du même pays, qui a mis en avant l'incompréhension de la volonté du législateur. Il n'empêche que si le *Digital Millenium Copyright Act* prévoit qu'il peut être exigé du fournisseur d'accès la prise de mesures raisonnables de blocage, seuls les tribunaux peuvent faire cette injonction. Valérie SÉDALLIAN rapporte à ce propos que les cours doivent tenir compte de la « *possibilité technique de prendre la mesure de blocage sollicitée, de la charge imposée au prestataire,*

---

[210] Alain STROWEL et Nicolas IDE, Responsabilité. Les auteurs suivent ainsi l'avis de Thomas HOEREN, Liability in the Internet and the new German multimedia law regulations, A&M, 1998.4, p. 310.

[211] Eric PIETERS, Protocole de coopération Justice - Télécommunications – ISPA, http://www.ispa.be.

[212] Il est à noter que si l'Etat membre en question ne saisit pas cette opportunité, le fournisseur d'accès sera exonéré de toute responsabilité même s'il a clairement connaissance du contenu illicite, partant du fait que l'art. 12 al. 1 de la directive ne fait pas référence à la notion de connaissance. La France profite de l'art. 12 al. 3 de la directive : si la loi française sur la société de l'information est adoptée en l'état du 13 juin 2001, l'art. 43-8-3 de la loi n° 86-1067 du 30 septembre 1986 relative à la liberté de communication devrait permettre au président du tribunal de grande instance de prescrire en référé, à un fournisseur d'accès comme à un fournisseur d'hébergement, « *toutes mesures propres à faire cesser un dommage occasionné par le contenu d'un service de communication publique en ligne, telles que celles visant à cesser de stocker ce contenu ou, à défaut, à cesser d'en permettre l'accès* ».

[213] Kenneth M. Zeran v. AOL, Inc., *U.S. Supreme Court*, Cert. Pet. 97-1488 (22 juin 1998).

[214] Cf. notamment Kenneth M. Zeran v. AOL, Inc., *U.S. District Court of Eastern District of Virginia*, 958 F. Supp. 1124 (1997).

[215] Cf. Partie 3 E. 2.3.2 p. 67.

des conséquences de la mesure sur l'accès à d'autres sites ne contenant pas de matériel contrefaisant, et du préjudice subi par le titulaire du droit d'auteur si des mesures ne sont pas prises »[216].

En Suisse, sur le plan pénal, l'Office fédéral de la justice est, a priori, d'avis que seule une autorité pénale peut exiger du fournisseur une action si coûteuse. En Belgique, Eric PIETERS précisait que l'*access provider* « *n'est ni un juge ni une instance habilitée. Ce n'est pas au fournisseur d'Internet de juger de la matière ; c'est l'instance habilitée qui s'en charge* ». C'est l'avis d'un professionnel d'Internet. Or, il peut paraître critiquable que le prestataire puisse garder les bras croisés, alors qu'il sait pertinemment qu'un contenu lèse les droits d'une personne et qu'une réaction peut raisonnablement lui être exigée. C'est pourquoi nous pensons que, si la mesure de blocage est raisonnable, le fournisseur d'accès doit agir en cas de notification du lésé en tant que le contenu est *prima facie* illicite. Mais comme déjà relevé, le problème est que, pour l'instant, cette mesure sera jugée irraisonnable dans la plupart des cas.

Nous reviendrons sur la notion de connaissance, notamment lorsque nous traiterons de la responsabilité des prestataires d'hébergement[217]. Nous verrons en particulier que l'instauration de procédures de notification et de retrait des contenus serait bénéfique.

2.4 Les autres « obligations »[218]

Si les possibilités d'engagement de la responsabilité du fournisseur d'accès paraissent faibles, il ne faut pas pour autant l'épargner de mesures qui pourraient aider au retour de la convenance sur le réseau des réseaux, sans amener une censure privée malsaine. En ce sens, quelques obligations pourraient être exigées du fournisseur d'accès, afin qu'on ne puisse lui reprocher un manque de diligence. Elles transformeraient le fournisseur d'accès en une sorte d'auxiliaire de police et de justice, sans pour autant le charger comme un mulet[219]. Il faut remarquer qu'il est « à la mode » d'exiger de la part de certaines entités une collaboration avec les autorités, pas trop lourde mais très utile à la communauté[220].

Faisons un catalogue de ces obligations, dont la mise en place est en partie encouragée par l'art. 15 al. 2 de la directive sur le commerce électronique et qui se retrouvent notamment dans les lois et projets de transposition français et belge.

2.4.1 L'obligation de conserver et de communiquer les *logs*

Un certain anonymat empêche le lésé d'obtenir réparation du premier responsable[221]. Le premier type d'obligation est logiquement lié à l'identification de l'auteur. Le fournisseur d'accès doit garder les fichiers *logs*[222], qui contiennent, entre autres, les adresses IP des machines qui se sont connectées sur le serveur du fournisseur et qui permettent ainsi de

---

216 Valérie SÉDALLIAN, Responsabilité.

217 Cf. Partie 3 E. 2.3.2 p. 70.

218 Il n'est pas question d'obligations au sens traditionnel du droit suisse. Il s'agit de mesures, dont l'absence peuvent amener la négligence du fournisseur d'hébergement et donc sa responsabilité.

219 A l'inverse de nombreux auteurs, nous n'utilisons pas péjorativement les expressions « auxiliaire de justice » ou « auxiliaire de police ».

220 Il suffit de penser à la Convention sur la cybercriminalité ou à la Loi fédérale sur la surveillance de la correspondance par poste et télécommunication du 6 octobre 2000 (LSCPT, RS 780.1).

221 Nous étudions plus précisément l'anonymat du fournisseur de contenu plus tard : cf. Partie 3 I. 3 p. 111.

222 Un fichier *log* - ou un *log* - enregistre les informations (dates et heures) sur la connexion sur un serveur et les opérations y faites.

« remonter » à leurs utilisateurs ou du moins à leurs propriétaires. En ce sens, l'art. 15 de la Loi fédérale sur la surveillance de la correspondance par poste et télécommunication exige que les fournisseurs de services de télécommunication conservent « *durant six mois les données permettant l'identification des usagers ainsi que les données relatives au trafic et à la facturation* ». En France, l'art. 43-9 de la loi n° 86-1067 du 30 septembre 1986 relative à la liberté de communication instauré par la loi n° 2000-719 du 1er août 2000 prévoit que les fournisseurs d'accès - et les hébergeurs - doivent « *détenir et conserver les données de nature à permettre l'identification de toute personne ayant contribué à la création d'un contenu des services dont elles sont prestataires* ». L'art. 14 du projet de Loi sur la société de l'information prescrit une durée maximale de conservation d'une année, durée qui doit être définie plus précisément par un décret selon le type de la donnée de connexion. Une obligation liée à l'identification d'une personne pose bien sûr le problème de la protection des données personnelles et de la vie privée. C'est peut-être en ce sens que la Suisse a choisi un délai plutôt court. C'est peut-être aussi pour diminuer les frais du fournisseur d'accès. Les frais de conservation et de recherche sont en effet à sa charge et ils pourraient s'avérer plus que conséquents lorsqu'on voit le nombre de pages *web* brassées par jour. En France, la CNIL craint « *que le coût final d'une telle obligation soit reporté sur les internautes* »[223]. L'art. 16 de la LSCPT prévoit, lui, l'attribution d'une indemnité équitable.
Le problème est que l'obligation créée par la Loi fédérale sur la surveillance de la correspondance par poste et télécommunication ne vaut que concernant certaines infractions et que la communication des *logs* ne peut être exigée que par le service institué à cet effet. Il faut déchanter : la Loi fédérale sur la surveillance de la correspondance par poste et télécommunication ne servira que si le dommage du lésé est constitutif d'une infraction listée dans l'art. 3 de la loi précitée. Donc rarement. Or, sans disposition spécifique, il semble très délicat d'imposer cette obligation au fournisseur d'accès. A la différence de l'hébergeur, il doit garder les données de connexion de toutes personnes se connectant et non seulement des fournisseurs de contenu. Un juge ne peut créer une obligation autant précise et lourde à la charge du fournisseur d'accès. Nous verrons s'il en ira de même pour l'hébergeur[224].

2.4.2 L'obligation d'avertir promptement les autorités

La seconde obligation consiste à avertir sans délai les autorités des informations illicites dont ils ont connaissance. L'art. 15 al. 2 de la directive sur le commerce électronique précise que l'obligation d'informer promptement les autorités ne peut être imposée par les Etats membres qu'en ce qui concerne les informations illicites alléguées : le prestataire doit seulement transmettre les plaintes des tiers aux autorités[225]. L'art. 22 al. 2 du projet de la loi belge sur la société de l'information oblige ainsi le fournisseur d'accès à informer promptement les autorités des informations illicites alléguées qu'un fournisseur de contenu proposerait. En matière civile, cette obligation est toutefois inutile. Une demande ne peut être déposée au tribunal que par le lésé[226]. En matière pénale, l'obligation prend à l'inverse toute sa mesure en ce qui concerne les infractions qui ne nécessitent pas une plainte de la victime. En Suisse, le

---

[223] Commission Nationale de l'Informatique et des Libertés, Avis sur le projet de loi sur la société de l'information, p. 10, disponible à l'adresse http://www.cnil.fr.

[224] Cf. Partie 3 E. 2.3.3 ii p. 77.

[225] Une telle obligation devrait, à notre sens, aussi être étendue aux cas où le fournisseur prend lui-même connaissance de certains agissements. L'art. 3 ch. 4 du code de conduite rédigé par l'ISPA va dans ce sens, puisqu'il oblige les fournisseurs d'accès à « *dénoncer aux autorités les agissements délictueux éventuels* »[225]. Il sera néanmoins difficile de prouver que le prestataire avait connaissance de contenus illégaux et n'a pas averti les autorités.

[226] Cf. par exemple l'art. 53 du code de procédure civile neuchâtelois (RSN 251.1) : « *Le juge ne peut être saisi que par la demande d'une partie* ».

prestataire Internet a actuellement un droit de dénonciation, mais « *aucune obligation de dénoncer des attitudes ou des contenus punissables vis-à-vis des autorités policières* »[227], comme le relève la Police fédérale.

2.4.3 L'obligation de promotion du filtrage privé

Le troisième type d'obligation est lié à la promotion des systèmes de filtrage privés. Quiconque a le droit de décider ce qui est bon de lire ou de regarder, pour lui et ses enfants notamment. La censure personnelle et domestique est globalement très saine. Le Parlement européen est de cet avis : concernant la protection des mineurs, il s'oppose à un filtrage systématique d'Internet et préconise l'usage de filtres par les parents[228]. Dans ce sens, la loi française du 1er août 2000 oblige le fournisseur d'accès à « *informer leurs abonnés de l'existence de moyens techniques permettant de restreindre l'accès à certains services ou de les sélectionner, d'autre part, de leur proposer au moins un de ces moyens* ».

2.4.4 L'obligation de surveillance ciblée

Si une surveillance générale ne doit pas être exigée du fournisseur d'accès, un contrôle ciblé pourrait très bien lui être ordonné. C'est dans ce sens que va le considérant (47) de la directive sur le commerce électronique, qui précise que l'art. 15 al. 1 de cette même directive ne vise que les « *obligations à caractère général* ». Une loi d'un Etat membre peut donc permettre, dans des cas spécifiques, une surveillance de tel ou tel destinataire de services. C'est ainsi que l'art. 22 al. 1 du projet de la loi belge sur la société de l'information prévoit que les autorités judiciaires peuvent « *imposer une obligation temporaire de surveillance dans un cas spécifique, lorsque cette possibilité est prévue par la loi* ». Le droit suisse connaît déjà ce type d'obligation, instauré par la Loi sur la surveillance de la correspondance par poste et télécommunication, mais il faut relever le même problème que pour l'obligation de conservation et de communication des *logs* : une telle surveillance ne peut être ordonnée que pour des actes punissables, énumérés à l'art. 3 de la loi en question. Elle ne touche donc pas le domaine civil, sauf en cas d'action civile subsidiaire à une action pénale.

2.5 Conclusions

Lorsque le prestataire est un pur fournisseur d'accès, c'est-à-dire tant qu'il ne fait qu'offrir les moyens techniques permettant l'accès aux informations, tant qu'il respecte le principe de « neutralité » vis-à-vis du contenu, il ne doit assumer aucune responsabilité dite éditoriale : exiger de ce prestataire une surveillance générale est actuellement - et pour très longtemps - exclu.

Si le fournisseur d'accès connaissait l'existence de contenus illicites et qu'il n'a pas procédé aux diligences raisonnables pour supprimer au mieux l'accès aux informations litigieuses, sa responsabilité pourra être engagée[229]. La détermination du caractère raisonnable des mesures et la délimitation de la notion de connaissance posent des problèmes complexes.

---

[227] Police fédérale suisse, Responsabilité pénale, p. 14.

[228] Etienne WÉRY, Le Parlement européen s'oppose au filtrage systématique du web comme moyen de protection des mineurs, http://www.droit-technologie.org, 15 avril 2002.

[229] Contra Markus BERNI, E-Commerce, p. 85. Il nous semble que l'auteur, par une déduction a contrario de l'arrêt du 156, exprime que le fournisseur d'accès ne peut être responsable que s'il a accompli un « *aktiven Beitrag* ». Par cette dernière expression, l'auteur comprend par exemple la mise en place d'une infrastructure propre à la commission d'actes illicites, situation non réalisée pour un « *reines Access Provider* ».

Des quatre obligations étudiées, aucune ne peut actuellement être exigée du fournisseur d'accès par un juge suisse. Par conséquent, leur « violation » ne peut pas amener la négligence et donc la responsabilité du prestataire.
Ces obligations devraient être mises noir sur blanc dans une loi. Elles constitueraient un plus incontestable dans le combat contre les contenus illicites. Nous pensons tout particulièrement à l'obligation de conserver et de communiquer les *logs* de connexion. En attendant ces beaux jours, le fournisseur d'accès se doit d'être vigilant, même si le risque de voir un lésé le convoquer au tribunal est faible.

3. La responsabilité pour les contenus illicites stockés sur un serveur *proxy*

Les fournisseurs d'accès mettent en place et exploitent des serveurs qui permettent ce qu'on appelle le *proxy caching* ou le *caching*[230]. Ces serveurs « caches », appelés *proxies*[231], gardent automatiquement et temporairement en mémoire les données les plus demandées qui ont déjà transité par leur biais et rendent ainsi plus efficace leur transmission ultérieure.
Si le fournisseur d'accès pratique, à outrance, ce type de reproduction, c'est pour limiter la congestion du réseau, fluidifier les communications en ligne. « *Faire des caches, c'est économiser près de 40% de la bande passante des fournisseurs d'accès* »[232]. En épargnant la bande passante, notamment lors des communications intercontinentales, le fournisseur d'accès améliore grandement ses performances. Le cybernaute ne consultera pas la page *web* originale stockée sur le serveur initial - peut-être localisé à 5000 kilomètres de chez lui - mais la copie de la page *web* en question, enregistrée sur le serveur *proxy* du fournisseur, peut-être situé à 500 mètres du point de connexion de l'internaute : le temps de réponse à la requête de dernier sera considérablement diminué. Si le *caching* est souvent pratiqué à l'insu de l'internaute, il ne lui est pas moins bénéfique.

La problématique de la responsabilité pour les contenus illicites stockés sur un serveur *proxy* est plutôt théorique puisque, à notre connaissance, aucune affaire, dans quelque pays que ce soit, n'a touché ce domaine jusqu'à présent. Mais, si la directive sur le commerce électronique et avant elle, le TDG et le DMCA, traitent de la responsabilité découlant du *caching*, c'est qu'il est important que toute activité liée à Internet possède un cadre juridique sûr. Si les textes de lois n'exonéraient que quelques joueurs d'Internet, les lésés se retourneraient contre le joueur non protégé.

3.1 La législation étrangère

3.1.1 Le *Teledienstgesetz*

L'art. 5 al. 3 du TDG a le contenu suivant : « *Dienstanbieter sind für fremde Inhalte, zu denen sie lediglich Zugang zur Nutzung vermitteln, nicht verantwortlich. Eine automatische und kurzzeitige Vorhaltung fremder Inhalte auf Grund Nutzerabfrage gilt als Zugangsvermittlung*. »

---

[230] On parle aussi de *server caching* ou de *system caching*, voire d' « antémémorisation ».
[231] Il faut remarquer que les *proxies* peuvent aussi faire office de *firewalls* et qu'il ne faut pas confondre les serveurs caches avec les sites miroirs, qui sont des dupliques volontaires d'un site Internet sur d'autres serveurs, généralement placés sur un autre continent, afin d'en faciliter l'accès.
[232] Pierre SIRINELLI, Responsabilité.

Cette seconde phrase vise le *proxy caching* et le routage de contenus illicites[233]. Elle assimile le stockage automatique et temporaire de contenus « étrangers » à la fourniture d'accès.

3.1.2 La directive sur le commerce électronique

L'art. 13 de la directive, nommé « Forme de stockage dite « *caching* » », dit :

1. Les Etats membre veillent à ce que, en cas de fourniture d'un service de la société de l'information consistant à transmettre, sur un réseau de communication, des informations fournies par un destinataire du service, le prestataire ne soit pas responsable au titre du stockage automatique, intermédiaire et temporaire de cette information fait dans le seul but de rendre plus efficace la transmission ultérieure de l'information à la demande d'autres destinataires du service, à condition que :

a) le prestataire ne modifie pas l'information ;
b) le prestataire se conforme aux conditions d'accès à l'information ;
c) le prestataire se conforme aux règles concernant la mise à jour de l'information, indiquées d'une manière largement reconnue et utilisées par les entreprises ;
d) le prestataire 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) le prestataire agisse promptement pour retirer l'information qu'il a stockée ou pour en rendre l'accès impossible dès qu'il a effectivement 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.

2. Le présent article n'affecte pas la possibilité, pour une juridiction ou une autorité administrative, conformément aux systèmes juridiques des États membres, d'exiger du prestataire qu'il mette fin à une violation ou qu'il prévienne une violation.

Si la directive distingue le *caching* de l'hébergement, certains auteurs pensaient autrefois que les prestataires exerçant l'une ou l'autre activité devaient être soumis au même régime de responsabilité[234].

3.2 Développements

Au regard du développement d'Internet, l'exploitation de *proxies* peut paraître comme une nécessité, mais elle relève en fait de la commodité[235]. Le *caching* permet « *d'améliorer la « disponibilité » du contenu mis à la disposition des internautes* »[236], mais n'est pas nécessaire au fonctionnement d'Internet, à l'inverse du routage[237], au cours duquel il y a aussi un stockage. C'est en ce sens que la responsabilité de l'exploitant d'un serveur *proxy* doit être examinée avec attention.

Comme pour le fournisseur d'accès, il est logique que l'exonération du prestataire ne peut avoir lieu que s'il est neutre vis-à-vis du contenu illicite : il ne doit pas modifier l'information stockée qui sera transmise aux utilisateurs ultérieurs. La directive sur le commerce

---

233 Alain STROWEL et Nicolas IDE, Responsabilité, p. 16.
234 Frédérique OLIVIER et Eric BARBRY, Hébergement, p. 1087.
235 Pierre SIRINELLI, Responsabilité.
236 Frédérique OLIVIER et Eric BARBRY, Hébergement, p. 1087.
237 Pour des notions, cf. Partie 3 D. 1 p. 59.

électronique impose une autre obligation d'abstention : celle de l'absence d'interférence sur les techniques utilisées dans le but d'obtenir des données et d'établir des statistiques sur l'utilisation de l'information. Le législateur européen a en particulier pensé aux « compteurs électroniques ». Il est important que le propriétaire de site ou l'auteur qui est rémunéré en fonction du nombre de visites du site ne voit pas son gagne-pain fondre de par l'exploitation de *proxies*. Comme le relève Pierre SIRINELLI, on ne peut *« ignorer les craintes des titulaires de droits qui font observer que le recours aux caches réduit le nombre d'accès directs aux sites et empêche le décompte des consultations des œuvres sur ceux-ci. Le phénomène serait particulièrement inquiétant dans l'hypothèse d'une rémunération de l'auteur fondée sur le nombre de consultations (« hits »)* »[238]. Même si le *proxy caching* d'œuvres protégées par le droit d'auteur n'apporte pas directement un revenu au fournisseur d'accès, on constate qu'il peut amener une diminution de la rétribution de l'auteur. Mais on voit mal en quoi cette problématique est liée à celle de la responsabilité du prestataire vis-à-vis du contenu illicite stocké sur son serveur cache. La condition de l'art. 13 al. 1 lit. d de la directive sur le commerce électronique a toutefois le mérite d'inviter l'intermédiaire à trouver des moyens techniques pour éviter un préjudice au propriétaire du site. A notre sens, les tribunaux ne devraient pas exiger une telle obligation au prestataire dans l'examen de la diligence exigée, tant il est vrai que les lésés en cause sont différents. Une fois, il s'agit de la victime d'une information illicite, l'autre fois, il s'agit du propriétaire du site ou d'un auteur lésés par l'activité de *caching* du prestataire.
Pour le prestataire pratiquant le *proxy caching*, une « *obligation de respect de certaines règles* »[239] est exigée par l'art. 13 al. 1 lit. b et c de la directive sur le commerce électronique. L'intermédiaire doit d'abord « *se conformer aux conditions d'accès à l'information* ». On pense en particulier au paiement d'un abonnement et à la fourniture d'un mot de passe. Le prestataire doit ensuite respecter les standards relatifs à la mise à jour de l'information. Autant l'obligation précédente ne semble pas primordiale, autant celle-ci l'est. Elle a le même but que l'obligation d'intervention que nous examinons ci-dessous, soit de ne pas permettre l'accès à un contenu illicite qui n'existerait plus à la source. En effet, si la victime d'une information préjudiciable obtient sa suppression, avec ou sans l'aide la justice, il ne doit pas voir l'atteinte perdurer et son dommage croître par la faute d'un exploitant de *proxy* qui n'aurait programmé qu'un « rafraîchissement » erratique des copies.

Si l'on a vu qu'un doute subsistait quant aux mesures de blocage de l'accès à l'information illicite qui pourraient être imposées au prestataire qui fournit l'accès à Internet, il est évident d'imposer à l'exploitant d'un serveur cache un certain degré d'intervention, c'est-à-dire la suppression immédiate de son serveur *proxy* de la copie temporaire de l'information s'il a connaissance de son caractère illicite. Il ne faut pas oublier que cette copie technique est temporaire, mais non volatile[240]. Cette obligation positive est logique, compte tenu du fait que l'information initiale a été ou aurait dû être supprimée en amont. Selon la directive, la connaissance du caractère illicite de l'information doit être effective, mais un des problèmes récurrents générés par ce texte est la détermination des actes qui amènent cette connaissance effective. Une notification est évidemment nécessaire, étant donné que l'intermédiaire ne s'intéresse pas aux contenus qu'il stocke temporairement. La notification d'une autorité judiciaire entraîne assurément connaissance, mais quid de celle du lésé ? Il semble que l'énoncé de l'art. 13 al. 1 lit. e de la directive veut que ces types de notifications suffisent. Les termes « *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* » ne parlent en effet pas

[238] Pierre SIRINELLI, Responsabilité.
[239] Alain STROWEL, Nicolas IDE et Florence VERHOESTRAETE, Directive, p. 143.
[240] Les informations peuvent être conservées quelques heures comme quelques jours.

du caractère illicite. On peut penser par là que le lésé, qui s'est adressé au propriétaire du site et qui a obtenu de ce dernier l'élimination de l'information préjudiciable, pourrait demander à un exploitant de *proxy* de supprimer cette information.

Il faut encore préciser que, d'une manière générale, on ne doit pas exiger de l'exploitant d'un serveur cache qu'il contrôle la licéité des informations qu'il stocke. Les arguments en faveur de cette opinion sont notamment le fait que le prestataire n'est pas en contact avec le fournisseur de contenu et que les informations qu'il stocke changent fréquemment. Pour le reste, la réflexion est grandement similaire à celle opérée ultérieurement pour le prestataire d'hébergement[241].

3.3 Conclusions

En Suisse, devraient être exigées du fournisseur d'accès, en tant qu'exploitant d'un serveur cache, trois des obligations vues ci-dessus : l'obligation de neutralité vis-à-vis du contenu, l'obligation de respect des règles instaurées par le site émetteur quant à la mise à jour de l'information et l'obligation d'intervention. Les deux autres obligations instaurées par la directive sur le commerce électronique, si elles semblent logiques et utiles, nous semblent moins liées à la problématique de la responsabilité délictuelle pour le contenu stocké dans le serveur cache.

3.4 Remarque

L'activité de *caching* pose surtout des questions en matière de droit d'auteur. Signalons seulement que l'art. 18a al. 2 de l'avant-projet de révision de la LDA prévoit que « *la simple fourniture d'installations afin d'utiliser une œuvre ne constitue en soi pas une utilisation de l'œuvre au sens de l'art. 10* ». Cet art. 18a al. 2 vise donc à limiter la responsabilité découlant du droit d'auteur que les fournisseurs d'accès, plus précisément les exploitants d'un serveur *proxy*, pourraient encourir[242]. Il suit en cela l'art. 5 al. 1 et le considérant (33) de la directive sur le directive 2001/29/CE du 22 mai 2001 sur l'harmonisation de certains aspects du droit d'auteur et des droits voisins dans la société de l'information.

C. Le transporteur (*carrier*)

1. Notions

Le transporteur s'occupe du transfert physique des paquets d'informations sur les canaux télématiques, en exploitant et administrant l'infrastructure de base, soit les lignes téléphoniques et autres canaux, qu'il loue de façon permanente[243] ou temporaire au fournisseur de réseau.
Le transporteur est en fait un opérateur de télécommunication[244]. L'art. 4 al. 1 de la Loi fédérale du 30 avril 1997 sur les télécommunications rend nécessaire une concession pour l'exercice d'une telle activité.

---

[241] Cf. Partie 3 E. 2.3.1 p. 67.
[242] Cf. le rapport explicatif de l'avant-projet, p. 8, disponible sur le site de l'Institut fédéral de la Propriété Intellectuelle à l'adresse http://www.ige.ch.
[243] On parle alors de lignes dédiées (*dedicated lines*).
[244] Comme exemples, on peut citer Swisscom, Sunrise, DiaX, France Telecom et Belgacom.

Il ne faut pas confondre le transporteur et le fournisseur de réseau. On rappelle qu'Internet est constitué de nœuds - relais et autres ordinateurs - et de liens entre ces nœuds. Les fournisseurs de réseau, ou fournisseurs d'infrastructure, sont les propriétaires des liens. Ces liens peuvent être des lignes téléphoniques, des câbles TV, des fibres optiques uniquement destinées à Internet ou encore des réseaux « mobiles ».
En Suisse, Swisscom a été pendant longtemps l'unique propriétaire du réseau téléphonique. Depuis la libéralisation du marché, des entreprises telles que Sunrise ou Tele2 ont posé leurs propres lignes. Ces lignes, des fibres optiques, ont toutefois seulement été tirées entre les grands centraux téléphoniques suisses, laissant l'acheminement local des conversations aux lignes de Swisscom[245].
Il existe beaucoup de propriétaires de fibres optiques[246], de réseaux câblés[247] ou de réseaux satellite. On voit que les fournisseurs du réseau Internet, qui donnent en location l'infrastructure de base aux transporteurs, sont plutôt nombreux.

Il est évident que les rôles de transporteur et de fournisseur de réseau sont parfois, voire fréquemment, tenus par la même entité. C'est pourquoi la doctrine les confond souvent. Mais que ce soit clair : il est simplement inimaginable qu'un fournisseur d'infrastructure soit tenu pour responsable des contenus illicites ayant transité par les canaux dont il est le propriétaire. Il faut rappeler que cet acteur d'Internet n'exploite même pas personnellement ces canaux. Nous n'étudierons donc que la responsabilité du transporteur.

2. La responsabilité pour les contenus illicites transportés

A notre connaissance, aucune action en responsabilité n'a à ce jour été intentée contre un transporteur pour avoir transmis des informations illicites. La question est donc plutôt théorique. Le transporteur n'a pas été pour autant oublié par la directive sur le commerce électronique, ce qui montre qu'il faut traiter de la responsabilité de chaque acteur, afin que chaque intermédiaire technique sache à quoi il doit s'en tenir.

2.1 La jurisprudence

2.1.1 La jurisprudence suisse sur les télékiosques

Thibault VERBIEST cite l'affaire dite du « 156 » comme concernant la responsabilité des transporteurs - même s'il parle de fournisseurs d'infrastructure[248]. Il déduit de l'arrêt que *« à l'instar des fournisseurs d'accès, la mise en cause de leur responsabilité n'est pas exclue lorsqu'ils ont eu connaissance du caractère illicite de certaines informations ayant transité par leur système* ».
Si l'auteur a raison de rapprocher le régime de responsabilité des transporteurs à celui des fournisseurs d'accès, nous avons vu plus haut que l'analogie entre le fournisseur de télékiosque et le fournisseur d'accès, à plus forte raison le transporteur, n'était pas appropriée, de part la différence en matière de pouvoir d'intervention en cas de connaissance d'activité ou d'information illicite[249].

---

[245] Le « dernier kilomètre » devrait pourtant être libéralisé tantôt, après que le Conseil fédéral ait révisé l'Ordonnance sur les services de télécommunications (RS 784.101.1).
[246] La plupart des universités en possèdent.
[247] Comme exemple de câblo-opérateurs, on peut citer Cablecom.
[248] Thibault VERBIEST, Acteurs.
[249] Cf. Partie 3 B. 2.1.1 p. 40.

2.1.2 La jurisprudence française sur le Minitel

Certains auteurs assimilent le transporteur à un opérateur de Minitel[250]. Le 15 mai 1992, le Tribunal de grande instance de Draguignan a jugé d'un cas où le responsable de France Telecom était incriminé pour avoir permis l'exploitation d'une « messagerie rose » par l'entremise du Minitel[251]. Le tribunal l'a relaxé, car il a considéré que l'opérateur ne pouvait voir sa responsabilité engagée pour les délits commis par les fournisseurs de services, au motif qu'il n'était pas établi qu'il avait connaissance des comportements atteignant aux bonnes mœurs commis sur ses réseaux. Cet arrêt laisse ouverte la question de la responsabilité de France Telecom pour les infractions commises par l'entremise du Minitel si cet acteur en avait eu connaissance. Il laisse même à penser qu'une telle responsabilité aurait été prononcée dans de telles circonstances[252].
Nous pouvons ici réitérer la remarque concernant le télékiosque 156. Si France Telecom veut couper l'accès à un contenu, il le fait. On a constaté que la situation était différente pour le fournisseur d'accès, d'autant plus pour le transporteur.

2.1.3 Conclusion sur la jurisprudence

Certains auteurs ont voulu conforter leur opinion par des analogies avec le fournisseur de télékiosque ou l'opérateur de Minitel. A notre avis, il faut s'éloigner de cette démarche pour les raisons susmentionnées. Il convient par conséquent d'admettre qu'il n'existe, à l'heure actuelle, aucune jurisprudence pertinente en matière de responsabilité des transporteurs.

2.2 La législation étrangère

Elle est identique à celle concernant le fournisseur d'accès[253].

2.3 Développements et conclusions

Le *(common) carrier* est, comme son nom l'indique, un simple convoyeur d'informations. Il ne « *s'intéresse nullement au contenu intellectuel de qu'il transporte* »[254]. Il n'a aucune maîtrise sur le contenu des informations, qui ne sont pour lui que des bits sans signification. En résumé, il a une fonction purement technique, à l'image de l'opérateur téléphonique ; or, il est incontestable que ce dernier, n'osant en général pas contrôler la teneur des messages transmis[255], n'est pas responsable des conversations des usagers du téléphone[256]. Une responsabilité a priori[257] du transporteur pour la propagation de contenus illicites sur Internet est en ce sens exclue tant que son devoir de neutralité vis-à-vis du contenu n'est pas violé. Le contraire serait extrêmement critiquable[258]. L'art. 12 al. 1 de la directive sur le commerce

---

250 Lionel THOUMYRE, Réglementation ; Alain STROWEL et Nicolas IDE, Responsabilité, p. 9 ; Gérard HAAS et Olivier DE TISSOT, Atteintes.
251 TGI Draguignan, 15 mai 1992, *D.I.T.,* 1992/4, p. 39-42.
252 Lionel THOUMYRE, Réglementation.
253 Cf. Partie 3 B. 2.2 p. 42.
254 Gérard HAAS et Olivier DE TISSOT, Atteintes.
255 L'unique exception étant constituée par les mesures de surveillance au sens de la Loi fédérale sur la surveillance de la correspondance par poste et télécommunication (RS 780.1).
256 Jérôme BENEDICT, Responsabilité, p. 32.
257 C'est-à-dire alors que l'opérateur ignore l'existence des informations illicites.
258 Dans l'affaire Estelle Hallyday, la Cour d'appel a d'ailleurs clairement exprimé que la jurisprudence qu'elle élaborait ne visait que l'opérateur qui excède « *manifestement le rôle technique d'un simple transmetteur d'informations* ».

électronique exprime bien l'avis de tous. Mais l'alinéa 3 du même article n'exclut pas le transporteur de son champ d'application. Les Etats membres peuvent prévoir, dans leur législation, qu'une juridiction ou une autorité administrative puisse exiger de cet intermédiaire de mettre un terme à la violation. Globalement, on ne peut être plus sévère à l'égard du *carrier* qu'on ne l'est à l'égard du fournisseur d'accès. Par conséquent, ce n'est que si l'on exigerait d'un fournisseur d'accès qu'il bloque l'information qu'on devrait examiner si de telles mesures peuvent être ordonnées au transporteur d'information. Nous nous référons à cet égard aux développements sur les mesures de blocage effectués dans le chapitre concernant le fournisseur d'accès[259], qui valent *mutatis mutandis* pour le transporteur. Mais au final, on ne pourra que remarquer qu'« *il paraît très difficile de pouvoir mettre en cause la responsabilité de l'opérateur, sauf pour défaillance technique* »[260].

3. La responsabilité du fait d'une défaillance technique

De manière générale, l'utilisateur n'est lié contractuellement qu'avec le fournisseur d'accès à Internet. Des conditions générales régissent le rapport entre ces deux acteurs et excluent la responsabilité du fournisseur d'accès à Internet en cas de défaillance technique. L'incorporation et la validité des conditions générales ne posant en principe aucun problème, le fournisseur d'accès est immunisé contre toute action en dommages-intérêts.
Pourtant, un dysfonctionnement technique touchant les services d'Internet peut avoir des conséquences pécuniaires importantes. De plus en plus de contrats sont passés par le biais d'Internet. Imaginons qu'un *e-mail* ait dû confirmer, dans un certain délai, la conclusion d'un contrat d'entreprise, mais que cette confirmation ne soit jamais arrivée suite à une quelconque erreur technique ou à des réparations ou transformations[261]. Ce genre de cas est certes rare aujourd'hui. Mais dans vingt ans ? Le lésé pourrait alors songer à actionner l'opérateur de télécommunication. De nombreuses difficultés se présenteront au lésé dans le processus de réparation de son préjudice.
Il lui faudra notamment prouver que l'opérateur a commis une faute. Cette tâche sera extrêmement compliquée, puisque la faute a lieu dans la sphère de l'opérateur, lieu secret auquel le lésé n'a pas accès. On pourrait peut-être imaginer que le prestataire fasse preuve de négligence lorsque, sachant qu'il doit faire des travaux qui empêcheront toute télécommunication pendant un certain laps de temps, il n'avertit pas le fournisseur d'accès afin que celui-ci en informe ses clients.
Si le lésé surmonte cet obstacle, il en restera un qui semble infranchissable[262] : il devra trouver une norme protectrice pour remplir la condition de l'illicéité. On rappelle que les intérêts patrimoniaux ne sont pas protégés en tant que tels. On imagine mal quelle disposition pourrait entrer en jeu. Il ne faut même pas penser au principe du danger créé, principe « bouche-trou », décrié et inadéquat en l'occurrence. En France, où le fait de causer un dommage est illicite en soi, on imaginerait plus volontiers l'action en dommages-intérêts pour défaillance technique porter ses fruits, même si elle reste du domaine de l'hypothétique.

Le temps avançant, l'utilisateur d'Internet sera de plus en plus exigeant et le moindre ennui de connexion le fera bondir de sa chaise. Pourtant, il y a toujours des coupures et des interférences dans la diffusion des chaînes de télévision. L'homme d'affaires aura tout intérêt

---

[259] Cf. Partie 3 B. 2.3.2 p. 44.
[260] Alain STROWEL et Nicolas IDE, Responsabilité, p. 9, suivant l'avis d'Olivier HANCE, Business et droit d'Internet, Best of publishing, Paris 1996, p. 211.
[261] Par exemple un changement de serveur.
[262] Dans ce sens, David ROSENTHAL, Projekt, p. 114.

à s'y prendre assez tôt pour envoyer l'*e-mail* décisif ou à couvrir ses arrières par un moyen plus sûr. Le courrier B ? Non, le sms...

D. L'exploitant de relais[263]

1. Notions

Les relais sont des équipements informatiques qui servent à véhiculer les informations sur un réseau. Il s'agit essentiellement des commutateurs, des routeurs et des passerelles.
Les commutateurs (*switchs*) sont les équipements capables d'effectuer la commutation de paquets, technique consistant à transmettre des informations en les découpant en paquets. Ces paquets - ou datagrammes -, qui portent tous l'adresse du destinataire, sont envoyés séparément, empruntent les chemins les plus idoines et sont réunis à la réception. Ils peuvent arriver dans un ordre quelconque chez le destinataire, car étant numérotés, l'ordinateur récepteur les remet dans l'ordre initial. Du protocole TCP/IP[264], TCP divise et transmet les informations dans un ordre aléatoire et IP s'occupe de donner aux datagrammes une adresse.
Les routeurs (*routers*) permettent l'aiguillage des paquets, soit le choix de la « bonne route », et la liaison entre les différents réseaux dont Internet est constitué. Les ordinateurs de routage sont des nœuds d'interconnexion.
Les passerelles (*gateways*) sont les machines effectuant certaines conversions de protocoles de communication : elles font le lien entre deux sections incompatibles du réseau des réseaux.

Les routeurs, passerelles et commutateurs que l'on trouve sur Internet sont la propriété de milliers de personnes, physiques et surtout morales[265], souvent des fournisseurs d'infrastructure[266].

Parmi ces différents relais, certains opèrent une copie technique des contenus qui transitent par eux. C'est plus particulièrement le cas des routeurs. C'est cette copie qui amène la question de la responsabilité des exploitants de relais.

2. La responsabilité pour les contenus illicites stockés dans le relais

2.1 La législation étrangère

2.1.1 Le Teledienstgesetz

L'art. 5 al. 3 du TDG a le contenu suivant : « *Dienstanbieter sind für fremde Inhalte, zu denen sie lediglich Zugang zur Nutzung vermitteln, nicht verantwortlich. Eine automatische und kurzzeitige Vorhaltung fremder Inhalte auf Grund Nutzerabfrage gilt als Zugangsvermittlung*. »

---

263 Les définitions présentes dans ce chapitre sont largement inspirées de Alain Dufour, Internet, p.5 et 117ss et de Pierre BREESE, Guide juridique de l'Internet et du commerce électronique, Paris 2000, p. 341ss.
264 Pour une définition, cf. Partie 1 B. 7 p. 12.
265 Dans un entretien électronique, le Professeur de l'Université de Neuchâtel Jacques SAVOY, spécialiste des moteurs de recherche, nous explique qu'un message envoyé depuis l'Université de Neuchâtel transite sur les routeurs appartenant à cette université, puis sur le nœud cantonal - routeur appartenant au canton de Neuchâtel - pour être conduit sur le réseau de Switch, etc.
266 Pour une définition, cf. Partie 3 C. 1 p. 55.

La seconde phrase de la disposition vise le *proxy caching*, mais aussi le routage de contenus.

2.1.2 La directive sur le commerce électronique

L'art. 12 al. 2 de la directive sur le commerce électronique prévoit que « *les activités de transmission et de fourniture d'accès visées au paragraphe 1 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* ».

L'exploitant du relais n'est donc pas responsable s'il est neutre vis-à-vis de l'information, c'est-à-dire s'il n'a pas pris la décision de transmettre l'information, s'il n'a pas choisi le destinataire de l'information et s'il n'a eu aucun rôle dans la composition de l'information.

Thibault VERBIEST et Lionel THOUMYRE précisent que « *le terme « automatique » fait référence au fait que le stockage s'effectue dans le cadre du fonctionnement normal de la technologie considérée. Le terme « intermédiaire » fait référence au fait que le stockage de l'information s'effectue au cours de la transmission. Le terme « transitoire » fait référence au fait que le stockage est effectué pour un laps de temps limité* »[267].

2.2 Développements et conclusions

La reproduction momentanée des contenus opérée par les relais, plus spécialement les routeurs, est une nécessité[268] : sans elle, les informations ne pourraient être dirigées et amenées à bon port. La « copie de transmission » pose moins de problèmes que le *proxy caching* parce que la reproduction est ici tellement brève que, si aucun contrôle des informations n'est possible[269], il en est de même d'une quelconque suppression de données illicites, puisque ces dernières n'ont été stockées dans le relais que quelques instants. C'est en cela que l'on assimile la copie de transmission a un simple transport d'informations. Nous dirons donc que, de manière générale, la responsabilité de l'exploitant d'un relais ne devrait pas être recherchée, tant qu'il reste neutre vis-à-vis du contenu des informations. Mais à l'instar de ce qui a été dit du fournisseur d'accès, il pourrait être imposé des mesures de blocage au responsable du relais. Ce dernier pourrait notamment bloquer l'adresse IP du serveur *web* concerné. On a vu plus haut qu'un tel blocage n'est adéquat que s'il n'empêche pas l'accès à de nombreux sites parfaitement légaux. Elle ne convient réellement qu'aux sites à contenu essentiellement illicite ayant leur propre serveur. Et on a déjà eu l'occasion de remarquer que les mesures de blocage n'étaient globalement pas très opérantes et comporteraient de nombreux inconvénients. Pour plus de détails, nous nous rapportons à ce qui a été développé pour le fournisseur d'accès[270].

---

[267] Thibault VERBIEST et Lionel THOUMYRE, Le mannequin et l'hébergeur, Juriscom.net, 25 février 1999, qui se rapportent à l'exposé des motifs de la directive sur le commerce électronique (COM (1998) 586 final, p. 29-30).

[268] Pierre SIRINELLI, Responsabilité.

[269] Cf. Partie 3 B. 2.3.1 p. 67. En plus des inconvénients cités dans ce passage, il faut ajouter que les relais - à l'exception des commutateurs - ne reçoivent que des paquets de messages, et non des messages entiers.

[270] Cf. Partie 3 B. 2.3.2 p. 70.

2.3 Remarque

Au niveau des droits d'auteur, il est évident que la reproduction que constitue la copie de transmission ne doit être soumise à aucune autorisation, en tant qu'elle est « *partie intégrante et essentielle d'un processus technique* », qu'elle est exécutée « *dans le seul but de permettre soit une transmission efficace dans un réseau entre tiers par un intermédiaire, soit une utilisation licite de l'œuvre* » et qu'elle n'a en elle-même « *aucune valeur économique propre* »[271]. Une telle façon de voir les choses est d'autant plus logique que la copie de transmission permet, comme son nom le veut, la transmission de l'œuvre : sans cette copie, l'internaute ne pourrait la visionner.

E. Le fournisseur d'hébergement (*host provider*)

1. Notions

Selon le Tribunal de grande instance de Nanterre, l'hébergement est une « *prestation durable de stockage d'informations que la domiciliation sur son serveur rend disponibles et accessibles aux personnes désireuses de les consulter* »[272]. Le fournisseur d'hébergement[273] fournit donc à ses clients - les fournisseurs de contenu - de l'espace disque pour stocker leurs applications informatiques et données électroniques. Les informations ainsi enregistrées peuvent être consultées par le biais d'un site Internet, car le serveur *web* de l'hébergeur est relié en permanence au réseau des réseaux.
Le prestataire d'hébergement gère ses systèmes techniques et informatiques, notamment son serveur *web*[274], et offre généralement un service de gestion des sites.
Les grands hébergeurs, soit les sociétés commerciales de renom, voire certaines entités publiques comme les universités, stockent des dizaines de milliers de sites, contre rémunération ou gratuitement. On peut comparer le contrat d'hébergement avec un contrat de bail : le fournisseur d'hébergement loue de l'espace disque à un particulier qui peut y faire « habiter » les informations qu'il souhaite, pour autant qu'elles soient légales et ne contreviennent pas aux règles contenues dans le contrat. A ce propos, le client peut à sa guise changer le contenu du site, sans passer par l'hébergeur.

2. La responsabilité pour le contenu illicite des sites hébergés

De part son influence sur le contenu, le fournisseur d'hébergement est indubitablement le premier visé comme responsable subsidiaire au fournisseur de contenu.

2.1 La jurisprudence

Deux affaires françaises doivent être analysées soigneusement, car le droit français sous l'empire duquel les décisions ont été prises, ressemblait au droit suisse actuel. Les juges ont

---

[271] Cf. art. 5 al. 1 et considérant (33) de la directive du 22 mai 2001 sur l'harmonisation de certains aspects du droit d'auteur et des droits voisins dans la société de l'information.
[272] TGI Nanterre, 1ère ch. A, 8 décembre 1999, Lynda Lacoste c. Multimania et autres, disponible à l'adresse suivante : http://www.juriscom.net/txt/jurisfr/img/tginanterre19991208.htm.
[273] En anglais, *host provider* ou *Internet presence provider*.
[274] En ce sens, l'*host provider* est aussi un *webmaster* car ce terme ne désigne rien d'autre que l'administrateur d'un serveur ou d'un site *web*. Pour de plus amples renseignements sur le *webmaster*, cf. Partie 3 I. 1 p. 109.

en effet utilisé les art. 1382[275] et 1383[276] du Code Civil français (CCF), qui composent un système proche de ce qu'on trouve en Suisse. La seule grande différence avec le système suisse de l'art. 41 du CO consiste dans le fait que tout acte qui cause un dommage à autrui est illicite[277]. La responsabilité de l'auteur n'est donc subordonnée qu'à trois conditions : l'existence d'un dommage, la faute et le rapport de causalité.
Il est primordial de s'attarder sur ces cas : ils risquent d'augurer ce en quoi consiste le régime de responsabilité des fournisseurs d'hébergement en Suisse.

2.1.1 L'affaire Estelle Hallyday

i. Décisions

Au début de 1998, Estelle Hallyday constate la présence d'une vingtaine de photographies privées la représentant partiellement ou complètement nue sur le site http://www.altern.org/silversurfer. Faute de pouvoir identifier le propriétaire du site, le mannequin assigne le gestionnaire et représentant du service d'hébergement « Altern.org », Valentin Lacambre, en référé devant le Tribunal de grande instance de Paris, en invoquant une violation de son droit à l'image et de l'intimité de sa vie privée. Le top model demande des dommages et intérêts et l'interdiction de poursuivre la diffusion de ces photographies.
La violation des droits d'Estelle Hallyday n'est pas contestée. Dans l'ordonnance de référé[278], le juge estime que « *le fournisseur d'hébergement a l'obligation de veiller à la bonne moralité de ceux qu'il héberge, au respect par ceux-ci des règles déontologiques régissant le web et au respect par eux des lois et des règlements et des droits des tiers* ». Il précise que l'hébergeur peut aller « *vérifier le contenu du site qu'il héberge* » et ainsi faire cesser les atteintes aux droits des tiers.
Il ajoute que « *pour pouvoir s'exonérer de sa responsabilité,* [le fournisseur] *devra donc justifier du respect des obligations mises à sa charge, spécialement quant à l'information de l'hébergé sur son obligation de respecter les droits de la personnalité, le droit des auteurs, des propriétaires de marques, la réalité des vérifications qu'il aura opérées au besoin par des sondages, et des diligences qu'il aura accomplies dès la révélation d'une atteinte aux droits des tiers pour faire cesser cette atteinte* ».
Le juge n'accorde pas les dommages-intérêts que la demanderesse sollicite et l'invite à saisir le juge du fond, jugeant que la problématique de la responsabilité des fournisseurs d'hébergement et la détermination des causes d'exonération susceptibles d'être invoquées dépasse ses compétences. Par contre, vu l'urgence, il enjoint Valentin Lacambre, « *sous astreinte de 100.000 francs par jour, de mettre en oeuvre les moyens de nature à rendre impossible toute diffusion des clichés photographiques en cause à partir de l'un des sites qu'il héberge* ».

Les parties se retrouvent devant la Cour d'appel de Paris[279]. Celle-ci infirme l'ordonnance quant aux mesures d'interdiction, au motif qu'elles étaient inutiles, dans la mesure où les photographies avaient été retirées du site, et qu'elles étaient, au surplus, non définies et

---

[275] « *Tout fait quelconque de l'homme, qui cause à autrui un dommage, oblige celui par la faute duquel il est arrivé, à le réparer* ».
[276] « *Chacun est responsable du dommage qu'il a causé non seulement par son fait, mais encore par sa négligence ou par son imprudence* ».
[277] Pierre ENGEL, Traité des obligations en droit suisse, 2e éd., Berne 1997, p. 447.
[278] TGI Paris, 9 juin 1998, E. Lefébure-Hallyday c. V. Lacambre, disponible à l'adresse suivante : http://www.legalis.net/legalnet/judiciaire/decisions/ord_0698.htm.
[279] CA Paris, 1ère ch. A, réf., 10 février 1999, V. Lacambre c. E. Lefébure-Hallyday, disponible sur le site http://www.droit-technologie.org.

difficiles d'exécution. Mais la cour définit surtout le rôle, juridiquement parlant, du fournisseur d'hébergement, qui, en stockant des contenus « *qui n'ont pas le caractère de correspondances privées*, […] *excède manifestement le rôle technique d'un simple transmetteur d'informations et doit, d'évidence, assumer à l'égard des tiers aux droits desquels il serait porté atteinte dans de telles circonstances, les conséquences d'une activité qu'il a, de propos délibérés, entrepris d'exercer dans les conditions susvisées et qui, contrairement à ce qu'il prétend, est rémunératrice et revêt une ampleur que lui-même revendique* ». Le juge considère ainsi que la diffusion des photographies dans les conditions de l'espèce engage manifestement la responsabilité de Valentin Lacambre et le condamne à payer à Madame Hallyday la somme de 300.000 FF à titre de dommages-intérêts.

ii. Commentaire

L'ordonnance du 9 juin 1998 a été un véritable électrochoc. Prenant le contre-sens d'une tendance prônant l'irresponsabilité des prestataires techniques[280], elle a grandement indigné les professionnels d'Internet et a secoué les politiques français, qui ont très vite délivré des projets d'amendement ou de loi. Très controversée et largement médiatisée, cette décision de principe inattendue a fait l'objet de nombreux commentaires. Parmi ceux-ci, on relèvera que Frédérique OLIVIER et Eric BARBRY se félicitent de cette « *décision audacieuse et courageuse* » qui, pour la première fois en France, admet clairement la responsabilité d'un intermédiaire technique d'Internet[281]. Mais, dans l'ensemble, la doctrine critique la motivation ambiguë de la décision. Le juge semble néanmoins assimiler le fournisseur d'hébergement au directeur de publication d'un journal par exemple[282]. La responsabilité de l'hébergeur dans cette affaire est donc de type éditorial. En tant que directeur de publication, il avait une obligation permanente de contrôle sur le contenu des sites hébergés. Le problème est que le contrôle systématique - a priori ou a posteriori - de milliers de pages *web* est techniquement impossible. Il est en plus socialement, économiquement et juridiquement inacceptable. Mais ne revenons pas sur la problématique de la liberté d'expression et de la censure : on voit bien que « *le mécanisme de la responsabilité éditoriale* […] *ne peut pas être transposé à la situation dans laquelle se trouve l'opérateur d'hébergement* »[283].
L'argumentation du juge Gomez était tellement floue que Michel VIVANT pense à l'inverse de beaucoup que l'ordonnance illustre parfaitement le triptyque « pouvoir - savoir - inertie »[284], selon lequel n'est fautif que celui qui a la possibilité technique d'intervenir, qui sait qu'il y a matière à intervenir et qui, pour finir, n'intervient pas.

L'arrêt de la Cour d'appel est un peu plus clair que l'ordonnance. Selon Frédérique OLIVIER et Eric BARBRY, la Cour d'appel « *n'a pas remis en cause l'analyse, ni la motivation* » du premier juge, mais a donné les conditions d'exonération de la responsabilité établie par la première instance. Nous n'en sommes pas si sûrs, tant l'argumentation est différente. Quoiqu'il en soit, la portée de l'affaire Estelle Hallyday est jugée restreinte par une grande partie de la doctrine, car la Cour d'appel de Paris a insisté sur les circonstances particulières de l'affaire : les « *conditions susvisées* ». En particulier, la nature anonyme de la fourniture d'hébergement semble avoir été décisive dans la décision de la Cour d'appel[285]. Si le

[280] L'élaboration de la directive sur le commerce électronique était en bonne voie mais le juge Gomez ne s'en est pas inspiré.
[281] Frédérique OLIVIER et Eric BARBRY, Hébergement, p. 1085.
[282] Lionel THOUMYRE : Les hébergeurs dans les filets de la justice, Juriscom.net, octobre 1998 ; Sébastien CANEVET, Rapport ; Jean-Claude PATIN, La responsabilité des hébergeurs n°2, Juritel.com.
[283] Sébastien CANEVET, Rapport.
[284] Michel VIVANT, Responsabilité, p. 2024.
[285] Notamment Blandine POIDEVIN, L'affaire Altern, Jurisexpert.com ; André Lucas, Responsabilité.

fournisseur d'hébergement souhaite conserver l'anonymat pour en tirer un avantage commercial, il doit assumer les risques qui en découlent[286]. L'application de la théorie du risque - ou du risque-profit -, qui affleure dans la décision[287], a été fortement critiquée car, selon la doctrine majoritaire, le droit commun lié à la notion de faute aurait dû rester au centre du débat.
Il faut ajouter que la gratuité du service n'est pas un critère d'exonération, car l'activité est évidemment rémunératrice. Pour s'en convaincre, il suffit de constater à quel prix se sont vendus certains domaines Internet et le revenu que procure une bannière publicitaire. Si l'activité de l'hébergeur avait été purement altruiste, il n'aurait peut-être pas été déclaré responsable[288].

Pour Frédérique OLIVIER et Eric BARBRY[289], l'affaire Estelle Hallyday pose pour la première fois le principe de l'existence d'obligations à la charge du fournisseur d'hébergement, mais ne donne pas un contour précis de ces obligations. C'est pourquoi l'affaire Lynda Lacoste qui suivit eut une importance toute particulière.

2.1.2 L'affaire Lynda Lacoste

i. Décisions

Au cours de l'été 1999, Lynda Lacoste a la déplaisante surprise de découvrir que des photos vieilles de 10 ans, la montrant dans le plus simple appareil, sont diffusées sans son autorisation sur plusieurs sites *web* aux noms évocateurs, hébergés par diverses sociétés, dont la très connue Multimania. Devant le Tribunal de grande instance de Nanterre, elle demande, sur la base des art. 9 et 1383 du CCF, des dommages et intérêts pour la violation de son droit à l'image.
Le tribunal[290] estime que l'activité du fournisseur d'hébergement « *excède la simple prestation technique d'un transmetteur d'informations* » et qu'il est tenu, sur le fondement de l'article 1383 du CCF, « *d'une obligation générale de prudence et de diligence* ». Il doit ainsi mettre en œuvre des « *moyens raisonnables d'information, de vigilance et d'action* » pour éviter que les droits des tiers ne soient lésés.
Selon le juge, l'obligation d'information consiste en particulier à inviter ses clients à respecter les droits d'autrui au moyen d'une charte à l'ouverture du compte et de lettres d'information périodiques par exemple. L'obligation d'action réside, dès que le site incriminé est identifié, en sa désactivation du réseau et en la vérification que ce site ne revienne pas en ligne chez l'hébergeur. Quant à l'obligation de vigilance, l'hébergeur ne doit pas « *exercer une surveillance minutieuse et approfondie du contenu des sites* », mais « *prendre les mesures raisonnables qu'un professionnel avisé mettrait en oeuvre pour évincer de son serveur les sites dont le caractère illicite est apparent, cette apparence devant s'apprécier au regard des compétences propres du fournisseur d'hébergement* ». L'hébergeur doit plus particulièrement détecter les sites illicites au moyen d'un moteur de recherche.

---

[286] Lionel BOCHURBERG, Internet et commerce électronique, 2e éd., Paris 2001, p. 229.
[287] Michel VIVANT, Responsabilité, p. 2023. Pour FG Associés (A propos de la décision Estelle Hallyday, Expertises, avril 1999, disponible sur le site Droitweb.com), l'application de cette théorie est même une évidence.
[288] Arnaud HAMON, Expression, p. 114.
[289] Frédérique OLIVIER et Eric BARBRY, Hébergement, p. 1086. Aussi dans ce sens, Gérard HAAS et Olivier de TISSOT, La mise à disposition de pages Web est-elle dangereuse ?, Juriscom.net, 5 juin 1999.
[290] TGI Nanterre, 1ère ch. A, 8 décembre 1999, Lynda Lacoste c. Multimania et autres, disponible à l'adresse suivante : http://www.juriscom.net/txt/jurisfr/img/tginanterre19991208.htm.

Ayant manqué en partie à leurs obligations, les défenderesses sont déclarées responsables des atteintes - non contestées - endurées par Lynda Lacoste et condamnées à des dommages et intérêts et à la mise en place d'un « *processus de recherche approprié permettant de retrouver et de supprimer des sites qu'elles hébergent toutes les photographies représentant Lynda Lacoste* ».

Seule la société Multimania forme appel de ce jugement. Bon lui en prit, puisqu'elle obtient la faveur de la Cour d'appel de Versailles[291], pour défaut de preuve de la « *négligence ou imprudence* » de la société appelante.
La cour a rappelé que le fournisseur d'hébergement est tenu à une *« obligation de vigilance et de prudence quant au contenu des sites qu'elle accueille,* […] *qui s'analyse en une obligation de moyens portant sur les précautions à prendre et les contrôles à mettre en œuvre pour prévenir ou faire cesser le stockage et la fourniture de messages contraires aux dispositions légales en vigueur ou préjudiciables aux droits des tiers concernés* ». L'obligation de moyens en question « *n'implique pas l'examen général et systématique des contenus des sites hébergés* », mais doit se traduire par « *des diligences appropriées pour repérer tout site dont le contenu est illégal, illicite ou dommageable* ». L'hébergeur doit mettre en œuvre ces diligences, dès qu'il prend connaissance ou est informé d'une situation illicite ou douteuse. En l'espèce, il ne peut être reproché à Multimania « *de n'avoir pas procédé spontanément au contrôle du contenu du site litigieux qui a pu, en l'occurrence, légitimement lui rester inconnu, dès lors qu'elle ne saurait être investie, sans risque pour la liberté d'expression, de communication ou de création, d'une mission qui la conduirait à s'ingérer systématiquement dans les rapports de droit entre les particuliers* ». La cour ajoute que même le repérage du site n'aurait pas permis de voir que son contenu était illicite.

ii. Commentaire[292]

Les décisions Lacoste sont dans la lignée des décisions Hallyday mais elles ont le mérite, elles, de donner un avis limpide sur la question de la responsabilité des intermédiaires techniques. Elles se sont vivement prononcées pour une responsabilité pour faute, en précisant les obligations à remplir pour qu'un professionnel puisse échapper à toute responsabilité.
Même si le Tribunal de grande instance de Nanterre parle d'obligation de vigilance, il impose en fait aux fournisseurs d'hébergement une « *véritable obligation de surveillance et de censure préventive* »[293]. Il semble à cet égard aller trop loin. En prétendant qu'un moteur de recherche interne permet facilement de détecter les sites illicites, le tribunal s'est trompé[294]. On sait combien il est difficile de déterminer la nature illicite d'une information et que le *web* est en perpétuelle mouvance.
En fait, les obligations imposées au prestataire amènent une responsabilité à laquelle il est quasiment impossible d'échapper. « *Le régime de la responsabilité de droit commun serait donc tout aussi draconien que celui de la responsabilité éditoriale* »[295].

Lionel THOUMYRE relève le brio de la Cour d'appel de Versailles, dont le souci du détail des développements est remarquable[296]. La cour confirme la responsabilité pour faute de l'art. 1383 du CCF. Elle précise que l'identification du fournisseur de contenu n'est pas une cause

---

[291] CA Versailles, 12ème ch. section 1, 8 juin 2000, Multimania c. Lynda Lacoste et autres, disponible à l'adresse suivante : http://www.juriscom.net/txt/jurisfr/img/caversailles20000608.htm.
[292] Pour un commentaire plus fourni, voir Lionel THOUMYRE, Détours.
[293] Lionel THOUMYRE, Réglementation.
[294] Murielle CAHEN, Responsabilité des hébergeurs, http://www.murielle-cahen.com, décembre 1999.
[295] Lionel THOUMYRE, Réglementation.
[296] Lionel THOUMYRE, Détours.

d'exonération de responsabilité. Mais globalement, la décision ne traite que de l'obligation à la charge des prestataires la plus préoccupante : l'obligation de vigilance et de prudence. En ce sens, Lionel THOUMYRE pense que la cour a voulu adoucir le régime de responsabilité à l'encontre du prestataire d'hébergement, en tenant compte de la réalité technique et en précisant que l'obligation en question n'était qu'une obligation de moyens.

La décision de la Cour d'appel de Versailles a été délivrée le 8 juin 2000. Le même jour que l'adoption de la directive sur le commerce électronique. L'impact de la jurisprudence Lacoste a donc été conséquemment limité, les articles 14 et 15 de la directive ayant un contenu fort différent. La jurisprudence Lacoste ne va pas non plus dans le sens de la Loi n° 2000-719 du 1er août 2000. Il est d'ailleurs surprenant que les juges français n'aient pas plus pris en considération les travaux législatifs européens et français.
Une partie de la doctrine s'est félicitée que la jurisprudence Lacoste soit restée - presque - lettre morte, jugeant les obligations de diligence à la charge du fournisseur d'hébergement trop lourdes, inadaptées au fonctionnement d'Internet ou encore attentatoires à la liberté d'expression. Il n'empêche que la notion de « diligences appropriées », si bien précisée par la Cour d'appel de Versailles, ne doit pas être oubliée si vite. Lorsque l'on lit le considérant (48) de la directive sur le commerce électronique, qui est en relative contradiction avec l'art. 15, on remarque que cette notion pourrait revenir sur le devant de la scène.

2.2 La législation

2.2.1 Le *Teledienstgesetz*

L'art. 5 al. 2 du TDG a ce contenu : « *Dienstanbieter sind für fremde Inhalte, die sie zur Nutzung bereithalten, nur dann verantwortlich, wenn sie von diesen Inhalten Kenntnis haben und es ihnen technisch möglisch und zumutbar ist, deren Nuztung zu verhindern* ».

Le fournisseur d'hébergement est donc exonéré de toute responsabilité s'il remplit une des trois conditions alternatives suivantes :
- le prestataire n'a pas connaissance des contenus illicites ;
- il n'a pas la capacité technique de neutraliser l'utilisation de ces contenus ;
- le blocage des contenus n'est pas raisonnable.

2.2.2 La directive sur le commerce électronique

L'art. 14 de la directive, nommé « Hébergement », dit :

1. Les Etats 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.

2. Le paragraphe 1 ne s'applique pas lorsque le destinataire du service agit sous l'autorité ou le contrôle du prestataire.

3. Le présent article n'affecte pas la possibilité, pour une juridiction ou une autorité administrative, conformément aux systèmes juridiques des Etats membres, d'exiger du prestataire qu'il mette un terme à une violation ou qu'il prévienne une violation et n'affecte pas non plus la possibilité, pour les Etats membres, d'instaurer des procédures régissant le retrait de ces informations ou les actions pour en rendre l'accès impossible.

On remarque, dans le paragraphe 1, que les informations stockées l'ont été à la demande d'un tiers. L'hébergeur ne bénéficie pas de privilèges lorsque est en question un contenu qu'il stocke pour lui-même. Il ne bénéficie pas plus de privilèges lorsqu'il supervise le contenu hébergé.

2.3 Développements

2.3.1 Le contrôle de la licéité des informations stockées

Comme tout utilisateur d'Internet, l'hébergeur a accès aux sites stockés sur son serveur et peut donc, a priori, en vérifier le contenu. La différence avec les autres acteurs d'Internet est qu'il peut tout bonnement supprimer le contenu. Sans fournisseur d'hébergement, le contenu n'est pas accessible aux internautes, excepté évidemment le cas où le fournisseur de contenu possède son propre serveur. En ce sens, l'hébergeur est le premier prestataire dont nous étudions la responsabilité qui, pour reprendre les termes de la Cour d'appel dans l'affaire Hallyday, « *excède manifestement le rôle technique d'un simple transmetteur d'informations* ». C'est pourquoi son rôle est primordial dans la lutte contre les contenus illégaux.

La question est de savoir si un certain contrôle des informations enregistrées peut être exigé du prestataire d'hébergement.

Il faut exclure d'emblée l'obligation permanente de contrôle, car elle est impossible à mettre en pratique pour la plupart des hébergeurs, qui stockent sur leur serveur une quantité gigantesque de pages *web*, pouvant être modifiées à leur insu à tout instant[297]. Imposer au prestataire d'hébergement une obligation impossible à tenir, le rendrait responsable de tous les maux du net.
Pour le bon développement d'Internet, économiquement parlant, on ne peut imposer un contrôle trop lourd des pages *web* hébergées. On sait qu'actuellement - et pour longtemps encore, voire pour toujours -, aucun logiciel de filtrage n'est efficace. Seul un contrôle humain peut amener des résultats. Et peu d'hébergeurs peuvent se permettre le luxe, à l'image de Wanadoo, d'engager cinq « surveillants » à plein temps[298]. On imagine que ces cinq employés, qu'on espère juristes, doivent avoir du travail plein les bras. Si dans certains cas, la violation de la loi est flagrante, il est souvent difficile de trancher, à plus forte raison que les atteintes possibles sont très diverses. L'appréciation juridique est souvent délicate en cas de diffamation, de droit d'auteur ou de marque. Même pour les juges, assistés par des spécialistes, les réponses sont malaisées. Les employés de Wanadoo risquent alors de tomber

[297] Le site est modifié, dans la très grande majorité des cas, sans que le prestataire d'hébergement intervienne d'une quelconque manière. Le fournisseur n'est même pas averti des changements, très nombreux : c'est le propre d'un bon site d'être mis à jour fréquemment.

[298] Comme nous l'apprend Irina COSTA-FORU, Les fournisseurs d'hébergement face à leurs responsabilités, Intellex, 2000, p. 16.

dans l'arbitraire et d'opérer une censure non souhaitable[299]. La Police fédéral constate toutefois à cet égard que la liberté d'expression est en moindre danger lorsqu'il est question de la relation entre le fournisseur de contenu et l'hébergeur car, « *en vertu de la liberté de contrat, le fournisseur d'hébergement est libre de mettre son serveur à la disposition de qui il veut et pour quoi* »[300].

L'ensemble de ces éléments amène plutôt à penser qu'il faut libérer l'hébergeur d'un rôle de juge qui n'est pas le sien. Mais un minimum de collaboration peut paraître nécessaire dans la lutte contre les contenus illégaux. Si le *Teledienstgesetz* était univoque, la directive sur le commerce électronique exprime bien ce dilemme. Certes, son art. 15 interdit catégoriquement aux Etats membres d'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* ». Cette disposition paraît explicite. Mais le considérant (48) y rattaché laisse perplexe : « *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 d'empêcher certains types d'activités illicites* ». La directive permettrait donc aux Etats membres d'imposer, à certaines conditions, une recherche préventive de la part de l'hébergeur. Alain STROWEL, Nicolas IDE et Florence VERHOESTRAETE pensent que ce considérant devrait être interprété strictement de façon à limiter le rôle des intermédiaires au niveau de la prévention[301]. Il ne faut en effet pas vider de son sens l'art. 15. Les auteurs proposent que cette recherche préventive ne vise que certains types d'activités illicites, notamment les « *contenus justifiant une surveillance particulière* »[302] : les auteurs pensent évidemment aux contenus liés à la pornographie enfantine.

On a vu que, dans le passé, certains tribunaux français ne sont pas allés dans le sens du futur article 15 de la directive sur le commerce électronique, bien qu'ayant connaissance du projet de la directive. On sait que la directive a été très influencée par l'industrie d'Internet, qui a imposé des normes similaires à celles qu'on trouvait dans le DMCA. A notre sens, les tribunaux rebelles ont voulu tirer la sonnette d'alarme et souligné le danger de la trop forte déresponsabilisation des prestataires Internet. En d'autres termes, la directive ne protègerait que trop faiblement les droits des tiers.
Cette façon de voir a été appréciée par certains, très critiquée par d'autres. Elle a au moins eu le mérite d'afficher l'existence d'un autre courant. Nous avons souligné plus haut que ce courant, notamment exprimé par la jurisprudence Lacoste, pourrait être repris par les cours suisses, tant que le droit suisse ne subira pas de modification[303]. Il s'agirait d'exiger de l'hébergeur une obligation de vigilance dans le sens que l'attendait la Cour d'appel de Versailles, soit une obligation de moyens qui permettrait de déceler les contenus illicites

---

[299] Rappelons à cet égard que Thibault VERBIEST et Etienne WÉRY (Responsabilité, p. 170) pensent que, en sus de la liberté d'expression, la censure privée contrevient sûrement à des principes tels que la présomption d'innocence ou la compétence du pouvoir judiciaire pour rendre la justice. Le prétendu cyberdélinquant a-t-il toujours le droit à ce que sa situation soit examinée par un juge impartial au terme d'un procès équitable et contradictoire ? A notre sens, non. Il est des cas où le bon sens de tout en chacun doit permettre d'éviter l'utilisation de la justice.

[300] Police fédérale suisse, Responsabilité pénale, p. 7.

[301] Alain STROWEL, Nicolas IDE et Florence VERHOESTRAETE, Directive, p. 133ss.

[302] Pierre SIRINELLI (Responsabilité) avance pourtant que la jurisprudence Lacoste pourrait « *se recommander des termes du 48° considérant de la directive communautaire du 8 juin 2000* ».

[303] Dans ce sens, Jérôme BENEDICT, Responsabilité, p. 35.

apparents[304], mais bien évidemment pas un contrôle général, continu et approfondi. Plus concrètement, il pourrait être imposé au prestataire d'hébergement la mise en place de contrôles humains, aidés par quelques moyens techniques tels que les moteurs de recherche. Une réflexion et une décision humaine sont à notre avis nécessaires à toute intervention préalable à une notification.

Si beaucoup d'auteurs doutent qu'un tel contrôle doive être imposé, certains pensent qu'un contrôle pourrait être exigé à un moment bien précis : lors de la première mise en ligne, soit lorsque les données sont transférées par le créateur du site sur le serveur de l'hébergeur et que ce dernier attribue une adresse URL au nouveau site. A cet instant du processus, le prestataire a la possibilité de contrôler le contenu des informations, à tout le moins de voir le genre de site auquel il a affaire. En 1997, Etienne WÉRY écrivait : « *il nous semble qu'à cet instant, le fournisseur de services a le devoir de contrôler la nature de l'information qu'il accepte d'héberger, ou à tout le moins qu'il commet une imprudence s'il ne le fait pas* »[305]. Thibault VERBIEST a logiquement ajouté que « *si, ayant constaté que l'activité projetée est illégale ou dommageable, le fournisseur accepte néanmoins d'héberger le site, sa responsabilité pourrait être engagée* »[306]. Ce contrôle préalable devrait rester grossier. Il aurait toutefois pour conséquence d'amener une présomption de connaissance du prestataire d'hébergement, quant aux violations flagrantes de la loi. L'hébergeur ne pourrait par exemple pas nier avoir eu connaissance d'un site proposant des MP3 illégaux, si ce site était entièrement consacré à cette pratique.

En Suisse, en matière pénale, la Police fédérale estime que des contrôles régulièrement répétés ne peuvent pas être imposés à l'hébergeur[307]. Mais si le prestataire doit légitimement avoir des doutes quant à la licéité des informations stockées pour tel client, « *il peut lui être imposé de contrôler les contenus de ce fournisseur au moins par sondage* »[308]. La Police fédérale met en particulier en avant que, lors de la conclusion du contrat d'hébergement, certaines informations pourraient mettre la puce à l'oreille de l'hébergeur. Le cas échéant, l'hébergeur doit « *procéder aux recherches complémentaire nécessaires, au besoin en faisant appel à une autorité de poursuite pénale ou à des tiers professionnellement qualifiés* ». Mais le fait est qu'il est, en principe, plus facile de repérer un contenu punissable qu'un contenu illicite.

La charge imposée au prestataire en matière pénale n'est, à notre sens, pas transposable en matière civile, pour laquelle il faut convenir que le doute subsiste. Il est bien difficile de présager de l'usage de l'art. 41 du CO par le juge qui sera saisi de la question. Tout dépendra des intérêts qu'il jugera prépondérants. S'il met l'accent sur la protection des droits des tiers, il imposera aux fournisseurs d'hébergement une obligation de vigilance à l'image de ce qui a été préconisé par la Cour d'appel de Versailles dans l'affaire Lacoste, voire un contrôle grossier préalable à la mise en ligne du site. S'il accorde plus d'importance au développement d'Internet et à la liberté d'expression, il libérera le prestataire de toute obligation de contrôle général. Si, plus haut, nous avons utilisé le conditionnel, c'est parce que nous pensons que cette dernière solution est la meilleure[309]. La souplesse du droit suisse permet

---

304 Rolf H. WEBER (E-Commerce, p. 518) rapporte qu'Ulrich LOEWENHEIM et Frank A. KOCH (Praxis des Online-Rechts, Weinheim 1998, p. 428) vont dans ce sens.

305 Etienne WÉRY, Internet hors-la-loi ? Description et introduction à la responsabilité des acteurs du réseau, Journal des Tribunaux (Bruxelles), n° 5846, 7 juin 1997.

306 Thibault VERBIEST, Acteurs.

307 Police fédérale suisse, Responsabilité pénale, p. 6.

308 Police fédérale suisse, Responsabilité pénale, p. 7.

309 Rolf H. WEBER (E-Commerce, p. 518) va aussi dans ce sens.

l'eurocompatibilité. C'est là un intérêt que nous, Suisses, devons prendre en compte, ayant connaissance de la nécessité d'harmonisation des cadres juridiques vis-à-vis des Etats avec qui nous avons le plus de partages[310]. Il faut ajouter que cette solution s'impose d'autant plus que les membres de l'Union européenne n'ont pas profité du considérant (48) pour introduire une quelconque obligation de contrôle.

Précisons encore que si l'art. 41 du CO permet de tenir compte des circonstances concrètes du cas d'espèce, de manière générale, il ne faudra pas, à notre sens, que le juge traite différemment le petit et le grand hébergeur. Si le premier héberge moins de pages que le second, il a aussi moins de moyens à disposition.

Au final, s'il ne paraît pas irraisonnable d'exiger des hébergeurs un certain contrôle de la licéité des informations contenues dans les sites qu'ils mettent à disposition sur Internet, l'harmonisation des solutions fait pencher la balance vers l'absence d'obligation générale de surveillance des sites hébergés et de recherche active de contenus illégaux.

2.3.2 L'intervention du fournisseur d'hébergement en cas de connaissance

i. Généralités

Il est acquis que le fournisseur d'hébergement doit agir rapidement pour supprimer le contenu illicite s'il en a connaissance[311]. Il faut encore définir ce que l'on entend par connaissance. Nous avons déjà abordé cette problématique, notamment lorsque nous traitions de la responsabilité du fournisseur d'accès[312]. Pour l'hébergeur, le débat prend une tout autre dimension, car le fait que ce dernier prestataire doive agir en cas de connaissance est une certitude, ce qui est loin d'être le cas pour l'*access provider*.
La détermination de la notion de connaissance est une question primordiale que la directive sur le commerce électronique laisse sans réponse[313]. Elle ne dit pas à partir de quand et selon quelles modalités, l'hébergeur a une connaissance suffisante de la présence d'informations illicites sur son serveur. Tout juste son considérant (46) précise-t-il que le retrait des contenus illicites doit avoir lieu « *dans le respect du principe de la liberté d'expression* ». Cette déficience est une des critiques les plus véhémentes formulées à l'encontre du législateur européen[314]. Il est vrai que l'art. 14 de la directive est difficile à cerner sans précision de cette notion. La simple notification du prétendu lésé peut-elle être suffisante à la connaissance de l'hébergeur et si oui, dans quels conditions ? Ou seule la réquisition formelle d'une autorité officielle oblige-t-elle le prestataire ? Ces deux questions résument tout le débat.

---

[310] Jérôme BENEDICT (Responsabilité, p. 35) relève aussi l'importance d'« *éviter les solutions contradictoires* ».

[311] Effective ou positive, par opposition à négative. L'hébergeur a réellement connaissance de l'information : le fait qu'il aurait dû en avoir connaissance n'entre pas en cause, à partir du moment où l'on admet que le prestataire n'a pas à opérer une surveillance des sites qu'il héberge.

[312] Cf. Partie 3 B. 2.3.2 p. 44.

[313] Le « grand sage » Michel VIVANT (Responsabilité, p. 2025) avait pourtant dit : « *A légiférer, il faut* […] *d'abord que soit précisé comment doit caractérisée la connaissance requise de l'intermédiaire pour que sa responsabilité puisse être engagée* ».

[314] Par exemple, Alain STROWEL, Nicolas IDE et Florence VERHOESTRAETE, Directive, p. 144 ; Etienne WÉRY, Skynet. Pour ce dernier auteur, la non-définition de la notion de connaissance « *est d'autant moins acceptable que le problème est surmontable et purement politique* » et « *le législateur européen savait que le texte est impraticable* ».

Pour une grande partie de la doctrine, il serait trop restrictif de limiter la connaissance à la réquisition d'une autorité, qu'elle soit judiciaire ou administrative[315]. La nécessité de l'intervention de la justice ou de l'administration peut être un frein dans la protection des droits de tous. Certains préféreront se raviser, ne souhaitant pas entrer dans une procédure officielle qui leur fait peur. C'est sûrement pourquoi une mise en demeure de la victime doit pouvoir amener connaissance, à certaines conditions bien sûr.
Aujourd'hui, les fournisseurs d'hébergement sont quotidiennement saisis de demandes qui tendent à supprimer l'accès à des contenus illicites. Les hébergeurs les plus consciencieux y font droit, quand la violation de la loi ou des engagements contractuels souscrits par leurs usagers ne leur paraît pas faire de doute[316]. Les autres suppriment simplement les contenus litigieux, risquant alors de pratiquer une censure préjudiciable à la liberté d'expression et de voir se retourner contre eux leurs clients désavoués. On voit bien l'importance de la délimitation de la notion de connaissance, afin que la sécurité juridique tant souhaitée soit consacrée.

ii. La jurisprudence

Précisons le débat, en examinant comment la jurisprudence étrangère, avant l'adoption de la directive sur le commerce électronique, avait délimité la notion de connaissance.

La jurisprudence Lacoste était claire : la Cour d'appel de Versailles estimait évidemment que la notification du lésé oblige le prestataire d'hébergement à opérer les diligences appropriées. Aux Pays-Bas, le Tribunal d'arrondissement de La Haye[317] a estimé en juin 1999 que l'hébergeur est lié par la notification du lésé, s'il « *ne peut raisonnablement douter de la justesse de la mise en demeure* »[318]. Le 2 novembre 1999, le Tribunal de commerce de Bruxelles est allé dans ce sens dans une affaire opposant la Fédération internationale de l'industrie phonographique (IFPI) et Polygrams Records contre Belgacom Skynet, société d'hébergement[319]. Cette dernière hébergeait des sites qui proposaient des liens hypertextes vers d'autres sites offrant des MP3, violant ainsi le droit d'auteur des ayants droit. Informée par les demanderesses, Belgacom Skynet n'a pas supprimé les liens en question. Elle a ainsi été reconnue responsable, car elle ne pouvait raisonnablement douter de l'exactitude de la notification des demanderesses, n'ayant en outre pas reçu de preuve quant à la licéité des liens créés par ses clients. La condition de la connaissance était remplie. Thibault VERBIEST et Etienne WÉRY font remarquer que le juge belge a opéré une sorte de renversement du fardeau de la preuve, puisqu'il a estimé qu'« *il appartenait à l'hébergeur d'obtenir des responsables des sites « suspects » la preuve de la licéité de leur contenu musical téléchargeable* »[320]. La décision du Tribunal de commerce de Bruxelles a été sèchement critiquée, car elle semblait présumer que MP3 est toujours synonyme d'illégalité. Le 13 février 2001, la Cour d'appel de Bruxelles a rendu un jugement au fond, qui a passablement surpris les observateurs. Cherchant une solution praticable, les juges ont créé une sorte de

---

315 Par exemple, Bertil COTTIER, Conférence non publiée ; André LUCAS, Responsabilité ; Pierre TRUDEL, Responsabilité.

316 Dans le mois de janvier 2000, l'hébergeur Multimania, qui abrite 350.000 sites, aurait, d'après son responsable Michel Meyer, coupé l'accès à 1000 sites (Florent LATRIVE, Les hébergeurs priés de sévir. La loi va les obliger à la vigilance sur les contenus de leurs sites, Libération, 6 avril 2000, disponible à l'adresse http://www.liberation.com/multi/20000403/20000406.html).

317 Tribunal d'arrondissement, La Haye, 9 juin 1999, Church of Spiritual Technology c. XS4all et autres, *Computerrech*t, 1999/4, p. 200, disponible à l'adresse http://www.xs4all.nl/~kspaink/cos/verd2eng.html.

318 Traduction d'Alain STROWEL et Nicolas IDE, Responsabilité, p. 39.

319 Trib. Comm. Bruxelles, 2 novembre 1999, IFPI et Polygram Records c. SA Belgacom Skynet.

320 Thibault VERBIEST et Etienne WÉRY, Responsabilité, p. 166.

procédure de notification[321] ! Ils ont en effet considéré que le fournisseur d'hébergement devait agir, lors de la notification d'un lésé, si certaines conditions étaient remplies et selon une procédure définie par le tribunal lui-même. Le plaignant doit ainsi rédiger sa notification de telle manière que la condition de l'illicéité du contenu paraisse *prima facie* remplie[322]. Si c'est le cas, le prestataire d'hébergement dispose de trois jours ouvrables pour amener la preuve de la licéité du contenu en question. S'il n'y parvient pas, il doit suspendre la mise en ligne du site ou restreindre l'accès au site. S'il y parvient, le site reste logiquement accessible. Le plaignant risque de voir sa responsabilité engagée si le contenu a été suspendu pendant un certains temps, mais est reconnu licite après coup. Par ces motifs, la Cour d'appel de Bruxelles a jugé que Belgacom Skynet ne devait pas être reconnue responsable. Etienne WÉRY note l'influence frappante des procédures instaurées par le DMCA[323]. Il se demande surtout sur quelle base la cour se permet de devenir législateur et regrette le renversement du fardeau de la preuve opéré, non conforme à l'art. 14 de la directive sur le commerce électronique : le fournisseur d'hébergement « *doit avoir effectivement connaissance de l'activité ou de l'information illicite* », ce qui fait dire à l'auteur qu'il incombe au plaignant d'établir le caractère illicite de l'activité ou de l'information.

iii. La directive sur le commerce électronique et le *Digital Millenium Copyright Act*

L'art. 14 de la directive sur le commerce électronique distingue deux types de connaissance : la connaissance effective et la connaissance « *circonstanciée* »[324].

Commençons par étudier la connaissance effective. La directive étant muette quant à la délimitation de cette notion, on aurait pu espérer que les lois de transposition des membres de l'Union européenne nous fassent part de leur avis sur la question, afin que leurs juges nationaux n'aient pas à se livrer à ce terrible exercice. Pour l'instant, que nenni ! Pour donner un exemple, la législation française laisse, a priori, la porte ouverte à la notification du lésé, sans véritablement prendre position. La Loi du 1er août prévoyait déjà que les personnes dont l'activité est la fourniture d'hébergement sont responsables « *si, ayant été saisies par une autorité judiciaire, elles n'ont pas agi promptement pour empêcher l'accès à ce contenu* ». Le projet de LSI ajoute qu'elles sont aussi responsables « *si, ayant effectivement connaissance du caractère manifestement illicite de ce contenu, elles n'ont pas agi promptement pour le retirer ou en rendre l'accès impossible* ». Cela démontre que le législateur français pense que la connaissance effective peut ne pas découler uniquement de la notification d'une autorité judiciaire et que, dans ce cas, il faut que le contenu soit manifestement illicite.

La législation française nous donne un tout petit début de réponse, mais l'incertitude règne toujours en maître sur la question. En Europe, toutefois. Les problèmes liés à la notion de connaissance n'existent pas aux Etats-Unis, en tout cas en ce qui concerne le droit d'auteur. Le DMCA prévoit en effet des procédures précises de « *notice and take down* » et de « *counter notice and put back* ». Si la notification du plaignant respecte les conditions légales, elle entraîne la connaissance du *service provider*, qui doit donc agir rapidement pour faire cesser le trouble. Mais une contre-notification de l'éventuel auteur de l'atteinte est possible.

---

321 Cour d'appel Bruxelles (8ème ch.), 13 février 2001, SA Belgacom Skynet c. IFPI et Polygram Records.

322 Ce passage est largement inspiré d'Etienne WÉRY, Skynet.

323 Cf. ci-dessous.

324 Cette expression est utilisée par Alain STROWEL, Nicolas IDE et Florence VERHOESTRAETE, Directive, p. 144. Roman KELTNER (Haftung und Überwachungspflicht der Suchmaschinenbetreiber und Hyperlinksetzer nach dem Entwurf zum ö. E-Commerce-Gesetz (ECG), www.it-law.at) parle, lui, de « *fahrlässige Unkenntnis* » ou de « *Kennenmüssen* » : l'auteur autrichien oppose ces notions à la « *tatsächliche Kenntis* », la connaissance effective ou positive.

Sous certaines conditions, le *service provider* devra rétablir l'état des choses d'avant la première notification.

Pour le bon déroulement de ces procédures, le *service provider* doit désigner un agent, chargé, principalement, de recueillir les notifications des plaignants. Ce mandataire doit être annoncé auprès du *Copyright Office*, qui met à disposition sur son site *web* une liste des mandataires habilités. Le *service provider* doit également mettre en place une « hot-line » sur son site, permettant au plaignant d'avertir le mandataire sans passer par le *Copyright Office*.

Lorsque le *service provider* reçoit une notification, il doit contrôler que celle-ci répond aux conditions de forme imposées par le DMCA. La « *notice* » doit être suffisamment précise pour, notamment, identifier la partie plaignante et l'œuvre protégée et localiser le matériel contrefaisant. Elle doit également être accompagnée d'une déclaration sur l'honneur du prétendu titulaire du droit d'auteur qu'il y a effectivement violation du *copyright* par le tiers en cause. Si ces conditions légales sont remplies, le *service provider* doit promptement retirer le contenu contrefaisant ou en supprimer l'accès, sous peine d'engager sa responsabilité.
Ensuite, s'il souhaite éviter tout risque d'action de la part du prétendu auteur de la violation, le *service provider* doit l'avertir de la suppression du contenu ou de son blocage. Le titulaire du contenu prétendument contrefaisait peut alors lui adresser une contre-notification. Celle-ci doit remplir des conditions parallèles à celles de la *notice*, auxquelles il faut ajouter la condition selon laquelle le fournisseur du contenu s'engage à « *se soumettre le cas échéant à une procédure juridictionnelle ou, s'il est établi à l'étranger, à un organisme judiciaire approprié* »[325]. Ces mentions formelles doivent également être vérifiées par le prestataire. Dès réception de cette contre-notification, il doit en informer le prétendu titulaire du droit d'auteur et permettre à nouveau l'accessibilité du matériel en question, dans un délai de 14 jours ouvrables, à moins qu'il ne soit notifié dans l'intervalle que le titulaire prétendu du *copyright* a intenté une action en justice contre le titulaire du contenu prétendu contrefaisant.

Les règles complexes données par le paragraphe 512 du DMCA sont censées résoudre un certain nombre de problèmes pratiques. Elles permettent aux parties de faire valoir leur droits et au prestataire de savoir précisément ce qu'on attend de lui. Si ce dernier agit conformément aux procédures, il ne peut être tenu d'une quelconque responsabilité. Le système prévu par le DMCA tend donc à éviter les situations boiteuses. Il permet également de contrer les notifications infondées et leurs conséquences désastreuses, notamment sur la liberté d'expression, puisque l'auteur d'une notification infondée « *engage sa responsabilité vis-à-vis du fournisseur de contenu* »[326].
L'avenir nous dira si ce système est pleinement efficace. A première vue, il est prometteur. Il amène, a priori, la sécurité juridique tant recherchée.

Le législateur européen connaît l'importance de ces procédures de notification et de contre-notification. On ne peut en douter lorsque le considérant (40) de la directive sur le commerce électronique dit que « *la présente directive doit 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. Il conviendrait que de tels mécanismes soient élaborés sur la base d'accords volontaires négociés entre toutes les parties concernées et qu'ils soient encouragés par les Etats membres. Il est dans l'intérêt de toutes les parties qui participent à la fourniture de services de la société de l'information d'adopter et d'appliquer*

[325] Thibault VERBIEST, Références 2.
[326] Valérie SÉDALLIAN, Responsabilité. Pour un autre complément d'information, voir Arnold P. LUTZKER, Susan J. LUTZKER et Carl H. SETTLEMEYER, The Digital Millenium Copyright Act, ALA Washington Office, 18 novembre 1998, disponible à l'adresse http://www.ala.org/washoff/osp.html.

de tels mécanismes ». Le législateur invite l'industrie et les Etats membres à s'atteler à l'instauration des procédures en question, mais n'a pas voulu régler la question lui-même[327]. Pourquoi cette paresse ?

Il faut reconnaître que tout n'est sûrement qu'une question de temps. La clause de révision prévue à l'art. 21 de la directive sur le commerce électronique permet en effet l'espoir : le Parlement européen recevra, d'ici juillet 2003, et ensuite tous les deux ans, un rapport sur le caractère nécessaire ou non de l'introduction des procédures en question. Thibault VERBIEST et Etienne WÉRY relèvent tout de même qu'il s'agit « *d'une maigre consolation lorsque l'on connaît les délais de négociation et d'adoption des directives communautaires* »[328].

La délimitation de la notion de connaissance effective n'est pas le seul point épineux de la directive. Comme relevé plus haut, l'art. 14 de la directive sur le commerce électronique parle aussi d'un autre type de connaissance « circonstanciée ». Cet art. 14 dit qu'« *en ce qui concerne une demande en dommages et intérêts* », la « *connaissance de faits ou de circonstances selon lesquels l'activité ou l'information illicite est apparente* » suffit. Le degré de connaissance requis est donc moins rigoureux qu'en matière pénale. Une grosse négligence pourrait ainsi engager la responsabilité de l'hébergeur en matière de dommages et intérêts, dans le cas où il aurait pu aisément voir que l'information en question était bel et bien illicite[329].
Le DMCA parle aussi d'apparence. Dans le cadre de la loi américaine, il nous semble que l'introduction de cette notion sert surtout les cas où le prestataire n'est pas notifié, mais découvrirait par un autre biais des faits ou circonstances qui font apparaître l'illicéité comme apparente. Cette fonction se retrouve aussi dans la directive sur le commerce électronique, mais le prestataire n'étant pas tenu à une surveillance générale, elle n'a que peu d'importance. En fait, dans le cadre de la directive, la notion d'« illicéité apparente » pourrait principalement servir, en l'absence de procédures de notification et contre-notification, à amener la connaissance nécessaire lorsque le lésé notifie l'atteinte illicite à l'hébergeur sans prouver que cette atteinte existe réellement[330].

Si la notion d'« illicéité apparente » a jusqu'à présent été moins discutée que la notion de « connaissance effective », elle n'en est pas moins problématique, étant donné que la directive ne précise pas plus la pensée du législateur européen.

iv. En Suisse

En Suisse, doit-on aussi différencier les seuils de connaissance selon qu'il s'agit d'une demande en dommages et intérêts ou non ? Certains auteurs s'interrogent sur la pertinence de la différenciation opérée par le législateur européen[331]. Cette distinction tient sûrement au fait qu'en matière pénale, la négligence est, en principe, moins souvent punie qu'en matière civile. Il nous semble que, tant que la Suisse ne connaîtra pas de procédures de notification et de contre-notification, une telle différenciation pourrait s'avérer intéressante, puisqu'elle

---

327 Cf. aussi l'art. 14 al. 3 et l'art. 17 de la directive sur le commerce électronique.
328 Thibault VERBIEST et Etienne WÉRY, Responsabilité, p. 172.
329 Thomas STADLER, Die Verantwortlichkeit der Inhaltsanbieter nach der E-Commerce-Richtlinie und dem EGG, 2001, www.afs-rechtsanwaelte.de.
330 Alain STROWEL, Nicolas IDE et Florence VERHOESTRAETE, Directive, p. 144 : « *On peut considérer que dans ce cas, la notification peut être moins formelle que celle nécessaire pour créer la connaissance effective* ».
331 Par exemple, Alain STROWEL, Nicolas IDE et Florence VERHOESTRAETE, Directive, p. 144.

empêcherait le prestataire d'hébergement d'échapper au paiement de dommages-intérêts lorsque l'illicéité n'est pas prouvée, mais qu'il ne peut raisonnablement douter de son existence. En fait, tout dépend de la définition de la connaissance effective. Si elle signifie que le prestataire a une connaissance sûre de l'illicéité du contenu, parce que des preuves irréfutables ont été présentées ou parce que la notification provient d'un juge, la différenciation serait très utile. Si elle signifie que la prestataire doit aussi agir si le contenu est manifestement illicite, sans qu'une preuve ait été apportée, la différenciation n'aurait pas de raison d'être. Par conséquent, il faut, à notre sens, convenir que le terme « apparente » a la même signification que le terme « manifeste ». Cela n'empêche en rien la difficulté pour le prestataire de juger un contenu manifestement illicite, en matière de propriété intellectuelle ou de droits de la personnalité.

En matière pénale, la Police fédérale considère comme raisonnable le fait d'exiger de l'hébergeur, s'il reçoit des informations « *concrètes et détaillées* » de la part d'un tiers, qu'il vérifie la véracité de ces informations « *au besoin en faisant appel à une autorité de poursuite pénale ou à des tiers professionnellement qualifiés* »[332] et supprime le cas échéant le contenu punissable. Des informations moins qualifiées - que celles provenant d'un tribunal - peuvent donc suffire à engager la responsabilité pénale du fournisseur d'hébergement.
L'avis en pénal de la Police fédérale est assez proche de l'avis en civil de Pierre TRUDEL. Pour le professeur québécois, le prestataire d'hébergement ne doit supprimer le contenu que lorsqu'il est manifestement illicite, car l'inverse « *reviendrait à conférer à toute personne se croyant lésée* […] *un pouvoir de censure préalable* »[333]. Si le contenu est, de premier abord, manifestement illicite pour l'hébergeur, il doit supprimer le contenu dès réception de la plainte. Si l'illicéité ne lui est pas immédiatement manifeste, l'hébergeur devrait demander un avis juridique indépendant et agir conformément à l'opinion de l'expert neutre en question. Si le spécialiste confirme les dires du plaignant, le contenu devient alors manifestement illicite et le prestataire doit agir pour l'effacer.

Rolf H. WEBER pense que, si la notification provient du lésé, il est raisonnablement exigible de demander au fournisseur d'hébergement de faire des vérifications[334]. Il propose à cet égard que le « *Prüfungspflicht* » soit proportionnel aux informations contenues dans la notification du lésé. En d'autres termes, si le lésé fournit des preuves détaillées sur l'existence de l'atteinte, le prestataire devrait procéder à un contrôle soigneux du contenu en question ; en revanche, s'il ne procure que des informations imprécises, le contrôle devrait être limité aux atteintes manifestes. Cette approche est intéressante, car si nous pensons que la notification du lésé peut amener la connaissance de l'hébergeur, nous n'en pensons pas moins que le rôle de « contrôleur » de l'hébergeur est plus que délicat.

En l'état actuel du droit, il faut assurément penser que la notification du lésé amène, à certaines conditions, le seuil de connaissance nécessaire à l'intervention de l'hébergeur. Laissons l'hébergeur faire preuve de jugeote et agir le plus raisonnablement que possible pour trancher en faveur du lésé ou en faveur du fournisseur de contenu. Il peut le cas échéant les mettre en relation, afin de trouver un arrangement. Mais nous ne pensons pas que le prestataire d'hébergement doive, afin de ne pas violer son devoir de diligence, demander l'avis d'un expert externe pour trancher : peu d'hébergeurs pourraient se permettre un tel luxe. Le fournisseur d'hébergement doit, avec ses propres compétences, évaluer la situation. Si le

[332] Police fédérale suisse, Responsabilité pénale, p. 12. Par rapport à ce qui est exigé du fournisseur d'accès, la Police fédérale justifie sa prise de position essentiellement par la relation contractuelle entre le fournisseur de contenu et l'hébergeur.
[333] Pierre TRUDEL, Responsabilité.
[334] Rolf H. WEBER, E-Commerce, p. 519.

contenu en question lui paraît manifestement illicite, parce que son caractère illicite saute aux yeux ou parce que les preuves ou indices du lésé sont convaincants, il doit le supprimer ; s'il reste apathique, sa responsabilité pourra être engagée. Si la situation nécessite une analyse profonde des droits en présence, il prévient le lésé de sa décision d'inaction et il peut l'inviter à saisir la justice. Sa vigilance doit peut-être être plus grande, si le propriétaire du site est anonyme[335].

Cette opinion ne va pas dans le sens de la sécurité juridique. Les contours du comportement requis de l'hébergeur restent flous. Mais faudrait-il simplement déclarer que seule la notification d'une autorité officielle amènerait la connaissance du prestataire et ainsi brader les droits des tiers ? On reste sur nos positions et on répond que non. Pourtant, la sécurité juridique est primordiale. On ne peut laisser indéfiniment le premier cas de responsabilité du prestataire d'hébergement être lié à une notion si mal déterminée, qu'est celle de la connaissance.

On le répète, tous ces problèmes de délimitation de notions pourraient trouver solution dans la procéduralisation du droit. A terme - si possible court -, il faut instaurer des procédures similaires à celles que l'on trouve dans le DMCA, que ce soit dans une loi ou dans le cadre d'un code de conduite élaboré par les acteurs d'Internet. Tant que ces procédures ne seront pas aménagées, le fournisseur d'hébergement sera obligé de trancher et l'incertitude dominera les débats.

Pour conclure ce chapitre sur l'obligation d'action de l'hébergeur, on ajoutera que, afin de ne pas violer son obligation de diligence, le prestataire d'hébergement doit instaurer un système d'alerte, afin que les tiers qui s'estiment lésés puissent l'en informer rapidement[336]. Il faut aussi demander au fournisseur d'hébergement d'empêcher, dans la mesure du possible, la réouverture du site retiré sur son serveur. En ce sens, on pourrait exiger de l'hébergeur qu'il conserve l'adresse IP de l'ordinateur utilisé par le fournisseur de contenu pour le transfert du site vers le serveur d'hébergement et faire obstacle au téléchargement de toute autre donnée de l'ordinateur précité vers le serveur.

2.3.3 Les autres « obligations »

D'autres mesures tendant à éviter des dommages aux tiers peuvent être raisonnablement imposées à l'hébergeur. Comme déjà dit dans le chapitre sur le fournisseur d'accès[337], il n'est évidemment pas question d'obligations au sens traditionnel. Il s'agit de mesures, dont l'absence peut amener un juge à déclarer le fournisseur d'hébergement négligent et par conséquent, à le tenir pour responsable.
Outre la question controversée de la surveillance sur les contenus, il est donc des cas où la responsabilité de l'hébergeur peut être engagée, sans qu'il ait eu connaissance des contenus illicites. A l'image de ce qui a été dit pour le fournisseur d'accès, ces mesures transforment le prestataire en une sorte d'auxiliaire de justice.

---

335 C'est du moins ce qu'avancent Thibault VERBIEST et Etienne WÉRY (Responsabilité, p. 169).
336 En visitant, au hasard, le site de Geocities, on a pu voir que ce système était loin d'être « apparent »…
337 Cf. Partie 3 B. 2.4 p. 49.

i. L'obligation d'information vis-à-vis du client

Dans le contrat conclu avec son client, l'hébergeur doit l'informer de son obligation de respecter la législation suisse et les droits des tiers : il s'agit de faire adhérer le client à une charte de comportement. On pourrait aussi imposer au fournisseur d'hébergement des rappels, à l'image de ce qui a été dit dans la jurisprudence Lacoste. Une telle obligation pourrait être imposée par les pays communautaires dans le sens du considérant (48) de la directive sur le commerce électronique. A ce propos, il semble à Thibault VERBIEST et Etienne WÉRY que l'obligation d'information devrait être instaurée par une loi et non par la jurisprudence[338].

ii. L'obligation d'identification ou la prohibition de l'anonymat

Certains hébergeurs conservent l'anonymat du propriétaire du site *web* « *par obligation contractuelle, en raison de choix techniques ou pour des motifs d'ordre éthique* »[339]. Cette pratique risque de leur coûter cher.

La jurisprudence française s'est souvent exprimée sur la question de l'identification et de l'anonymat de l'auteur. Dans l'affaire Estelle Hallyday, on sent que l'anonymat dont avait bénéficié le propriétaire du site Silversurfer a été la cause principale de la responsabilité de Valentin Lacambre, ou, du moins, une circonstance aggravante. Dans l'affaire Lynda Lacoste, la Cour d'appel de Versailles a jugé que, parmi les diligences appropriées à la charge de l'hébergeur, celui-ci devait prendre « *des mesures préventives telles la prohibition de l'anonymat ou de la non-identification* »[340]. Aux Pays-Bas, il faut noter que dans l'affaire XS4all, citée plus haut[341], le tribunal a obligé le prestataire d'hébergement à divulguer l'identité du fournisseur de contenu dans les trois jours à compter de la demande par l'ayant droit, faute de voir sa responsabilité engagée.

Au niveau législatif, on rappelle qu'en France, l'art. 43-9 de la loi n° 86-1067 du 30 septembre 1986 relative à la liberté de communication instauré par la loi n° 2000-719 du 1er août 2000 prévoit que les hébergeurs - et les fournisseurs d'accès - doivent « *détenir et conserver les données de nature à permettre l'identification de toute personne ayant contribué à la création d'un contenu des services dont elles sont prestataires* ». Le fournisseur d'hébergement peut, comme le fournisseur d'accès, conserver ses fichiers *logs*[342]. Il possède aussi les informations qu'il a pu glaner lors de la conclusion du contrat d'hébergement. Mais comme l'a justement remarqué le Tribunal de grande instance de Nanterre dans l'affaire Lacoste, en général, l'hébergeur « *se borne à recueillir ses déclarations sur ce point sans en vérifier la réalité, se contentant d'une adresse e-mail pour ouvrir un compte* »[343].
L'art. 15 al. 2 de la directive sur le commerce électronique permet aux Etats membres d'instaurer l'obligation « *de communiquer aux autorités compétentes, à leur demande, les*

---

338 Thibault VERBIEST et Etienne WÉRY, Responsabilité, p. 169. Les auteurs notent aussi que le premier projet de directive sur le commerce électronique prévoyait que l'obligation d'information était une condition de l'exonération de responsabilité.

339 Frédérique OLIVIER et Eric BARBRY, Hébergement p. 1088.

340 CA Versailles, 12ème ch. section 1, 8 juin 2000, Multimania c. Lynda Lacoste et autres, disponible à l'adresse suivante : http://www.juriscom.net/txt/jurisfr/img/caversailles20000608.htm.

341 Cf. Partie 3 E. 2.3.2 ii p. 70.

342 Il ne pourra toutefois pas découvrir le propriétaire de la machine correspondant à l'adresse IP révélée par les *logs* sans l'aide d'un fournisseur d'accès. Cf. à ce propos Partie 3 I. 3 p. 111.

343 TGI Nanterre, 1ère ch. A, 8 décembre 1999, Lynda Lacoste c. Multimania et autres, disponible à l'adresse suivante : http://www.juriscom.net/txt/jurisfr/img/tginanterre19991208.htm.

informations permettant d'identifier les destinataires de leurs services avec lesquels ils ont conclu un accord d'hébergement ». « *L'anonymat pourra être source de responsabilité autonome dès lors qu'un Etat membre, usant de la faculté qui lui reconnaît l'article 15-2, oblige les hébergeurs à identifier leurs clients* »[344].
Le projet belge de transposition prend la balle au bond, en prévoyant, à son art. 22 al. 2, un devoir de communiquer aux autorités compétentes, à leur demande, les informations permettant d'identifier le propriétaire du site. L'*E-Commerce-Gesetz* autrichien va plus loin. Tout d'abord, l'art. 18 al. 2 prévoit, pour tout prestataire, l'obligation de communiquer, sur demande d'un tribunal, les informations qui permettent d'identifier l'utilisateur du service afin d'empêcher, de déterminer, d'expliquer et de poursuivre des infractions pénales. Ensuite, l'art. 18 al. 3 dit que l'hébergeur - et seulement lui - doit délivrer, sur injonction d'une autorité administrative, les noms et adresse de son client dans la mesure où la connaissance de ces informations constitue une condition essentielle de l'accomplissement du devoir des autorités. Finalement, la loi autrichienne prévoit, à son art. 18 al. 4, que le prestataire d'hébergement doit transmettre les noms et adresse de son client sur demande de tierces personnes, à la condition que ces personnes rendent vraisemblable un intérêt juridique prépondérant à l'établissement de l'identité du fournisseur de contenu et d'un état de faits manifestement illicite et si la connaissance de ces informations constitue une condition essentielle de la poursuite judiciaire. Le lésé - ou une association de consommateurs - peut donc demander directement à l'hébergeur de divulguer l'identité du fournisseur de contenu.

Aux Etats-Unis, l'art. 512h du DMCA prévoit que le titulaire du droit d'auteur peut solliciter une « *subpoena to identify infringer* » au greffe de n'importe quel tribunal de district du pays : cette mesure oblige le *service provider* à révéler l'identité du prétendu contrefacteur.

En Suisse, l'hébergeur n'est actuellement soumis à aucune obligation de conserver ses fichiers *logs* au sens de la Loi fédérale sur la surveillance de la correspondance par poste et télécommunication, car cette dernière ne s'applique pas aux hébergeurs, conformément à l'art. 1 al. 2. De plus, cette obligation n'aurait que peu concerné les cas d'engagement de responsabilité civile[345]. Autant on n'en déduisait que l'obligation de conserver et de communiquer les *logs* de connexion ne pouvait alors pas être exigée par le juge du fournisseur d'accès, autant il faudrait, à notre sens, convenir de l'inverse pour l'hébergeur parce que cette obligation est bien moins lourde que pour le fournisseur d'accès. Pour pouvoir éviter qu'un tribunal le déclare négligent et le tienne pour responsable, l'hébergeur devrait prendre toutes les mesures, afin d'être en mesure d'identifier le fournisseur de contenu. Il devrait donc demander les noms et adresse de son client, et pas seulement une adresse *e-mail*. S'il promet l'anonymat à son client, il devrait également prévoir dans le contrat une clause qui lui permette de mettre fin à son obligation de discrétion en cas d'infraction pénale ou d'atteinte aux droits d'un tiers : sinon, il se retrouverait tiraillé entre deux obligations, dont il ne pourrait en satisfaire qu'une seule. Si le système technique mis en place ne permet pas de déterminer l'adresse IP de l'ordinateur utilisé par son client, il devrait en changer, car l'adresse Internet reste le meilleur moyen d'identifier les internautes, qui ont trop souvent tendance à jouer à Pinocchio. Quant aux considérations éthiques, qui seraient un frein à la « dénonciation » du fournisseur de contenu, elles ne sont pas pertinentes. De toutes façons, comment l'hébergeur pourrait-il se cacher derrière la morale, quand il empêche le lésé de pouvoir s'attaquer à la personne premièrement responsable du préjudice subi[346] ?

---

[344] Thibault VERBIEST et Etienne WÉRY, Responsabilité, p. 169.
[345] Cf. Partie 3 B. 2.4.1 p. 49.
[346] Pour de plus amples développements, cf. Frédérique OLIVIER et Eric BARBRY, Hébergement, p. 1088.

Reste à savoir qui peut exiger du prestataire d'hébergement le communication des informations permettant l'identification du fournisseur de contenu. Alors que la France était vierge de toute disposition législative touchant à la question, Sébastien CANEVET pensait que le prestataire ne devait donner suite à une telle requête qu'à « *certaines conditions de fond et de procédure bien précises, ceci afin de préserver la confidentialité des informations recueillies* »[347]. C'est ainsi que l'auteur préconisait que le fournisseur d'hébergement ne communique les fichiers *logs* que sous injonction d'une autorité officielle, à l'image de ce qui peut exister en matière de surveillance téléphonique. Au décompte des législations, seule l'Autriche permet au lésé, à certaines conditions, de demander au fournisseur d'hébergement la divulgation de l'identité de l'auteur - présumé - de l'atteinte. La Suisse doit-elle suivre cette voie ? La tradition nous ferait dire non, mais le bon sens nous pousse vers le oui. En effet, si le prestataire doit supprimer un contenu manifestement illicite à la requête du lésé, pourquoi ne devrait-il pas aussi révéler l'identité du cyberdélinquant, toujours si le contenu est manifestement illicite ? On n'y voit aucune raison valable[348], même si l'art. 15 al. 2 de la directive parle seulement de « *communiquer aux autorités compétentes* ».

A notre sens, la prohibition de l'anonymat doit être une condition de l'exonération du prestataire d'hébergement en Suisse. L'anonymat est souvent malsain. Même s'il n'est que relatif[349], il amène fréquemment le sentiment d'irresponsabilité et pousse certaines personnes à perpétrer des agissements que les mêmes personnes auraient évités à visage découvert. A notre avis, les tribunaux suisses devraient par conséquent tendre vers un système proche de celui instauré en Autriche.

Il faut encore noter que, si le propriétaire du site doit être connu du prestataire d'hébergement, il ne devrait pas être connu de tous : une obligation de dévoiler son identité à tout internaute par des indications sur le site ne nous semble pas adéquate au niveau de la liberté d'expression[350].

iii. L'obligation d'avertir promptement les autorités

Nous nous reportons à cet égard à ce qui a été dit concernant le fournisseur d'accès[351]. En résumé, une telle obligation est inutile en matière civile, un juge ne pouvant être saisi que par la partie lésée. En ce sens, l'art. 15 al. 2 de la directive sur le commerce électronique ne sert qu'en matière pénale. L'art. 21 al. 3 du projet belge de transposition de la directive sur le commerce électronique prévoit ainsi que « *lorsque le prestataire a une connaissance effective d'une activité ou d'une information illicite, il les communique sur le champ au Procureur du Roi qui prend les mesures utiles…* » ; tant que le Procureur n'a pas tranché, le prestataire d'hébergement ne peut qu'empêcher l'accès aux informations. On parle du « Procureur », donc bien du domaine pénal.

iv. L'obligation temporaire de surveillance

Comme expliqué pour le fournisseur d'accès, s'il ne faut pas exiger de l'hébergeur une surveillance générale et continue, une obligation spécifique et temporaire pourrait lui être

---

347 Sébastien CANEVET, Rapport.

348 Selon nous, il ne faut pas craindre, de la part du lésé, un comportement attentatoire à la protection des données personnelles.

349 Cf. Partie 3 I. 3 p. 111.

350 Dans ce sens, Sébastien CANEVET, Rapport.

351 Cf. Partie 3 B. 2.4.2 p. 50.

demandée. C'est dans ce sens que va le considérant (47) de la directive sur le commerce électronique. Mais encore faut-il qu'une telle charge soit consacrée par une loi : à notre avis, un juge ne peut créer une obligation aussi lourde. Actuellement, l'hébergeur n'est ainsi pas assujetti à une telle obligation, car, comme déjà relevé, il n'est pas soumis à la Loi fédérale sur la surveillance de la correspondance par poste et télécommunication. Il ne peut donc pas être astreint à une surveillance au sens de cette loi, qui, plus est, ne concerne que le domaine pénal.

2.4 Conclusions

Aujourd'hui, le degré de diligence requis de l'hébergeur est en Suisse difficile à circonscrire : ce prestataire a beaucoup de cartes en main, mais il est difficile de déterminer celles qu'il doit jouer afin d'éviter toute responsabilité. Selon nous, en matière civile, il faut en tout cas lui imposer l'obligation d'action - l'intervention en cas de connaissance -, l'obligation d'information vis-à-vis de son client et l'obligation d'identification de ce client.

F. Le gérant d'un outil de recherche

1. Notions

Les outils de recherche sont les lieux incontournables du *World Wide Web*. Les services qu'ils fournissent ont constitué l'un des éléments essentiels au développement d'Internet en permettant la réunion des chercheurs d'informations et des donneurs d'informations.
Sans les instruments de localisation de l'information[352], nul espoir de tomber par hasard sur la page courue si l'internaute « voyage » sans adresse précise. Il ne faut pas oublier qu'il existe des milliards de pages *web* et qu'elles ont la fâcheuse tendance d'être en perpétuel mouvement.
Sans les instruments de localisation de l'information, un site *web* serait invisible sur la toile, sauf publicité. Pour survivre, un site doit être répertorié dans un outil de recherche, si possible en haut de liste. Vanina SPACENSKI parle en ce sens de « *référencement nécessaire* »[353].

Les outils de recherche sont principalement de deux types : les moteurs de recherche[354] et les annuaires ou répertoires[355]. La confusion entre ces deux outils est grande chez le non-initié. Cela provient particulièrement du fait qu'un annuaire est souvent lié à un moteur de recherche, afin de pallier au manque d'exhaustivité des listes de sites qu'ils proposent. Ainsi, l'annuaire Yahoo utilise le moteur de recherche Goggle[356] et l'annuaire juridique Findlaw[357] utilise le moteur de recherche LawCrawler[358].
De fonctionnement différent, les moteurs de recherche et les annuaires souffriront un traitement juridique distinct. L'architecture technique de ces outils de recherche sera, comme pour les autres fournisseurs de services Internet, très importante dans la détermination de leur régime de responsabilité.

---

352 Traduction de « *information location tools* », expression utilisée dans le DMCA.
353 Vanina SPACENSKY, Promotion.
354 Comme exemples, on peut citer le célèbre Lycos (http://www.lycos.com) et l'efficace Google (http://www.google.net).
355 L'exemple le plus évident est Yahoo! (http://www.yahoo.com).
356 Danny SULLIVAN, How search engines work ?, disponible à l'adresse suivante : http://www.searchenginewatch.com/webmasters/work.html.
357 http://www.findlaw.com.
358 http://www.lawcrawler.com.

2. La responsabilité des outils de recherche pour les contenus illicites référencés

2.1 Généralités

Malgré leur caractère quasi indispensable dans la chaîne de diffusion des informations sur la toile, les outils de recherche n'en sont évidemment pas moins soumis au respect des lois. En tant que ces outils d'aide à la navigation offrent un accès direct à des pages *web* au moyen de liens hypertextes, ils peuvent engager leur responsabilité pour avoir facilité la découverte d'un contenu illicite[359]. Après les vifs débats sur la responsabilité des fournisseurs d'accès et des prestataires d'hébergement, les discussions concernant les outils de recherche vont être au cœur de l'actualité ces prochains temps, notamment en Europe, puisque la question n'est pas réglée par la directive sur le commerce électronique. Leur caractère d'aide essentielle devrait néanmoins amener les législateurs et les juges à « *avoir à leur égard une attitude tolérante* »[360].

En Suisse, à l'instar des autres prestataires Internet, il faut appliquer aux outils de recherche le droit commun de la responsabilité civile et plus spécialement l'art. 41 du CO. Les circonstances de l'espèce seront décisives, mais nous esquisserons déjà quelques grandes lignes du débat.

2.2 La législation

Si, comme déjà dit[361], la directive sur le commerce électronique ne traite pour l'heure pas de la responsabilité des outils de recherche, ni de celle des fournisseurs de liens hypertextes, elle introduit un moratoire en la matière : l'art. 21 de la directive nous fait dire que la régulation européenne de la question n'est qu'une question de temps. Il appartient néanmoins aux Etats membres de l'Union européenne de légiférer dans le domaine. L'Autriche a saisi la balle au bond et nous délivre une réglementation assez surprenante. Le législateur espagnol prévoit aussi la responsabilité des outils de recherche et des fournisseurs de liens dans son projet du 22 février 2002. Mais examinons, en premier lieu, l'appréhension de la responsabilité des outils de recherche par le DMCA.

2.2.1 Le *Digital Millenium Copyright Act*

Le premier texte en vigueur traitant de la responsabilité des outils de recherche est le *Digital Millenium Copyright Act*. L'article 512d de cette loi aborde la responsabilité, pour complicité de violation du droit d'auteur, des *service providers* qui ont amené les internautes à un contenu ou une activité contrefaisants « *by using information location tools, including a directory, index, reference, pointer, or hypertext link* ». Les conditions d'exonération sont les mêmes que celles de l'hébergeur. Plus précisément, le prestataire :

---

359 « *Pour les infractions les plus graves, il n'est pas concevable de déresponsabiliser a priori un maillon de la chaîne de navigation de l'information, et de proclamer que tel ou tel acteur bénéficie d'une immunité* » dixit Vanina SPACENSKY (Promotion).

360 Jérôme BENEDICT, Responsabilité, p. 39.

361 Cf. Partie 2 C. 1.2.4 p. 28.

- ne doit pas avoir une connaissance effective - ou de fait - du contenu ou de l'activité violant le droit d'auteur et ne doit pas être conscient de faits ou circonstances qui rendraient le caractère contrefaisant apparent ;
- doit promptement retirer les informations en question ou en bloquer l'accès, s'il a la connaissance ou la conscience décrites au premier point ;
- ne doit pas percevoir un avantage financier provenant directement de l'activité contrefaisante, dans le cas où le fournisseur a le droit et la capacité de contrôler cette activité ;
- et doit respecter les règles de procédure de notification et contre-notification vues précédemment[362].

2.2.2 Le *E-Commerce-Gesetz* autrichien

L'art. 14 al. 1 du *E-Commerce-Gesetz* prévoit les mêmes exceptions de responsabilité pour les moteurs de recherche et autres moyens électroniques de recherche d'informations étrangères que ce que prévoit la directive sur le commerce électronique pour les fournisseurs d'accès. Le prestataire n'est donc pas responsable s'il n'est pas à l'origine de la transmission des informations demandées, ne sélectionne pas le destinataire des informations demandées et ne sélectionne, ni ne modifie les informations demandées.
L'alinéa second de l'art. 14 prévoit que l'alinéa 1er ne s'applique pas lorsque le destinataire du service agit sous l'autorité ou le contrôle de l'outil de recherche. Il ressemble en cela à l'art. 14 al. 2 de la directive sur le commerce électronique, qui touche le fournisseur d'hébergement.
Mais l'important est que les conditions d'exonérations sont typiquement celles d'un fournisseur d'accès. Cette façon de voir est d'autant plus étonnante que le projet du *E-Commerce-Gesetz* du 25 juin 2001 prévoyait les mêmes conditions d'exonération que pour les fournisseurs d'hébergement ! A dire vrai, nous verrons que le rapprochement avec les fournisseurs d'accès n'est de loin pas approprié.

2.2.3 Le projet espagnol de loi sur les services de la société de l'information et du commerce électronique[363]

L'art. 16 du projet espagnol dit (traduction libre) :

1. Les prestataires de services de la société de l'information qui fournissent des liens vers d'autres contenus ou incluent des contenus dans leurs répertoires ou instruments de recherche ne sont pas responsables de l'information vers laquelle ils dirigent les destinataires de ses services, à condition que :
a) ils n'aient pas effectivement connaissance du caractère illicite de l'activité ou de l'information à laquelle ils renvoient ou qu'ils recommandent, ou du fait qu'elle peut léser les biens ou les droits d'un tiers susceptibles d'indemnisation ou ;
b) s'ils en ont connaissance, ils fassent preuve de diligence pour supprimer ou mettre hors d'état le lien correspondant.
Sans préjudice des procédés de détection et de retrait des contenus que les prestataires appliquent en vertu d'accords volontaires et d'autres moyens de connaissance effective qui pourraient s'établir, on considèrera que les circonstances signalées en a) sont caduques quand une autorité compétente aura déclaré l'illicéité des données, ordonné qu'on les retire

[362] Cf. Partie 3 E. 2.3.2 iii p. 72.
[363] Boletín Oficial del Congreso de 22 de febrero de 2002, Nùm 68-1.

ou que leur accès ait été rendu impossible, ou aura déclaré l'existence du dommage, et le prestataire connu la « correspondiente resolución ».

2. L'exemption de responsabilité établie par le premier paragraphe n'est pas opérante dans le cas où le destinataire du service agit sous la direction, l'autorité ou le contrôle du prestataire qui facilite la localisation des contenus en question.

Le projet espagnol rapproche donc la situation des outils de recherche de celle des hébergeurs.

2.2.4 Remarques

Premièrement, il est intéressant de remarquer que deux des trois législateurs qui ont souhaité traiter de la responsabilité des outils de recherche ont simplement repris les conditions d'exonérations des fournisseurs d'hébergement. Cela peut paraître étonnant, étant donné que l'influence technique de l'outil de recherche sur le contenu est moindre que celle de l'hébergeur[364]. Si un outil de recherche ne permet plus l'accès à un contenu illicite, ce dernier n'en reste pas moins accessible par un autre chemin. A l'inverse, l'hébergeur peut supprimer le contenu[365]. C'est pourquoi on peut penser, a priori, qu'en l'état actuel du droit suisse, la responsabilité de l'outil de recherche devrait être plus difficilement engagée que celle d'un hébergeur.

Deuxièmement, il faut aussi noter que les textes en question assimilent les moteurs de recherche et les annuaires dans leurs réflexions. C'est surprenant dans la mesure où le fonctionnement de ces deux instruments de recherche est bien différent. Nous verrons par la suite si cette assimilation peut se justifier en Suisse.

3. Les moteurs de recherche (*crawler-based search engines*)

3.1 Notions

Les moteurs de recherche sont des logiciels d'orientation placés sur un site Internet, qui permettent à l'internaute de trouver, à l'aide de mots-clés, l'information qu'il souhaite sur le *web*. Lorsque l'internaute soumet un ou plusieurs mot-clés au moteur de recherche, le site lui délivre un extrait de sa base de données, soit une liste d'hyperliens renvoyant aux pages *web* contenant le ou les mots-clés soumis. Les pages indiquées sont censées contenir l'information recherchée.

Plus schématiquement, un moteur de recherche peut être décomposé en trois parties bien distinctes :

- Un logiciel d'exploration, appelé « robot »[366]. Il explore les pages *web* du monde entier[367] en suivant les hyperliens de ces pages et les indexe automatiquement dans une base de données. L'indexation s'accomplit surtout en fonction des mots-clefs que ces pages renferment, notamment dans l'URL du document HTML, dans leur titre ou dans les

[364] Dans ce sens, Rolf H. WEBER, E-Commerce, p. 532.
[365] Même s'il est vrai qu'il y a tous les risques qu'il réapparaisse sur le serveur d'un autre prestataire d'hébergement.
[366] En anglais, « *spider* » ou « *crawler* ».
[367] En fait, selon le site http://www.dicofr.com, BrightPlanet évalue à seulement 16% les pages *web* prises en compte par les moteurs de recherche classiques.

balises meta-tags[368]. Le référencement devient très efficace, lorsque ces méthodes sont combinées avec d'autres, à l'image de celle qui fait dépendre le référencement du nombre d'hyperliens renvoyant au site visité[369].

- La base de données[370], « *gigantesque mémoire où est enregistrée pour chaque mot-clé présent dans les pages d'Internet, une liste des pages contenant ce mot* »[371]. Elle est mise à jour automatiquement à intervalles réguliers[372].
- Le programme qui cherche dans la base de données l'URL des pages qui correspondent au(x) mots-clé(s) soumis par l'utilisateur et qui les classe dans l'ordre qui lui semble le plus relevant. L'ordre des documents proposés est fixé selon un « score de pertinence », qui dépend, entre autres, de la fréquence d'occurrence des mots-clés.

Ainsi, quand un internaute clique sur « Va chercher ! » sur le site de Lycos, le chien ne clique pas à la vitesse de la lumière sur toutes les pages *web* du monde pour trouver l'information requise : il se contente de fouiner dans la base de données. Le travail d'indexation a déjà eu lieu. Cette indexation est automatique. Il n'y a aucun contrôle humain. Ce contrôle n'a d'ailleurs, a priori, aucun sens puisque la vocation d'un moteur de recherche est « *l'indexation exhaustive et non sélective de l'information* »[373].

Il faut noter l'existence d'une exception à l'automaticité de l'indexation. Les moteurs de recherche proposent souvent un fichier de soumission, que peut remplir tout propriétaire de site souhaitant voir son site être référencé. On parle d'indexation « *manuelle* »[374] . Peut-on alors rapprocher le régime de responsabilité du moteur de recherche à celui d'un annuaire ?

3.2 La responsabilité pour le contenu illicite des sites référencés

L'indexation étant automatique et censée exhaustive, il est évident que des sites illicites feront partie du lot. Les moteurs de recherche doivent-ils pour autant en être tenus pour responsables ? Un cas d'engagement de leur responsabilité semble évident : le refus de « déréférencer » le site litigieux en cas de connaissance de son caractère illicite. Mais la responsabilité du moteur de recherche pourrait également être engagée du fait de sa négligence, pour avoir facilité l'accès à des contenus illicites. Deux éventuels cas de négligence du moteur de recherche méritent d'être étudiés : l'acceptation de mots-clés suspects dans la base de données et le non-contrôle des sites référencés[375].

3.2.1 Le refus de désindexer un site illicite en connaissance de cause

Ce comportement est le plus apte à engager la responsabilité du moteur de recherche. Si le gérant du moteur de recherche a connaissance du caractère illicite d'un site indexé et qu'il ne

---

368 Les meta-tags ou metas sont des informations incluses dans le code source d'une page *web*, invisibles pour l'internaute. Les metas permettent non seulement au *webmaster* de donner des mots-clés au moteur de recherche, mais aussi une brève description de la page par une « phrase-clé ». Voir Murielle CAHEN, Les metas, http://www.murielle-cahen.com, février 2001 ; Thibault VERBIEST, Références 1.

369 Pour de plus amples renseignements sur les méthodes d'indexation, voir Thibault VERBIEST, Références 1.

370 En anglais, « *index* » ou « *catalog* ».

371 Recherche intelligente sur Internet, par les membres du projet Clever, Pour la science, n° 262 août 1999, p. 52.

372 Les mises à jour se font généralement tous les mois ou tous les deux mois.

373 Murielle CAHEN, Mémoire cache et responsabilité, http://www.murielle-cahen.com, avril 2001.

374 Thibault VERBIEST, Références 1, p. 4.

375 Ces cas sont inspirés de Valérie SÉDALLIAN, Outils. Ils ont aussi été repris par Carole ABOUT, Responsabilité.

le déréférence pas, sa responsabilité pourra être engagée. Il est clair que si la dénonciation est l'œuvre d'une autorité judiciaire compétente, le moteur de recherche n'a de choix que de suivre l'injonction du juge, sinon il sera certainement tenu pour civilement responsable[376]. Mais les notifications peuvent aussi être émises par le lésé. Certains moteurs de recherche permettent de telles dénonciations par des fenêtres spéciales de soumission[377]. Dans tous les cas, il est très souvent possible d'envoyer un *e-mail* au responsable du site. Ces dénonciations privées obligent-elles le moteur de recherche à action ? On en revient à la délimitation de la notion de connaissance et à la problématique des procédures de notification. Il convient de se référer à ce qui a été dit au sujet des fournisseurs d'hébergement[378]. Les deux situations sont pleinement assimilables - à la différence de celle du fournisseur d'accès par exemple -, car il est techniquement autant facile de déréférencer un site - et de ne pas le référencer à nouveau - que de le supprimer d'un serveur. Le responsable du moteur de recherche doit, par conséquent, mettre en place un système d'alerte ou, au moins, placer une adresse *e-mail* valable sur le site, afin que tout lésé puisse opérer une notification. Si Valérie SÉDALLIAN relève que « *la raison d'être d'un outil de recherche est de donner accès à l'information, pas de porter des jugements de valeur* »[379], il faut se résoudre à demander au moteur de recherche de distinguer les contenus manifestement illicites des autres contenus. Il devra déréférencer les pages *web* qui mènent aux contenus manifestement illicites, sous peine de voir sa responsabilité engagée. Par contre, s'il reste un doute quant à l'illicéité du contenu, le moteur de recherche doit attendre une réquisition judiciaire.

3.2.2 L'acceptation de mots-clés suspects

Afin de ne pas violer leur devoir de diligence, les moteurs de recherche devraient-ils refuser d'indexer les sites ou pages *web* dont les mots-clés font référence à des comportements illicites, tels que « négationnisme » ou « pédophilie » ? La réponse est délicate, car on en revient à la fameuse problématique des techniques automatiques de filtrage.

Techniquement, il est aisé d'éviter le référencement de sites contenant ce genre de mots suspects : une liste noire et le tour est joué. Cette pratique simpliste de filtrage est du reste courante. Les moteurs de recherche tentent de préserver au mieux leur image, partie importante de leur capital[380]. Mais comme le remarque justement Valérie SÉDALLIAN[381], aucun logiciel n'est « *apte à juger du contenu d'un site* ». Un programme informatique n'a pas d'intelligence propre. Il n'agit que selon les ordres de son programmateur. Lorsque l'on voit la peine que peut avoir un juge à déterminer ce qui est conforme aux mœurs en matière de pornographie, lorsque l'on voit les nécessaires intervention de spécialistes et utilisation de bases de données pour régler certaines questions de propriété intellectuelle, on se doute bien de l'incapacité d'un logiciel à juger de l'illicéité d'un site. Sans parler du manque de légitimité démocratique d'une telle appréciation. Ainsi, tous les sites contenant un mot de la liste noire, y compris des sites licites, seront exclus de l'indexation et vice et versa. Si le gérant du moteur souhaitait éviter d'indexer des sites à caractère pornographique, il mettrait par exemple sur sa liste noire le mot « sein ». Le filtrage basé sur la liste noire entraverait alors les recherches des personnes intéressées par les derniers développements en matière de traitement du cancer du sein, à cause de la simple connotation sexuelle du substantif en

376 C'est sans compter la responsabilité pénale pour violation de l'art. 292 du CPS.
377 Thibault VERBIEST et Etienne WÉRY, Responsabilité, p. 170.
378 Cf. Partie 3 E. 2.3.2 p. 70.
379 Valérie SÉDALLIAN, Outils.
380 Comme nous l'apprend, dans un entretien électronique, le Professeur de l'Université de Neuchâtel Jacques SAVOY.
381 Valérie SÉDALLIAN, Outils.

question. On voit bien que la présence sur un site de mots appartenant à la liste noire n'est qu'un élément qui permet une certaine suspicion, mais elle n'amène sûrement pas la vérité.

Par ailleurs, si les propriétaires des sites litigieux apprennaient l'existence de la pratique de la liste noire, ils veilleraient à ne plus user de certains mots présumés suspects. Pour parer cette parade, la liste noire devrait être mise à jour continuellement au risque de couvrir un champ d'impact large, mais plus très efficient. Plus elle serait étendue, plus la proportion de sites légitimement écartés serait faible.
En outre, enlever des mots du système d'indexation ne permettrait pas directement de repérer des images ou des vidéos. L'URL de ces fichiers multimédia ne contient pas forcément de mots explicites. En tous les cas, il y a belle lurette que les propriétaires de pages *web* de pornographie enfantine n'y utilisent plus le mot « pédophilie ». Leur déficience est psychologique, pas intellectuelle.
On peut ajouter que la pratique de non-référencement des sites contenant des mots explicites n'aurait d'effets que dans un champ d'application restreint : elle ne servirait grosso modo qu'en matière de pornographie et de haine raciale.
On pourrait aisément rallonger la liste des limites de la liste noire. Cette technique simple de filtrage pourra à l'avenir être aisément améliorée, en peaufinant les instructions données au logiciel. Mais les malintentionnés trouveront toujours un subterfuge à de telles techniques, aidés involontairement par les fabricants de programmes de cryptographie. Mais nul besoin de surenchères technologiques pour tromper la vigilance des techniques de filtrage : de simples codes, à l'image du chiffrement de César, suffisent la plupart du temps.

Depuis le début des développements présents, on parle en terme de résultat : on se demande si les techniques de filtrage sont efficaces. On voit que non : un site illicite peut passer entre les mailles du filet et à l'inverse, un site licite peut ne pas être indexé pour contenir un mot placé sur la « liste noire ». Mais pour se départir de sa responsabilité, on peut penser que la simple mise en place d'un système de liste noire pourrait suffire. On parlerait alors en terme de moyens. L'absence d'efficacité totale technique n'empêche pas pour autant un tribunal d'exiger un certain comportement du prestataire. Il faut que le tribunal juge si le bien généré par la technique de filtrage est supérieur au mal provoqué, ou, autrement dit, si un tel système nuit dans une trop grande proportion à la liberté d'expression par rapport aux avantages qu'il procure dans la lutte contre les contenus illégaux. En fait, la question revient à se demander si, juridiquement, la mise en place d'un système de filtrage est acceptable.

La réponse est directement liée aux faiblesses actuelles des techniques de filtrage. Elle semble sauter aux yeux. On ne peut déjà envisager qu'avec peine l'éviction de mots qui se rapportent à des activités interdites : même les mots les plus explicites, ceux qui se éveillent des images d'horreur - révisionnisme, pédophilie - ne méritent pas telle sanction. Si certains mots peuvent éveiller des soupçons et méritent la plus grande vigilance, ils ne sont pas illicites en eux-mêmes. Aucun mot n'est illicite en soi. La non-acceptation de ces mots explicites commanderait par exemple la disparition des bases de données des moteurs de recherche des sites luttant contre la pédophilie ou le négationnisme. Alors quid de mots qui ne sont que plus ou moins liés à une certaine illicéité ? La non-acceptation de substantifs tels que ceux évoquant la nudité et la beauté abolirait notamment le référencement de certains sites s'intéressant à l'art ou à la médecine. Quelle devrait être la nature et le nombre de termes à bannir du moteur de recherche pour éviter de référencer les sites qui reproduiraient sans autorisation des photographies consacrées aux charmes féminins ? Cet exemple montre bien que vouloir exclure certains mots des bases de données des moteurs de recherche, au motif qu'ils peuvent être utilisés pour accéder à des sites illicites, ne serait pas compatible avec le

principe de la liberté d'expression[382]. « *L'universalité de l'accès à l'information que permet l'utilisation des moteurs de recherche doit être préservée* »[383].

En définitive, la non-acceptation de mots-clés est juridiquement très contestable, de part les faiblesses techniques actuelles d'une telle pratique. Si la technologie le permet un jour, l'obligation de filtrer les sites fera peut-être son apparition. Elle deviendrait alors partie intégrante du devoir de diligence demandé à l'exploitant de l'outil de localisation d'information.

Aujourd'hui, peu nombreux sont les moteurs de recherche qui offrent une possibilité de filtrage basée sur une liste noire. De plus, ils laissent toujours le choix à l'internaute du mode sans filtrage[384] : il ne faut pas oublier que les mots-clés les plus souvent entrés dans le champ de recherche du moteur touchent au sexe. Selon le site http://www.dicofr.com, les deux mots-clés les plus fréquemment soumis aux outils de recherche francophones lors de l'année 2000 sont « sexe » et « MP3 ». Inutile de dire que la recherche avec filtrage n'est pas au goût du jour.

3.2.3 L'absence de contrôle des sites indexés

Un moteur de recherche devrait-il vérifier le contenu des sites référencés avant que la base de données puisse être utilisée par les internautes ? Bien sûr que non. A l'instar des opérateurs d'hébergement et des fournisseurs d'accès, le nombre considérable des pages référencées interdit un contrôle minutieux de leur contenu. Un tel contrôle préventif amènerait également à tous les coups une entrave à la liberté d'expression, les doutes quand à l'illicéité d'un site devant logiquement entraîner une censure illégitime. Un moteur de recherche n'est pas censé opérer une indexation sélective, mais bien exhaustive : il n'est pas juge. Même si la directive sur le commerce électronique ne traite pas de la responsabilité des moteurs de recherche, son art. 15 instaure un principe fondamental dont les Etats membres ne peuvent s'écarter pour les outils de recherche. Il serait « *injustifié, voire discriminatoire, de traiter plus sévèrement les fournisseurs de moteur de recherche* »[385], dont on a dit qu'ils avaient une influence technique sur le contenu moindre que les hébergeurs.

En cas de soumission d'un site *web* de la part de la part de son propriétaire, un contrôle ne devrait pas non plus être exigé du moteur de recherche, et cela pour de multiples raisons. D'abord, le traitement de ces soumissions est automatisé : le moteur de recherche ne classant pas les sites selon des thèmes, mais uniquement selon des mots-clés, il n'examine pas le site en question. Ensuite, imposer une telle obligation amènerait simplement le moteur de recherche à supprimer cette possibilité d'indexation volontaire, qui ne lui est finalement que peu bénéfique. Finalement, les développements subséquents touchant au contrôle des sites référencés par les annuaires valent aussi ici[386].

---

382 Valérie SÉDALLIAN, Outils.
383 Valérie SÉDALLIAN, Outils.
384 Thibault VERBIEST, Références 1.
385 Thibault VERBIEST et Etienne WÉRY, Responsabilité, p. 171.
386 Cf. Partie 3 F. 4.2.3 p. 90.

3.2.4 Conclusions

Le fournisseur de moteur de recherche pourrait voir sa responsabilité engagée s'il a connaissance du site illicite référencé et qu'il ne déréférence pas ce site. Pour recevoir les notifications des lésés, il devra mettre en place une procédure d'alerte
Par contre, on ne peut exiger du moteur de recherche de refuser certains mots-clés, encore moins de contrôler les sites auxquels ils donnent accès, car l'important est de permettre au moteur de recherche d'« *assurer l'accès le plus universel possible aux différentes informations accessibles sur Internet* »[387].

On voit que les cas d'engagement de la responsabilité civile des moteurs de recherche existent, mais sont limités[388]. On remarque également que, si l'on est parti avec l'idée que la responsabilité du moteur de recherche ne devait pas forcément être traitée de façon identique à celle de l'hébergeur, force est de constater qu'un parallèle existe. Selon les circonstances, il faudrait néanmoins éventuellement être plus clément à l'égard du moteur de recherche, qui a une influence technique moindre sur le contenu illicite et qui n'a aucun contact avec le fournisseur de contenu.

Etudions encore deux cas particuliers de responsabilité liés aux moteurs de recherche.

3.2.5 Le cas Google

Google est, à notre connaissance, le seul moteur de recherche à proposer une version « En cache » des sites indexés. Cette version montre le site tel qu'il était lors du passage du robot. Cette pratique a l'avantage d'accélérer la connexion au site de l'internaute et d'éviter les erreurs 404[389]. « Googlebot », le *crawler* de Google, visite le *web* environ tous les mois. Il est évident que les sites subissent quelques modifications entre-temps. C'est pourquoi Google permet également la consultation du site actuel, comme un moteur de recherche traditionnel.
Lorsque l'on clique sur la version « En cache », Google précise qu'il « *n'est ni affilié aux auteurs de cette page ni responsable de son contenu* ». Cette phrase n'exclut évidemment en rien sa responsabilité pour les contenus illicites dont il permet l'accès.

Imaginons que le robot indexe une page *web* au moment où celle-ci contient une information illicite. Quelques heures après le passage de « Googlebot », le propriétaire du site supprime l'information litigieuse. Or, désormais stockée sur le serveur cache de Google, la page et son information illicite sont accessibles pendant environ un mois par l'entremise de ce moteur de recherche. Qui doit-on tenir pour responsable ? Le propriétaire du site est le premier responsable, même si sa faute est légère. Mais qu'en est-il de Google ?
Sa situation est assez ambiguë. Le *caching* que Google pratique n'est en tout cas pas un hébergement au sens de l'art. 14, car il ne stocke pas les informations à la demande d'un destinataire de services : il le stocke pour lui-même, pour améliorer ses performances et ainsi attirer des internautes. En sus, ce *caching* n'est, à notre avis, pas celui décrit dans l'art. 13 de la directive sur le commerce électronique, parce qu'on ne peut pas le décrire comme temporaire. Le terme « temporaire » est certes indéfini, mais il devrait plutôt viser des stockages de quelques jours et non de plusieurs semaines.

---

[387] Valérie SÉDALLIAN, Outils.
[388] Vanina SPACENSKY, Promotion ; Valérie SÉDALLIAN, Outils.
[389] Ces erreurs dénoncent l'impossibilité de localiser le site à cause de sa disparition entre l'indexation et le moment de la recherche de l'internaute

Google est au minimum responsable dans la même mesure qu'un prestataire d'hébergement : il devra donc supprimer de son serveur les informations dont il sait qu'elles sont illicites. Mais on pourrait presque se demander si Google ne devrait pas faire preuve d'une plus grande diligence afin d'éviter toute responsabilité, de part le fait qu'il pratique seul ce type de *caching*, qui génère un risque de plus dans la survenance et l'augmentation d'un dommage. On en reviendrait presque à la décision de la Cour d'appel dans l'affaire Estelle Hallyday : Google devrait-il assumer les conséquences d'une activité qu'il a délibérément décidé d'exercer, à l'inverse des autres prestataires de sa branche ? La question reste en suspens, mais n'oublions pas que le développement d'Internet reste un critère important dans la détermination de la réponse à chaque problème que pose ce médium.

3.2.6 Les méta-moteurs de recherche

Les méta-moteurs de recherche, ou métachercheurs, sont des « *serveurs qui passent des requêtes à plusieurs moteurs de recherche et/ou répertoires et résume les résultats* »[390]. Regroupant le travail de dizaines d'outils de recherche, ils sont très efficaces[391].
Etant donné qu'ils s'approprient - certes légitimement - le travail d'autres outils de recherche, les métachercheurs doivent assumer, vis-à-vis des tiers, la même responsabilité que ces outils de recherche.

4. Les annuaires (*human-powered directories*)

4.1 Notions

Les annuaires, ou répertoires, sont des listes de sites *web*, classés par thèmes et sous-thèmes[392]. On y retrouve donc une classification hiérarchique. Tout propriétaire de site qui souhaite voir son bébé dans les listes d'un répertoire doit l'inscrire par le biais d'un formulaire. Il donne le titre de son site, son adresse URL et une brève description de son contenu, choisit les mots clés attribués au site, voire aussi la catégorie dans laquelle il figurera dans le répertoire. Les spécialistes de l'annuaire vérifient, au moins succinctement, la correspondance des données fournies par le propriétaire du site avec la réalité et jugent de l'intérêt, voire de la qualité du site. Ils examinent en particulier si le choix de la catégorie est judicieux. « *L'annuaire, en tant qu'éditeur, a la possibilité de modifier parfois ces choix* »[393]. Plus précisément, chez Nomade, les vérifications sont effectuées avant la mise en ligne : l'annuaire se réserve ainsi le droit de refuser certaines soumissions, notamment si le contenu du site est illicite. En revanche, chez Yahoo!, il semblerait que les sites soient évalués par les internautes eux-mêmes[394] : le site est donc accessible avant vérification.

On voit qu'il n'est ici pas question d'indexation automatique. Le référencement nécessite la démarche volontaire d'une personne physique et un traitement « manuel » par l'équipe de l'annuaire.

---

390 Telle est la définition donnée par le site http://www.dicofr.com.
391 Debriefing (www.debriefing.com) est un bon exemple de métachercheur.
392 C'est pourquoi Yahoo! France se définit comme un guide thématique.
393 Murielle CAHEN, Moteurs.
394 « *Les surfeurs de Yahoo! France explorent les sites suggérés et, si les critères de sélection sont remplis* [dont la conformité avec la loi]*, décident des catégories où ces sites apparaîtront* ».

4.2 La responsabilité pour le contenu illicite des sites référencés

4.2.1 Le refus de désindexer un site illicite en connaissance de cause

Ce qui a été dit pour les moteurs de recherche vaut pour les annuaires[395]. Il faut donc exiger de l'annuaire la mise en place d'une procédure d'alerte et le déréférencement du site en question, s'il connaît son caractère illicite.

4.2.2 La création de rubriques explicites

Un annuaire pourrait-il être tenu responsable pour avoir créé des rubriques dont on se doute qu'elles contiennent des sites au contenu illicite ? Pour répondre à cette question, prenons trois exemples de rubriques explicites.

Si tous les annuaires possèdent une catégorie « MP3 », on peut remarquer qu'il est difficile d'y trouver des sites contenant des fichiers musicaux illégaux. On y découvre surtout des sites proposant à des artistes de se faire découvrir en leur laissant un de leurs titres, mais pas de copies compressées en MP3 de musique protégée. Les annuaires ont l'air de prêter une attention toute particulière à ce problème. On a pu remarquer avec l'affaire Napster que les *majors* n'hésitaient pas à attaquer en justice ceux qui leur font perdre un peu de leur profit.
Nombreux sont les répertoires qui proposent une sous-rubrique offrant des photographies de célébrités dénudées, souvent cachée dans des rubriques curieuses. Ainsi, chez Yahoo! France, on en trouve une dans l'arborescence « Commerce et économie > Produits et services pour les particuliers » ! Yahoo! France doit se douter que sous une telle rubrique se cachent des contenus illicites, notamment des photos violant le droit à l'image des stars représentées en tenue d'Eve. Mais tous les sites y référencés ne sont pas illicites. Comme le remarque Valérie SÉDALLIAN, ce n'est pas parce qu'une célébrité est nue sur une photo distribuée sur le site de quelqu'un qu'elle ne connaît pas, que l'on se trouve en face d'une situation illicite : par exemple, « *en droit américain, les cessions de droits sur des clichés peuvent être totales et illimitées* »[396]. Les photos de telle star pour tel magazine peuvent le cas échéant être réutilisées par quiconque.
Permettez-nous de prendre un troisième exemple, comment dirons-nous, plus osé : Yahoo! France propose une rubrique « Scatologie et ondinisme ». Inutile de vous décrire les sites y proposés. Un système d'inscription freine quelque peu l'accès aux sites, mais ne l'empêche en rien : même un gosse de 8 ans n'aurait aucune difficulté à accéder aux contenus d'horreur que l'on peut trouver sur ces sites. La responsabilité pénale de Yahoo! France ne fait ici aucun doute : la création de cette rubrique constitue une faute. Yahoo! France pourrait faire l'objet d'une poursuite en Suisse sur la base de l'art. 197 al. 3 du CPS.

Juridiquement, éviter de proposer des rubriques explicites permettrait aux annuaires d'être plus sereins. Economiquement, un annuaire ne peut se passer des sujets qui intéressent le plus notre vile société. L'annuaire n'hésitera pas trop longtemps. D'autant plus qu'on conviendra qu'en matière civile, la création de rubriques explicites ne constituera en général pas la faute nécessaire à la responsabilité de l'annuaire. Il faut plutôt se référer au contenu des sites proposés dans telle ou telle thématique[397]. Cela nous amène au contrôle du contenu par l'annuaire.

---

[395] Cf. Partie 3 F. 3.2.1 p. 84.
[396] Valérie SÉDALLIAN, Outils.
[397] Dans ce sens, Valérie SÉDALLIAN, Outils.

4.2.3 L'absence de contrôle des sites indexés

On a vu plus haut que l'annuaire opère un contrôle, plus ou moins rigoureux, lors de la soumission du site par son propriétaire : la visite du site vise surtout à vérifier si son catalogage est correct.
L'annuaire a donc une certaine connaissance du contenu du site. En ce sens, certains auteurs affirment que les annuaires doivent assumer une responsabilité éditoriale[398]. Cette façon de voir a plusieurs défauts. Elle oublie notamment qu'à la différence du responsable d'un journal, le volume des informations est considérable. De plus, si le contrôle d'un éditeur de journal tend en grande partie à empêcher des cas de diffamation et d'autres atteintes aux droits de la personnalité, le responsable d'un annuaire devrait faire face à des questions complexes, en particulier de propriété intellectuelle : la difficulté récurrente de détermination de l'illicéité des informations est indubitablement plus présente pour l'annuaire. Or, l'annuaire, comme tout autre prestataire, n'est pas juge. Même un examen minutieux du site ne permettrait pas toujours de séparer le licite de l'illicite. Et il n'empêcherait pas un site qui ne contenait initialement rien de suspicieux d'atteindre par la suite les droits d'autrui. A chaque instant, les informations peuvent en effet être modifiées à l'insu de l'annuaire : le contenu d'un site *web* n'est pas fixé comme celui d'un magazine. Faudrait-il alors imposer une obligation de contrôle permanente ? Evidemment que non. Le DMCA le dit clairement et l'art. 15 de la directive sur le commerce électronique s'appliquerait aux annuaires, si la directive traitait de leur responsabilité.

Ces arguments nous font dire que la responsabilité éditoriale n'est pas appropriée à la situation de l'annuaire[399]. A notre avis, s'il ne veut pas voir sa responsabilité engagée, le répertoire doit, entre la soumission du site par son propriétaire et sa mise en ligne, procéder à un contrôle grossier du contenu du site. Concernant l'hébergeur, nous ne préconisions finalement pas la mise à sa charge d'un quelconque contrôle[400]. Notre opinion ici divergente tient au fait que l'annuaire a pour fonction de proposer des sites à information ciblée : il a un contact assez étroit avec l'information. Si un prestataire d'hébergement décidait de ne stocker que des sites au contenu informationnel similaire, il aurait un lien resserré avec l'information, car il aurait contrôlé, au moins brièvement, ces sites. Dans ce cas, il pourrait le cas échéant se faire reprocher de ne pas avoir détecté des contenus manifestement illicites.

Précisons encore un peu notre pensée. Imaginons qu'un juge traite d'un cas où un site référencé contenait des informations manifestement illicite. Le juge ne pourra pas admettre la responsabilité de l'annuaire sans autre, car le contenu litigieux peut avoir été introduit sur le site après que l'annuaire ait procédé au contrôle grossier. Mais il est une chose que le juge n'ignorera pas : un site ne change pas de but. Le propriétaire d'un site a toujours un objectif, que ce soit partager ses photos de famille avec le monde ou faire de la vente de livres. Si le but du propriétaire de site est de gagner un peu d'argent avec des bannières publicitaires en attirant des « surfeurs » grâce aux proposant des MP3 illicites qu'il met gracieusement à disposition, il ne proposera pas le temps du référencement des recettes de cuisine, sinon l'annuaire le classera dans la catégorie « Cuisine » et le site perdra toute clientèle.

---

[398] Thibault VERBIEST, Références 1, p. 21 ; Thibault VERBIEST et Etienne WÉRY, Responsabilité, p. 171 ; Murielle CAHEN, Moteurs.

[399] En ce sens, Valérie SÉDALLIAN (Outils) dit que « *le fait que les annuaires procèdent à une indexation manuelle des sites référencés et, donc, aient l'occasion d'en vérifier le contenu, ne devrait pas en soi être considéré comme un indice suffisant pour voir engager automatiquement leur responsabilité, en l'absence d'une faute caractérisée* ».

[400] Cf. Partie 3 E. 2.3.1 p. 67.

Lors du contrôle grossier, l'annuaire doit donc « sentir » le but du site : sa vérification doit permettre de jauger si la raison d'être principale du site en question est la fourniture de contenus illicites[401]. Ainsi, si le but du site est manifestement de fournir des contenus illicites, le répertoire ne devra pas le référencer, sous peine de prendre le risque de voir sa responsabilité être engagée. Si l'annuaire a un gros doute, il aura tout intérêt à ne pas le référencer, à plus forte raison que le juge pourrait « sentir » différemment le but du site.

Nous avons parlé de contrôle « grossier ». On pourrait se demander, lorsque le propriétaire du site propose de le classer dans une catégorie dite explicite, si l'attention de l'annuaire ne devrait pas être supérieure, voire si l'intermédiaire ne devrait procéder à quelques vérifications de temps en temps.

Finalement, remarquons que, selon nous, il ne faudrait pas exiger d'un « petit » annuaire un contrôle plus détaillé qu'à un « grand ». Ce qui a été dit à ce sujet de l'hébergeur vaut aussi ici[402] : plus l'annuaire est petit, plus ses moyens de contrôle sont minces. Mais tant qu'il n'y aura pas de réglementation spécifique, le risque existera toujours de voir un annuaire régional être traité plus sévèrement qu'un annuaire régional.

4.2.4 Conclusions

L'indexation humaine à laquelle procèdent les répertoires ne devrait pas amener à admettre trop facilement la responsabilité de ces prestataires. A l'inverse, il faudrait quelque peu s'éloigner de la législation américaine sur le droit d'auteur, un peu trop libérale à notre goût, vis-à-vis des annuaires. Contrairement à l'avis de Vanina SPACENSKY[403], nous pensons qu'il ne faut pas assimiler moteurs de recherche et annuaires dans la détermination de leur responsabilité : à fonctionnement différent, régime de responsabilité différent, dirons-nous.
Au final, l'annuaire doit déréférencer le site qu'il sait illicite. Il doit également procéder à un contrôle grossier des sites qu'il référence, afin de déterminer la « direction » licite ou illicite du site et de choisir l'attitude adéquate pour éviter au mieux les atteintes aux droits des tiers. Par contre, même s'il risque de s'attirer les foudres des procureurs, libre à lui de créer des rubriques explicites en matière civile.

---

401 On pense par exemple aux sites proposant des photos de célébrités. On a pu constater que le droit français est très protecteur en la matière. On pariera toutefois que les annuaires prendront le risque de ne pas abandonner la branche. Faut-il rappeler que le sexe est le principal gagne-pain des annuaires ? Le jeu en vaut la chandelle. En tout cas, tant que les vedettes de l'Hexagone ne partiront pas en croisade sur Internet. Et s'il est entré dans les mœurs - des stars - d'attaquer régulièrement les journaux people, il est évident que ce *modus vivendi* parviendra un jour sur le net, sans que les célébrités en question ne doivent essuyer une pluie de critiques outrageuses de la part de la cybercommunauté, à l'image de ce qu'elle a fait subir à Estelle Hallyday.

402 Cf. Partie 3 E. 2.3.1 p. 67.

403 Vanina SPACENSKY, Promotion.

G. Le fournisseur de lien hypertexte

1. La notion de lien hypertexte ou d'hyperlien (*hyperlink*)

1.1 Notions générales

D'un point de vue technique, le lien hypertexte est « *l'indication interactive de la coordonnée d'une page web, d'une image, d'un endroit spécifique à l'intérieur d'une page web ou de tout autre document numérisé* »[404]. Autrement dit, l'hyperlien, ou plus simplement le lien, est un code HTML[405] qui indique au navigateur[406] la coordonnée, soit l'URL de la cible.

Dans le sens habituel du terme, le lien hypertexte est la représentation visuelle du code HTML en question, cette représentation prenant la forme d'un texte - un ou plusieurs mots - ou d'une image. On parle alors aussi de « pointeur ». Grâce à cet élément « perceptible », l'internaute sait où il doit cliquer pour poursuivre sa quête d'informations.
A noter qu'il existe des liens qui ne nécessitent aucun clic de souris pour jouer leur rôle de renvoi. On parle alors de liens automatiques[407].

Les liens hypertextes constituent l'essence et l'arborescence du *World Wide Web* et sont la principale clé du prodigieux succès d'Internet. Ils offrent à l'internaute une information mondiale et interdisciplinaire et permettent à la toile de se tisser. Sans les hyperliens, les moteurs de recherche n'existeraient pas et les annuaires d'adresses URL seraient le seul moyen de trouver son bonheur sur le *web*.

1.2 Les différents types de liens hypertextes

1.2.1 Le lien hypertexte simple ou lien en surface (*link* ou *surface link*)

Un lien hypertexte simple est un « *lien vers la page d'accueil d'un site web* »[408]. Une fois ce lien cliqué et la page chargée, le site sur lequel naviguait l'internaute n'apparaît plus à l'écran.

1.2.2 Le lien hypertexte profond ou en profondeur (*deep link*)

Le lien hypertexte profond pointe à l'intérieur d'un site *web*, sur une page secondaire, contournant ainsi sa page d'accueil (*homepage*). L'exemple-type est le lien qui pointe sur un article reproduit sur un autre site. A l'inverse des prochains types de liens, celui-ci ne crée - en principe - pas l'illusion de rester sur le même site : le fournisseur du lien en question ne s'approprie pas le contenu cible[409].

---

404 Définition de la CIPertexte, site conçu par François-Xavier FARASSE et Eric LABBÉ, disponible à l'adresse http://www.lexum.umontreal.ca/cipertexte.

405 L'acronyme HTML désigne l'expression HyperText Markup Language. Il désigne le langage de présentation des documents sur le *web* ou, autrement dit, le langage de programmation avec lequel on écrit des pages *web*.

406 Appelé en anglais *web browser* ou *browser*, le navigateur est le logiciel permettant de consulter les informations qui se trouvent sur les pages du *World Wide Web*. Comme exemples, on peut citer les très connus Internet Explorer et Netscape.

407 Cf. Partie 3 G. 1.2.4 p. 94.

408 Définition de la CIPertexte, disponible à l'adresse http://www.lexum.umontreal.ca/cipertexte.

409 Le contenu « cible » ou « pointé » est le contenu auquel renvoie un hyperlien.

Remarquons seulement un grand problème que pose le lien en profondeur, sans toutefois en amener la solution. Beaucoup de sites *web* vivotent grâce aux bannières (*banners*) publicitaires, généralement placées sur la page d'accueil. Le prix d'une bannière est en principe calculé selon le nombre de visites de la *homepage*, la fréquentation de l'ensemble des pages *web* du site ou le nombre de clics sur la bannière. Si un internaute arrive directement dans une page profonde, les chiffres diminuent et le propriétaire du site supporte un manque à gagner. Ce dernier n'aura pas la tâche facile pour obtenir un dédommagement et/ou la cessation de la pratique litigieuse.

1.2.3 Le cadrage (*framing*)

Le cadrage n'est pas un lien proprement dit[410]. Il s'agit d'un code HTML qui permet au *webmaster* de scinder un site *web* en plusieurs fenêtres ou cadres (*frames*). Chacun de ses cadres constitue une page *web* indépendante, un document HTML autonome. Lorsqu'un site est divisé en deux *frames*, une *frame* contient le nom du site et son plan, constitué de rubriques, et entoure une autre *frame* montrant le contenu de la rubrique choisie. Le visiteur d'un site cadré ne quitte donc pas la fenêtre d'origine du lien hypertexte et l'URL indiquée dans la barre du *browser* ne change pas.
Le plus couramment, le cadrage est employé pour proposer les pages d'un même site, mais il permet aussi « *d'afficher n'importe quel document disponible sur la toile dans l'une des fenêtres de sa page personnelle* »[411]. Il permet ainsi au propriétaire du site cadré d'offrir le travail ou l'œuvre d'un autre propriétaire de site. Dans ce dernier cas, l'internaute ne sait souvent pas qu'il visite un autre site, étant donné que l'adresse indiquée dans son navigateur n'a pas changé[412]. Il peut croire toujours consulter un site suisse, alors qu'il lit les informations d'un site québécois.
Le cadrage pose surtout des questions de droit d'auteur et de concurrence déloyale que nous n'étudierons pas dans ce mémoire. De telles questions juridiques, autant palpitantes soient-elles, ne devraient à l'avenir n'avoir que peu d'importance pratique de part l'existence d'une parade technique. Le propriétaire d'un document qui souhaite ne pas être « spolié » par l'entremise de la technique du cadrage peut en effet insérer dans le corps du document en question un *javascript*[413] de quelques lignes qui empêchera tout cadrage : le document s'affichera toujours dans la totalité de la fenêtre du navigateur de l'internaute[414]. Cet exemple de remède technique nous montre qu'il est souvent plus sûr et rapide de se défendre techniquement que juridiquement.

1.2.4 Le lien automatique ou intégré (*inline link* ou *embedded link*)

L'image que l'on peut trouver sur une page *web* a une adresse différente de celle de la page *web*. Le lien automatique utilise cette caractéristique technique en permettant d'inclure dans une page *web* une image provenant d'une autre page *web*, notamment d'un site étranger, sans la reproduire sur son propre site. Ce procédé s'appelle l'insertion par lien hypertexte. Une

---

410 Alain STROWEL et Nicolas IDE (Hyperliens) parlent pourtant de lien cadre ou d'hyperlien de cadrage.
411 Lionel THOUMYRE, Liens hors-la-loi, Juriscom.net, septembre 1998.
412 Contra : Alain STROWEL et Nicolas IDE, Hyperliens : « *L'internaute, s'il se rend habituellement compte du fait qu'il consulte le contenu d'un autre site…* ».
413 Selon le site http://www.dicofr.com, le *javascript* est un « langage de développement assez proche de Java et utilisé dans la conception de pages *web* ».
414 Murielle Cahen (Les Liens hypertextes, http://www.murielle-cahen.com, janvier 2001) nous donne ce script :
<BODY onLoad="if (self != top) top.location = self.location">
<BODY TEXT="#000000" BGCOLOR="#FFFFFF" onLoad="if (self != top) top.location = self.location">.

telle technique peut même être utilisée pour faire jouer une musique en temps réel sans la dupliquer.
Cet hyperlien est assez perfide, car il permet à un propriétaire de « s'approprier » les bases de données d'autrui. Pour le visiteur du site, la manipulation est la plupart du temps invisible : ce n'est pas l'internaute qui active le lien, mais le navigateur. Le seul point de repère est l'affichage de l'URL de l'image au bas du navigateur lorsque la souris passe sur cette image. Mais cette trace est peu apparente, si elle existe, ce qui loin d'être toujours le cas. L'internaute ne peut en tout cas pas se fier à l'adresse indiquée dans la barre de navigation de son *browser*, qui reste la même.

2. La responsabilité du fournisseur du lien hypertexte pour le contenu illicite du site cible

La question est de savoir si le fournisseur d'un lien hypertexte peut voir sa responsabilité engagée en cas de renvoi à un site contenant des informations illicites, par exemple des déclarations diffamatoires. La réponse est délicate, d'autant plus que les solutions jurisprudentielles vues ici et là sont souvent contradictoires[415]. Elle va dépendre du type de lien hypertexte utilisé et devra être donnée au cas par cas en application de l'art. 41 du CO : les circonstances particulières du cas d'espèce seront décisives[416]. Il paraît par exemple improbable qu'un site luttant contre la haine raciale soit jugé responsable pour avoir fourni des liens vers des sites contenant des idées racistes[417], afin de montrer leur stupidité. En ce sens, il faut peut-être se rapprocher de la notion de complicité en droit pénal : pour qu'il y ait faute du fournisseur de lien, celui-ci doit participer consciemment à l'activité illicite en question. Mais n'enterrons pas tout de suite la responsabilité pour négligence.

Il faut remarquer qu'à la différence de ce qu'on a dit du fournisseur d'hébergement, l'action contre le créateur de lien ne permet pas de voir disparaître le contenu illicite. Il y aura toujours d'autres chemins menant à l'information illicite, notamment celui qui consiste simplement à introduire l'URL du site *web* litigieux. « *En s'attaquant au fournisseur de lien, on frappe donc en quelque sorte à la mauvaise porte* »[418].

Avant d'attaquer le plat de résistance, tordons le coup à une fausse idée. Pour plusieurs auteurs[419], un hyperlien serait assimilable à une citation bibliographique ou à une simple note de bas de page. Or, l'auteur d'une référence bibliographique ne peut généralement pas voir sa responsabilité engagée pour le contenu de l'ouvrage cité. Une telle opinion entraînerait l'absence de toute responsabilité pour le fournisseur de lien. Dans l'affaire Ticketmaster Corp. v. Tickets.com[420], la Federal District Court de Los Angeles est allée dans ce sens.

---

[415] Pour exemple, deux tribunaux américains ont dû statuer sur un cas similaire, soit sur la responsabilité du fournisseur d'un hyperlien qui guidait vers le code source permettant de décrypter le système de protection des DVD, code protégé et censé resté secret. Le 20 janvier 2000, la Cour supérieure de Californie déclarait irresponsable le défendeur, alors que le 17 août 2000, la Cour du district sud de New-York décidait d'interdire le lien en question.

[416] Comme le relèvent Ursula WIDMER et Konrad BÄHLER, Rechtsfragen beim Electronic Commerce, Sichere Geschäftstransaktionen im Internet, 2e éd., Zürich 2000, p. 368.

[417] Carole ABOUT, Responsabilité.

[418] Alain STROWEL et Nicolas IDE, Hyperliens.

[419] Par exemple, Pierre Mondie, Message de la liste droit-net, 26 mai 1998 16:43 : « *Il est donc généralement défendable d'assimiler un hyperlien à une référence bibliographique…* ».

[420] US District Court, Central District of California, 27 March 2000, Ticketmaster Corp. v. Tickets.com Inc., disponible à l'adresse www.gigalaw.com/library/ticketmaster-tickets-2000-03-27.html.

Une telle façon de penser nous paraît indéfendable, car ce serait oublier que la fonction d'un hyperlien dépasse largement celle d'une référence bibliographique, en offrant un accès direct et immédiat à l'information illicite[421]. La responsabilité du fournisseur de lien doit pouvoir le cas échéant être engagée.

Dans nos développements, nous distinguerons entre liens visibles et liens invisibles. Mais avant, examinons brièvement la jurisprudence et la législation applicables à la question.

2.1 La jurisprudence

2.1.1 L'affaire IFPI v. Beckers[422]

Sur action de la Fédération internationale de l'industrie phonographique (IFPI), le tribunal de première instance d'Anvers a condamné, le 21 décembre 1999, un étudiant à la fermeture de son site pour avoir fourni quelques 25'000 liens vers des sites donnant accès à des reproductions d'enregistrements musicaux illégales, car sans autorisation des ayants droit. L'étudiant a opposé son droit fondamental à la liberté d'expression, mais le juge a estimé que l'établissement d'un lien ne représente pas une opinion et que la liberté d'expression ne permet pas de commettre un délit.
Pour condamner le propriétaire du site, le tribunal a utilisé comme fondement l'article 1382 du Code civil belge[423] et a jugé « *qu' un hyperlien n'est pas simplement une note de bas de page. En activant un lien de cette nature, un accès est donné à un site. Pour obtenir un accès à un site, il doit être possible de le localiser et de l'activer. Créer un hyperlien a précisément pour but de fournir ce service à l'utilisateur potentiel. En l'espèce, le défendeur a, sciemment et en pleine connaissance de cause, établi des liens vers des sites qui permettent de télécharger de manière illicite de la musique* »[424]. Le nombre considérable de liens et le fait que le site ait été réouvert sous d'autres adresses après sa fermeture consécutive aux avertissements de l'IFPI démontre l'intention « détestable » de l'étudiant belge.

Ce n'était pas le premier coup d'essai de l'IFPI. Elle s'était déjà fait la main - il est vrai sans succès - dans le premier cas de ce genre en Europe. Il s'agissait d'une affaire l'opposant à un étudiant suédois de 17 ans, qui fut menotté et placé en détention préventive pour des agissements similaires à ceux de l'étudiant belge[425].
Au début de l'ère MP3, l'IFPI souhaitait faire un précédent. Elle se contente aujourd'hui de mettre en garde les contrefacteurs sans utiliser la justice : même lorsqu'elle gagnait, elle ne récupérait généralement pas les frais de procédure.

2.1.2 L'affaire Steinhöfel c. Best[426]

En Allemagne, Joachim Steinhöfel reprochait à Michael Best d'avoir placé sur son site une véritable compilation d'hyperliens débouchant sur des textes qui attentaient à l'honneur du demandeur. Après notification de Steinhöfel, le défendeur avait retiré les liens litigieux. Pour

---

421 Dans ce sens, Vanina SPACENSKY, Promotion.
422 Prés. Civ. Anvers (référé), 21 décembre 1999, IFPI Belgium c. Werner Guido Beckers, non publié, R.G., n° 99/23830.
423 Qui a le même contenu que l'art. 1382 du Code civil français. Cf. Partie 2 B. 1 p. 22.
424 Traduction du flamand de Thibault Verbiest et Etienne WÉRY, Responsabilité, p. 171.
425 Gta, Cour d'appel, 27 décembre 1999 , IFPI c. T. Olsson, non-publié, nr. B 1009/99.
426 Landgericht Hamburg, 12 mai 1998, 312 O 85/98, disponible à l'adresse suivante : http://www.netlaw.de/urteile/lghh_6.htm, consultée le 20 avril 2000.

des questions d'argent, l'affaire se termina devant les tribunaux. Michael Best a mis en avant la liberté d'expression, mais on sait que celle-ci ne doit pas permettre de violer les droits d'autrui. Le Landgericht de Hambourg a choisi de privilégier l'intérêt de protection de la personnalité du demandeur. Il a en outre affirmé que Michael Best avait fait siens les textes diffamants : en choisissant de ne renvoyer qu'à des textes préjudiciables à Joachim Steinhöfel, le défendeur ne s'était pas suffisamment distancié de ces contenus. Le tribunal a par conséquent retenu la responsabilité civile de Michael Best et l'a condamné au paiement de 40'000 DM à titre de dommages et intérêts.

2.2 La législation

La législation examinée pour les outils de recherche est applicable aux liens hypertextes, mis à part ce qui touche la loi autrichienne de transposition. Nous nous rappellerons aussi aux bons souvenirs du *Teledienstgesetz*.

2.2.1 L'*E-Commerce-Gesetz* autrichien

La loi autrichienne de transposition prévoit une norme spécifique à la fourniture de liens hypertextes, qui reprend l'art. 14 de la directive sur le commerce électronique sur l'hébergeur. L'art. 17 du *E-Commerce-Gesetz* autrichien dit en effet (traduction libre) :

1. Le prestataire qui, au moyen d'un lien hypertexte, permet l'accès à des informations étrangères, n'est pas responsable de ces informations à condition que :

a) il 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) dès le moment où il a de telles connaissances, il agisse promptement pour supprimer le lien hypertexte.

2. Le paragraphe 1 ne s'applique pas lorsque la personne qui est à l'origine des informations, agit sous l'autorité ou le contrôle du prestataire, ou lorsque le prestataire fait siennes les informations étrangères.

2.2.2 Le *Teledienstgesetz*

On rappelle que la loi allemande de transposition de la directive sur le commerce électronique, l'*Elektronischer Geschäftsverkehr-Gesetz* (EGG), a modifié le *Teledienstgesetz* (TDG). Il faut néanmoins signaler que, sous l'empire de l'ancien *Teledienstgesetz*, la doctrine dominante allemande a élaboré une opinion, selon laquelle l'art. 5 du TDG s'appliquait à la problématique des liens[427]. Ces auteurs n'étaient toutefois pas unanimes quant aux alinéas applicables aux hyperliens. Une partie de la doctrine[428] considérait que l'art. 5 al. 3 du TDG[429] était applicable, car il fallait assimiler le fait de créer un lien à une sorte de fourniture d'accès à un contenu étranger. Mais cette façon de voir était très contestée, parce qu'elle procurait un

[427] Roman KELTNER, Haftung für Hyperlinks am Beispiel der ersten höchstgerichtlichen Entscheidung in Österreich, www.it-law.at, p. 5. Thomas STADLER (Links) pense aussi que le législateur allemand a voulu instaurer un privilège pour les « *linksetzer* ».

[428] Par exemple, Thomas STADLER, Links. Alain STROWEL et Nicolas IDE citent aussi Torsten BETTINGER et Stefan FREYTAG, Civil Law Responsibility for Links, IIC, 8/1999, 883-907.

[429] Pour rappel, l'art. 5 al. 3 du TDG a comme contenu : « *Diensteanbieter sind für fremde Inhalte, zu denen sie lediglich den Zugang zur Nutzung vermitteln, nicht verantwortlich* ».

privilège souvent injustifié[430]. Une autre partie de la doctrine souhaitait l'application de l'art. 5 al. 2 du TDG. Cette disposition visant quasi expressément l'hébergement, elle ne devrait pourtant pas s'appliquer à la problématique des liens. En fait, c'est l'alinéa premier de l'art. 5, inchangé mais désormais l'alinéa premier de l'art. 8, qui a été le plus souvent utilisé. La jurisprudence l'a notamment utilisé dans les cas où le fournisseur du lien faisait sien le contenu lié[431]. S'il s'identifie avec le contenu, s'il ne s'en distancie pas suffisamment, il le fait sien et doit donc logiquement en être responsable.
L'*Elektronischer Geschäftsverkehr-Gesetz* ne traitant pas de la responsabilité des fournisseurs de liens, les principes dégagés ci-dessus ont de bonnes chances de perdurer pendant quelques temps encore.

2.3 Le lien hypertexte simple et le lien hypertexte profond : les liens visibles

2.3.1 Les cas de responsabilité

Il faut examiner plusieurs comportements ou abstentions qui pourraient engager la responsabilité du fournisseur de lien.

i. Le refus de supprimer le lien en cas de notification

Il est clair que le propriétaire du site peut voir sa responsabilité engagée s'il refuse d'enlever le lien litigieux, sachant que le site auquel il renvoie est illicite. La problématique est similaire à celle des hébergeurs et des outils de recherche. Si la requête provient d'un tribunal, le fournisseur de lien ne doit pas hésiter un instant à supprimer le lien. Si la requête provient du lésé, ce dernier doit amener les éléments qui amèneront le fournisseur de lien à considérer que le contenu lié est manifestement illicite. En effet, s'il suffit au lésé d'indiquer que le contenu est manifestement illicite, on tombe dans le cas de responsabilité suivant.

Par rapport aux outils de recherche, il faut ajouter que la liberté d'expression est un peu moins en danger de part la possibilité de juger du fournisseur de lien, car l'hyperlien au centre du débat n'est qu'un chemin peu emprunté pour atteindre l'information en question. A l'inverse, les moteurs de recherche et les annuaires sont des passerelles très importantes dans l'accessibilité à l'information en général.

ii. Le *linking* en cas de connaissance

Parfois, la condition de la connaissance ne nécessite aucune notification pour être remplie. C'est ce que nous avons vu dans les deux cas de jurisprudence examinés ci-dessus[432] : la responsabilité du fournisseur de lien devait logiquement être engagée, car il ne pouvait nier avoir eu connaissance de l'illicéité du contenu. Il s'agissait là de cas d'école. D'une manière générale, on ne peut pas présumer de la connaissance du caractère illicite de l'information cible par le fournisseur de lien, au contraire de ce qu'a laissé entendre l'Oberste Gerichtshof in Österreich. Dans l'affaire Jobmonitor.com[433], la plus haute cour d'Autriche a en effet déclaré *« Durch das Setzen eines Links auf die Website B macht sich der Ersteller der Website*

[430] Stefan ERNST, Hyperlinks.
[431] Voir l'affaire Steinhöfel c. Best ci-dessus.
[432] Cf. Partie 3 G. 2.1 p. 96.
[433] OGH 4 Ob 274/00y.

A deren Inhalt zu eigen und haftet daher für deren Inhalt », et cela sans condition. Evidemment, la doctrine autrichienne a sévèrement critiqué cet avis[434].

En fait, pour savoir si le fournisseur de lien a connaissance du contenu illicite qu'il a lié, il faudrait raisonner avec la notion de but du site, que nous avons déjà utilisée au sujet de l'annuaire[435]. Si l'on ne peut présumer que le fournisseur de lien connaisse le caractère illicite de tout le contenu cible, on peut présumer qu'il connaisse, grosso modo, le but du site qu'il lie : il est en quelque sorte supposé avoir opéré un contrôle grossier du site cible. Si le but de ce site est manifestement de procurer des contenus illicite, sa responsabilité peut être engagée. Si le but illicite du site ne saute pas aux yeux, il faut considérer qu'il n'y a pas connaissance. Mais, si le fournisseur de lien a des doutes quant à l'illicéité du but poursuivi par le propriétaire du site lié, il prend un risque à maintenir le lien en question, considérant qu'un tribunal pourrait néanmoins décider que la condition de la connaissance était remplie. Le tribunal pourrait également considérer que le doute aurait dû amener l'intermédiaire à contrôler plus attentivement le site.
Ce même tribunal pourrait-il aussi reprocher au fournisseur de lien de n'avoir pas procédé à un contrôle régulier du site cible ?

iii. L'absence de contrôle périodique

Le contenu cible peut changer. Il peut être licite au moment de la création du lien, comme devenir illicite quelques instants plus tard. Le fournisseur peut-il être tenu responsable du contenu lié pour ne pas avoir contrôlé que ce contenu était toujours licite ?

Dans l'affaire Radikal[436], Madame Angela Marquardt a été poursuivie pour avoir établi un hyperlien vers la revue néerlandaise « Radikal », « *magazina non grata* » en Allemagne. Il est vrai que ce magazine avait publié un article expliquant comment saboter les rails de chemins de fer. Or, l'accusée avait créé le lien hypertexte deux mois avant que le magazine ne publie l'article en question. Elle n'avait donc pas connaissance du texte illicite lors de l'établissement du lien. La prévenue aurait-elle dû contrôler les contenus pointés par le lien fourni ? L'Amtsgericht de Tiergarten a estimé qu'il ne fallait pas imposer de vérification périodique aux fournisseurs de lien. L'obligation serait trop lourde. Madame Angela Marquardt a donc été relaxée.

A notre sens, il faudrait suivre l'approche dégagée dans cet arrêt. Nous avons pu voir précédemment qu'imposer des contrôles périodiques n'était pas très « à la mode ». Si on admettait l'obligation de contrôle périodique, il s'agirait évidemment d'un contrôle grossier, qui permettrait de déceler les grosses illicéités. Dans la grosse majorité des cas, ce genre d'agissements existent pourtant dès le début du site ou n'existent pas : il y aurait alors responsabilité pour un *linking* en cas de connaissance dans le sens vu ci-dessus. Il faudrait aussi résoudre un problème majeur : à quelle fréquence le fournisseur de lien devrait-il procéder à ce contrôle grossier ? Tant que ce point n'est pas fixé, imposer un contrôle, même grossier, amènerait le fournisseur de lien à procéder aux vérifications très fréquemment, puisqu'il pourrait difficilement prouver avoir fait un contrôle à telle ou telle date. Une telle charge ne peut être mise sur le dos des créateurs de sites.

---

434 Par exemple, Franz SCHMIDBAUER, Link ist nicht gleich Link, http://www.internet4jurists.at.
435 Cf. Partie 3 F. 4.2.3 p. 90.
436 AG Tiergarten, 30 juin 1997, MMR, 1998/1, p. 49.

En conclusion, nous convenons, à l'instar de Thibault VERBIEST et d'Etienne WÉRY, qu'en ce qui concerne le fournisseur de lien, il paraît « *difficile de retenir sa responsabilité s'il n'a aucune connaissance du caractère illicite du site lié* ». Mais, faut-il rappeler que tant que l'insécurité juridique règnera, un juge suisse pourrait avoir l'idée d'imposer un tel contrôle ?

2.3.2 La distinction entre liens directs et liens indirects

Jusqu'alors, nous parlions de liens directs. Or, il est nécessaire de distinguer ces liens des liens qui ne mènent qu'indirectement à l'information illicite[437], soit des liens qui renvoient à des sites, qui contiennent des liens, qui, eux-mêmes, renvoient à un contenu illicite. Les risques de responsabilité du fournisseur de lien indirect sont infimes[438]. Isabelle Larate va plus loin[439] : aucune responsabilité ne serait possible pour les liens indirects. L'auteur ne donne toutefois pas d'explication. Pour Alain STROWEL et Nicolas IDE, qui parlent de multiples hyperliens, « *l'élément de connaissance de l'existence du contenu illicite devient dans ce cas à ce point hasardeux, que* […] *il ne peut être question de responsabilité dans le chef du premier fournisseur de lien* »[440]. Les auteurs citent l'affaire américaine Bernstein v. Penney[441], où le juge a écarté la responsabilité du fournisseur du lien originel.

Il est évident que, plus la chaîne de liens nécessaires à la visualisation de l'information illicite est longue, moins la condition de la connaissance a de chances d'être réalisée. De plus, on ne peut demander au fournisseur du lien de vérifier où mènent les liens se trouvant sur le site pointé, sans compter les sites cibles des liens placés sur le troisième site, etc[442]. L'inverse serait absurde, les chaînes de liens étant innombrables et quasi infinies.

Au final, dans le cas d'un lien indirect, le fournisseur du lien originel ne verra que difficilement sa responsabilité engagée. A plus forte raison, qu'il sera très délicat, pour le lésé, d'amener une quelconque preuve.

2.4 Le *framing* et le lien automatique : les liens invisibles

Le fournisseur de lien est bien évidemment responsable des contenus montrés par les techniques du *framing* et du lien intégré, si ces contenus lui appartiennent. Mais l'usage de *frames* et d'*inline links* permet aussi au fournisseur de lien d'intégrer à son site la réalisation d'autrui. Cette opération est généralement transparente pour le cybernaute, si le fournisseur de lien n'indique pas que le contenu montré provient du site de telle ou telle personne. Cette confusion permet au fournisseur de lien de s'approprier le contenu. Il le « *ratifie* »[443]. On ne peut profiter du travail d'autrui sans assumer une certaine responsabilité. Le fournisseur de

---

437 FG Associés, Les incidences juridiques des liens hypertextes, Expertises, novembre 1998 et février 1999, disponible sur Droitweb.com ; Isabelle Larate, Les liens hypertextes, Intellex, 2000.

438 Carole ABOUT, Responsabilité, p. 29.

439 Isabelle LARATE, Les liens hypertextes, Intellex, 2000, p. 3.

440 Alain STROWEL et Nicolas IDE, Hyperliens, p. 34.

441 US District Court, Central District of California, 29 septembre 1998, Gary Bernstein v. JC Penney Inc., non publié.

442 Rolf H. WEBER, E-Commerce, p. 532 ; Vanina SPACENSKY, Promotion. Plus nuancé, Stefan Ernst (Hyperlinks) pense que l'on peut exiger une telle vérification si le document lié laisse prévoir des liens vers des pages au contenu illicite.

443 Alain STROWEL et Nicolas IDE, Hyperliens, p. 20.

lien répond logiquement de ce contenu, comme s'il était le sien[444]. En ce sens, il faut adhérer à la jurisprudence élaborée sur la base de l'art. 5 al. 1 du TDG, avant sa modification.

A l'inverse, s'il n'existe aucun doute quant à l'appartenance du contenu - par exemple parce que le contenu révèle intrinsèquement son appartenance -, le fournisseur de lien engage sa responsabilité de la même manière que s'il avait utilisé un lien visible[445]. Ainsi, s'il montre clairement que le contenu n'est pas le sien, mais que ce contenu est manifestement illicite, il en répondra.

2.5 Conclusions

Dans le cas d'un lien hypertexte direct visible, le fournisseur sera tenu responsable du contenu illicite, s'il refuse de supprimer le lien en cas de notification et s'il a créé le lien alors qu'il avait connaissance du caractère illicite du contenu cible. En cas de lien indirect, le fournisseur n'encourt que de très minces risques d'être tenu pour responsable. Dans le cas d'un lien invisible, le fournisseur de lien sera jugé responsable, s'il avalise le contenu.
On voit que la loi autrichienne de transposition de la directive sur le commerce électronique choisit la bonne voie, au contraire du DMCA.

Au final, on remarque que « liaisonner » n'est pas une activité aussi innocente que le citoyen lambda peut le croire. Pourtant, nous n'avons même pas cité les – très nombreux – problèmes en matière de propriété intellectuelle. A chaque créateur de site, même amateur, de prendre conscience qu'il ne peut pas faire n'importe quoi et, en particulier, qu'il risque gros à se lier avec des contenus qu'il sait illégaux.

Concluons par une question pratique.

2.6 Quid de l'URL non activable ?

Nous avons plus haut différencier le lien hypertexte de la note de bas de page, en ce sens qu'il permet l'accès direct et immédiat au contenu[446]. Une adresse *web* inactivable ne peut être définie comme un hyperlien[447]. Juridiquement doit-elle néanmoins être assimilée à un hyperlien, ou alors à une note de base de page ? A notre sens, le fournisseur d'une URL sur un site Internet doit assumer la même responsabilité que le fournisseur de lien. En effet, il suffit à l'internaute de copier l'adresse dans la barre de navigation pour accéder au contenu. L'accès est donc presque autant direct et immédiat qu'avec un hyperlien. Par contre, la question est plus délicate en ce qui concerne une adresse *web* placée, par exemple, sur un cd-rom ou dans un article. Pour Alain STROWEL et Nicolas Ide, « *le résultat est similaire* »[448]. Nous ne sommes pas autant catégorique. D'un côté, l'immédiateté du lien hypertexte a dans ce cas totalement disparu et l'adresse *web* a en ce sens une fonction proche de celle d'une note de bas de page. D'un autre côté, il est vrai qu'il suffit à toute personne d'allumer un ordinateur pour accéder au contenu en moins de deux minutes. La solution dépendra des circonstances et

---

444 Rolf H. WEBER, E-Commerce, p. 532. L'auteur se rapporte à Stefan M. FREYTAG, Haftung im Netz, Verantwortlichkeit für Urheber-, Marken- und Wettberwerbsrechtsverletzungen nach § 5 TDG und § 5 MDStV, München 1999, p. 232 et Ulrich LOEWENHEIM et Frank A. KOCH, Praxis des Online-Rechts, Weinheim 1998, p. 264.

445 Rolf H. WEBER, E-Commerce, p. 533.

446 Cf. Partie 3 G. 2 p. 95.

447 Comme le confirme le groupe de travail « Liens hypertextes - Forum des droits sur l'Internet », http://www.foruminternet.org.

448 Alain STROWEL et Nicolas IDE, Hyperliens, p. 7.

le juge devra « sentir » si le fournisseur de l'URL souhaitait favoriser la diffusion des informations illicites.

H. Les autres fournisseurs de services

La plupart des acteurs dont nous avons examiné la responsabilité étaient des fournisseurs de services. Mais comme le relève Bertil COTTIER, d'autres prestataires offrant des prestations à valeur ajoutée, qu'il appelle « relayeurs d'informations », sont à même d'influer sur le contenu de l'information, notamment en le sélectionnant ou en le mettant à jour[449]. L'auteur pense en particulier aux « *personnes qui gèrent les archives en ligne, qui monitorent des forums de discussion …* ».

1. L'*information broker* et la banque de données en ligne

1.1 Notions

L'*information broker*[450] collectionne, trie et prépare des données sur demande de ses clients. A cet effet, il utilise des banques de données en ligne ou d'autre sources d'informations. L'*information broker* peut être spécialisé dans un domaine : spécialiste de la propriété intellectuelle, il se chargera par exemple de la recherche de brevets. Mais, il est la plupart du temps « généraliste » et s'occupe de la recherche de publications et fichiers de tout genre.
Le service d'un *information broker*, même s'il est onéreux, permet un gain de temps considérable au client.

Les banques de données donnent, souvent contre paiement, accès à des textes, images, et vidéos. Elles ne produisent qu'une petite part des données. Elles constituent un chemin plus direct à l'information. C'est lorsque l'internaute ne sait pas à quelle banque de données s'adresser pour trouver le document recherché, qu'il se tourne vers l'*information broker*.

1.2 La responsabilité pour les contenus illicites fournis

Au contraire de l'*information broker*, la banque de données en ligne produit une petite partie des données qu'elle procure. Elle assume à ce titre une responsabilité en tant que fournisseur de contenu[451]. En revanche, l'*information broker* et la banque de données en ligne endossent une responsabilité éditoriale pour les contenus créés par d'autres personnes[452].
A l'inverse du domaine pénal[453], la responsabilité civile de l'éditeur n'est pas traitée, en tant que telle, par la législation suisse. Elle est par conséquent régie par les règles générales de responsabilité et notamment les art. 41ss du CO. En revanche, l'art. 55 du CO et l'art. 55 du CCS ne sont pas applicables dans les cas de l'*information broker* et de la banque de données.

---

449 Bertil COTTIER, Impact, p. 6.
450 Traduction française littérale : courtier en informations. Pour de plus amples informations sur cet acteur d'Internet, voir Dirk SCHMITZ, Die vertraglichen Pflichten und die Haftung der Informationsanbieter im Internet : nationale und internationale Haftungsgrundlagen, Stuttgart 2000, p. 110ss.
451 Cf. Partie 3 I. 2 p. 110.
452 Pour Rolf H. WEBER (Haftung, p. 546), il y a lieu de traiter un prestataire Internet comme un éditeur, dès qu'il utilise des procédés « mécaniques » pour traiter l'information.
453 Cf. l'art. 27 du CPS.

Le lésé doit donc prouver la faute de l'éditeur et faire jouer la solidarité de l'art. 50 du CO. L'éditeur participe, intentionnellement ou par négligence, à l'atteinte en rendant accessible au public l'information par sa diffusion. « *Le critère opérant n'est pas celui de la maîtrise ou non du contenu, mais de l'offre faite au public* »[454]. Il est clair que si le fournisseur de services a connaissance du caractère illicite de l'information, il a le droit et le devoir d'empêcher l'accession du public à l'information litigieuse[455]. Son inaction constitue une faute intentionnelle. Si l'on ne peut pas toujours exiger de l'*information broker* ou de la banque de données qu'ils aient une connaissance parfaite de l'information fournie, on doit néanmoins considérer qu'ils en ont a une certaine connaissance : « *les contenus offerts font l'objet d'un choix objectif* »[456], après tout. Il doit, en sa qualité de professionnel, vérifier la licéité des informations fournies[457]. Si cet examen est trop succinct et n'a pas permis à l'éditeur de déceler l'illicéité d'une information, il doit en subir les conséquences et répondra de sa négligence.

2. L'exploitant et le modérateur d'un groupe de discussion (*newsgroup*) ou d'un forum de discussion

2.1 Notions

Techniquement, il faut distinguer les groupes de discussion et les forums de discussion.

Les *newsgroups* sont des groupes de discussion thématiques, classés selon une structure hiérarchique, disponibles sur Usenet[458], système de discussion mondial et distribué[459]. Ils offrent un moyen de communication et d'échange d'informations remarquable, en permettant à leurs abonnés de lire et de publier des messages, notamment de poser des questions ou d'y répondre.
L'utilisateur doit s'abonner à un groupe de discussion en le choisissant parmi les milliers disponibles dans la liste du fournisseur de services. Pour pouvoir consulter les messages ou articles (« *postings* »), il « appelle » le groupe de discussion et le serveur de *news* (*news server*) Usenet lui délivre les messages stockés[460].
Le processus de diffusion d'un message se présente ainsi : le *posting*, touchant à un « *thread* »[461], est envoyé par son auteur sur le *news server* du fournisseur de services, soit généralement son fournisseur d'accès, qui le répand à travers Internet sur les *news servers* des autres fournisseurs de services. Même s'il est parfois destiné à une personne en particulier, par exemple un amateur de « *trash-talking* », le *posting* a une diffusion planétaire. Potentiellement, des centaines de millions de personnes risquent de vous narguer, si votre anglais laisse à désirer. Plus sérieusement, on imagine l'ampleur des dégâts causés par une campagne de dénigrement par le biais des *newsgroups*.
Il existe des groupes de discussion pour tous les goûts. Une petite partie des *newsgroups* sont modérés : avant d'être disponibles, les articles sont contrôlés par un modérateur qui choisira

---

454 G. VERCKEN, Responsabilité sur Internet, Rev. Nov'Art, no 21, octobre 1996 – janvier 1997, p. 34.
455 Pierre-Ami CHEVALIER, Les rapports éditeur-rédacteur et les tiers, in Aspects du droit des médias, tome I, Fribourg 1983, p. 194.
456 Frédérique OLIVIER et Eric BARBRY, Hébergement, p. 1087.
457 Cela est déduit de la jurisprudence française dégagée sur les agences de renseignement par le Conseil d'Etat français. Voir l'étude du Conseil d'Etat, Internet et les réseaux numériques, 2 juillet 1998, 4e partie, disponible à l'adresse suivante : http://www.internet.gouv.fr/francais/textesref/rapce98/sommaire.htm.
458 *User's Network*.
459 Arnaud DUFOUR, Internet, p. 64.
460 Charles PONCET, Intégration, p. 207.
461 Un *thread* est un fil de discussion, selon le site http://www.dicofr.com.

ou non de les diffuser. Une telle pratique permet de vérifier la conformité des messages avec les normes régissant le *newsgroup*. Elle permet surtout d'éviter les messages risquant de mettre le feu aux poudres ou les messages sans valeur ou sans rapport avec le thème, en particulier les *spams*[462] : en d'autres termes, le modérateur enlève le « bruit ». Les *newsgroups* modérés renferment en conséquence des messages de qualité supérieure, mais ces groupes sont très peu fréquentés[463], les utilisateurs n'aimant pas se sentir restreints dans leur liberté de parole.

Les forums de discussion ressemblent passablement aux *newsgroups*. Ils sont aussi organisés par thèmes et peuvent être modérés ou non. Mais ils ne sont pas liés au service Usenet, ce qui induit des différences dans la consultation et la diffusion des messages. La plupart du temps, on trouve les forums de discussion sur des sites *web* ou des *bulletin board services*[464]. De ce fait, se dégage une autre différence de taille entre les forums de discussion et les *newsgroups*. L'exploitant des premiers en est aussi le créateur[465], alors que l'exploitant des seconds ne le sera que dans des cas extrêmement rares : il ne fait que stocker sur son serveur les messages de *newsgroups* créés par on ne sait qui.

A ses origines, ces deux services permettaient surtout le partage du savoir scientifique. Aujourd'hui, ils servent trop souvent de défouloir.

Remarquons encore que ce qui sera dit pour les forums de discussion sera dans l'ensemble valable pour les contenus délivrés dans un « livre d'or ». Un livre d'or sur Internet a la même fonction que dans la vie réelle : il permet à quiconque de délivrer ses impressions, notamment en ce qui concerne le site qu'il visite.

2.2 La responsabilité pour le contenu illicite des *postings*

Si nous avons différencié techniquement les groupes de discussion et les forums de discussion, c'est qu'il y a lieu de dissocier nos réflexions sur les responsabilités délictuelles qui peuvent découler de tels services, même si des ressemblances sont présentes.

2.2.1 La jurisprudence

i. L'affaire Demon

La société Demon Internet Limited gère un serveur de *news* Usenet, qui permet d'accéder à un *newsgroup* qui contient un *posting* que Laurence Godfrey trouve obscène et diffamatoire à son égard. La victime notifie immédiatement Demon Internet en le priant de supprimer le message, mais ce dernier reste encore accessible dix jours. Le fournisseur d'accès n'ayant pas donné suite à se demande, Laurence Godfrey l'actionne en justice sur le fondement du *Defamation Act* de 1996. Dans son jugement du 26 mars 1999[466], la Queen's Bench Division of the High Court of Justice donne raison au demandeur. Certes, Demon Internet n'est ni

[462] On rappelle qu'un *spam* est un courrier électronique non sollicité, généralement à caractère commercial.

[463] Le groupe non modéré fr.rec.cinema.discussion compte régulièrement des centaines de messages disponibles. Le groupe modéré fr.rec.cinema.selection dénombre en général deux ou trois messages.

[464] Pour une définition, cf. Partie 3 H. 4.1. p. 108.

[465] A moins, bien évidemment, que l'exploitant commande la réalisation du forum à un spécialiste. Mais cela ne change que peu de choses quant à la réflexion juridique.

[466] Laurence Godfrey v. Demon Internet Ltd, 26 mars 1999, QBD, Case N° : 1998-G-N° 30, disponible à l'adresse suivante : http://www.cyber-rights.org/documents/godfrey_decision.htm.

l'*author*, ni l'*editor*, ni le *publisher* du message, mais la société n'a pas fait preuve d'un « *reasonable care* » vis-à-vis de la publication et se savait contribuer à l'acte de diffamation. Demon Internet avait la capacité technique de supprimer le *posting* litigieux : en tant qu'il choisit de stocker les messages, il peut aussi facilement les supprimer. Il n'a donc pas pu invoquer l'exception de « dissémination innocente » et fut condamné.

La décision rend donc responsable le fournisseur d'un groupe de discussion non modéré, s'il a connaissance d'une atteinte aux droits d'autrui et qu'il ne réagit pas. En l'occurrence, la condition de la connaissance était-elle vraiment remplie ? Etienne WÉRY en doute[467]. On en revient à la détermination de la notion de connaissance.

En tous les cas, la décision a soulevé de nombreuses inquiétudes parmi les fournisseurs de services d'Angleterre, qui n'avaient pas vu voir le danger à l'adoption du *Defamation Act*. Il semblerait qu'aujourd'hui, ces prestataires n'hésitent pas à supprimer tout message faisant l'objet d'une plainte, sans même en examiner succinctement le bien-fondé. Il est vrai que la transaction opérée en mars 2000 a eu de quoi en refroidir certains : Demon Internet Ltd a dû verser plus de 200'000 £ à Laurence Godfrey. Mais pourrait-on raisonnablement demander aux exploitants de *newsgroups* anglais d'étudier juridiquement tous les messages qui font l'objet d'une notification ? Les prestataires rétorquent qu'ils perdraient leur marge de profit[468]. Une telle jurisprudence a évidemment faire craindre une pluie de plaintes non fondées, afin que des informations non souhaitées par certaines multinationales ou autres groupes influents soient rapidement censurées. Pour protéger la liberté d'expression, une simple notification d'un tiers ne devrait pas être suffisante, clament les *Internet service providers*.

ii. L'affaire Aftonbladet[469]

En octobre 2000, plusieurs *postings* au contenu anti-sémite sont disponibles sur le forum de discussion du site d'Aftonbladet[470], journal de renom suédois. Les messages restent plusieurs jours sur ce forum ouvert, mais modéré. Poursuivi pour provocation à la haine raciale, le directeur éditorial du journal est condamné par un tribunal de Stockholm, le 7 mars 2002. Le modérateur du forum aurait dû censurer les *postings* litigieux.

iii. L'affaire Père Noël[471]

Le 27 mai 2002, les responsables du site Defense-consommateur.org ont été condamnés au paiement de 80'000 Euros de dommages-intérêts à Pere-Noel.fr. La société de vente en ligne reprochait aux défendeurs d'avoir contribué à la publication de messages diffamatoires à son encontre. Dans la décision, le Tribunal de grande instance de Lyon[472] passe son temps à déterminer si les *postings* en question sont diffamatoires. Ces derniers étaient certes

---

467 Etienne WÉRY, Responsabilité des fournisseurs d'accès : la liste noire continue, http://www.droit-technologie.org , 12 avril 1999.

468 Bertil COTTIER, Conférence non publiée.

469 Les informations de ce passage proviennent de l'article : Le créateur d'un forum peut être tenu responsable de son contenu, News Vivre Le Net, 11 mars 2002, disponible à l'adresse http://www.vivrele.net/node/345.html.

470 http://www.aftonbladet.se.

471 Les informations de ce passage proviennent de l'article : Defense-consommateur devra indemniser le Père-Noël(.fr), News Vivre Le Net, 29 mai 2002, disponible à l'adresse http://www.vivrele.net/node/653.html.

472 Tribunal de grande instance de Lyon, Chambre des urgences, 28 mai 2002, SA Pere-Noel.fr contre Franz Molenda, Emmanuelle Chouteau et SARL Deviant Network, disponible sur le site http://www.foruminternet.org.

véhéments, mais les pratiques de Pere-Noel.fr sont plus que douteuses. La société a d'ailleurs fait l'objet de plaintes pour escroquerie. Le tribunal ne s'attarde, par contre, guère sur l'imputabilité de la responsabilité de ces messages. Il dit simplement « *qu'il est constant que les* [responsables] *ont pris l'initiative de créer un service de communication audiovisuelle en vue d'échanger des opinions sur des thèmes définis à l'avance et en l'espèce, relatifs aux difficultés rencontrées par certains consommateurs face à certaines sociétés de vente ; qu'ils ne peuvent donc pas opposer un défaut de surveillance des messages qui sont l'objet du présent litige ; qu'ils se considèrent eux-mêmes comme les concepteurs du site incriminé et doivent donc répondre des infractions qui pourraient avoir été commises sur le site qu'ils ont créé* ». Pour le tribunal, les responsables d'un forum de discussion doivent toujours surveiller le contenu des messages postés. En clair, tout forum de discussion doit être modéré…

Les défendeurs vont faire appel et nul doute qu'ils ont de bonnes chances de trouver grâce auprès de l'organe d'appel, tant la décision est absurde.

2.2.2 Développements et conclusions

Les réflexions sur les *newsgroups* et les forums de discussion publics se rapprocheront en général de celles opérées lors du traitement de la responsabilité de l'hébergeur pour les sites *web* publics. Par le terme « public », nous entendons évidemment qualifier un contenu qui n'a pas le caractère privé au sens décrit précédemment[473]. Si le forum de discussion est dit privé[474], il faudra alors se rapporter au même passage, pour déterminer les responsabilités qui peuvent découler du contenu illicite des *postings*.

Si le gérant d'un *newsgroup* ou d'un forum de discussion a connaissance d'un message illicite, il doit le supprimer ou en bloquer l'accès. On en revient à la délimitation de la notion de connaissance. Si la notification provient d'une autorité officielle, l'intermédiaire doit agir. Si c'est le lésé qui l'a notifié, il doit agir si le contenu est manifestement illicite. Pour le reste, nous nous référons à ce qui a été dit précédemment[475].

Dans les groupes et les forums de discussion, les atteintes touchent surtout à l'honneur et la réputation des tiers. Dans ce cas, le droit de réponse est fréquemment un bon moyen pour le lésé d'atténuer le dommage. Le réseau Usenet étant accessible à tous, ce droit peut être exercé facilement. En matière de forums de discussion, l'exploitant devra veiller à ce que le lésé puisse, le cas échéant, s'inscrire et s'exprimer.

Donnons maintenant quelques indices de ce que peut être le régime de responsabilité du prestataire, selon qu'il est question d'un *newsgroup* ou d'un forum de discussion et selon que ces espaces de discussion sont modérés ou non.

i. Les *newsgroups* non modérés

L'intermédiaire sélectionne les *newsgroups* qu'il désire rendre accessibles. S'il donne accès à des groupes de discussion clairement illicites[476], sa responsabilité peut être engagée. Tel était

---

473 Cf. Partie 3 A. 4.2 p. 36.

474 L'accès à un forum de discussion est assez fréquemment conditionné par une inscription et peut parfois être limité à quelques élus. On parle dans ce dernier cas de forums fermés. En revanche, à notre connaissance, le réseau Usenet n'est jamais limité dans son accès par une telle inscription.

475 Cf. Partie 3 E. 2.3.2 iv p. 74 et F. 3.2.1 p. 84.

476 Par exemple, « alt.sex.pedo » ou, en matière civile, « alt.warez ».

le cas dans l'affaire CompuServe. Si le groupe de discussion n'amène pas nécessairement des contenus illicites, mais a un intitulé pouvant susciter une certaine suspicion[477], le fournisseur de services se doit peut-être de le visiter une fois, histoire de se donner une idée plus précise des informations s'y trouvant. Si ces informations sont manifestement illicites, il doit alors décider de ne pas le rendre accessible.
D'une manière générale, pour les groupes apparemment licites, il ne faut pas obliger l'exploitant à contrôler tous les messages. On a vu qu'un tel contrôle n'était pas exigible des prestataires d'hébergement[478] et nous devons aussi nous tenir à cette idée pour le fournisseur de services en question.

ii. Les forums de discussion non modérés

En dehors du cas où l'intermédiaire a connaissance du message illicite, nous voyons deux cas d'engagement de responsabilité.
L'intermédiaire créé les forums de discussion selon des thèmes choisis par lui. Si le forum de discussion aménagé vise à inciter les internautes à calomnier telle ou telle personne, son exploitant est bien évidemment responsable des contenus s'y trouvant.
Si le forum est assurément de nature à pouvoir amener des contenus illicites, l'exploitant doit faire preuve de plus de diligence qu'à l'encontre d'un autre forum et doit supprimer les messages manifestement illicites qu'il aurait découverts. C'est peut-être en ce sens que le Tribunal de grande instance de Lyon a condamné les responsables du site Defense-Consommateur.org. Le problème est que, dans cette espèce, les messages postés sur le forum n'étaient, de loin pas, manifestement illicites : ce fait est bien démontré par les hésitations du tribunal.

iii. Les *newsgroups* et les forums de discussion modérés

Si le *newsgroup* ou le forum de discussion est modéré, le modérateur doit, d'une manière générale, assumer une responsabilité éditoriale. C'est son rôle que de superviser les messages qui lui sont soumis et de choisir de les diffuser ou non, selon qu'il estime qu'ils sont contraires à la loi ou aux règles de l'espace de discussion. Le modérateur est censé connaître chaque information diffusée. Il valide, le cas échéant, le contenu illicite émis. Son « *pouvoir de censure est la contrepartie normale de la responsabilité qu'il encourt…* »[479]. Pour Rolf H. WEBER, le modérateur fait preuve de la diligence nécessaire à exclure sa responsabilité, s'il procède à un contrôle grossier du contenu des messages[480].

Il faut noter que le modérateur d'un groupe de discussion Usenet, à l'inverse de celui d'un forum de discussion, ne sera, la plupart du temps, pas lié avec le prestataire y donnant accès. Le modérateur a même de très grandes chances d'avoir son domicile à l'étranger, ce qui rendra l'exécution du jugement difficile.

---

477 Le mot « *sex* » pourrait mettre la puce à l'oreille de l'exploitant.
478 Cf. Partie 3 E. 2.3.1 p. 67.
479 Gérard HAAS et Olivier DE TISSOT, Atteintes.
480 Rolf H. WEBER, E-Commerce, p. 519.

3. Le gérant d'un service de messagerie électronique

3.1 Notions

Nombreux gérants d'un serveur de messagerie électronique sont des fournisseurs d'accès, mais les plus connus sont les Yahoo!, Hotmail et autre Caramail. Ces fournisseurs de services procurent - presque toujours gratuitement - aux internautes une adresse *e-mail* et une boîte aux lettres électronique, qui conserve les messages électroniques, en attendant que les destinataires les téléchargent sur leur machine.

3.2 La responsabilité du fait de la mise à disposition d'un compte *e-mail*

Nous avons vu plus haut[481] que le courrier électronique est protégé par le secret des télécommunications. A partir du moment où le prestataire n'a pas le droit de consulter - et encore moins de contrôler - ce courrier et qu'il remplit ce devoir d'inaction, il ne peut encourir aucune responsabilité civile à l'égard de leur contenu. Il faut en ce sens le comparer à des entreprises telles que la Poste ou DHL.

Ne devant pas se mêler de qui transite par ses services, l'exploitant de la messagerie électronique ne peut, a priori, pas voir sa responsabilité engagée en cas d'envoi d'un virus par un de ses abonnés à un tiers. Toutefois, il nous semblerait raisonnable qu'une loi impose au prestataire l'utilisation d'un anti-virus, afin de contrôler les fichiers joints des messages stockés sur son serveur. Sans exiger une obligation de résultat de l'exploitant d'un service de messagerie, une obligation de moyens permettrait déjà de limiter conséquemment la diffusion de virus fort préjudiciables. Il est clair que le nombre d'*e-mails* circulant par le serveur du gérant est gigantesque. Mais l'avancée technologique permettra tantôt aux anti-virus de parcourir à une très grande vitesse des données innombrables, en ne ralentissant que peu les performances de l'intermédiaire.

4. Le gérant d'un *bulletin board service*

4.1 Notion

Un *bulletin board service* (BBS) est un système informatisé consultable via Internet, qui offre une foultitude de services. Un BBS donne avant tout accès à une banques de données, dans laquelle on trouve d'une part des articles, annonces, critiques ou interviews, et d'autre part des fichiers, tels que des *freewares*[482] ou *sharewares*[483]. Les données sont tantôt fournies par le gérant du BBS, tantôt par les utilisateurs. La personne ayant accès au serveur BBS peut donc autant lire que poster une annonce, autant télécharger (*download*) que charger (*upload*) un fichier. Mais un BBS offre aussi souvent un forum de discussion, modéré ou non, et des services de *chat*[484] ou de messagerie électronique.

---

[481] Cf. Partie 3 A. 4.2 p. 36.

[482] Un *freeware* est un logiciel pouvant être utilisé gratuitement.

[483] Un *shareware* est un logiciel qui peut être testé gratuitement pendant une certaine durée et que l'utilisateur doit payer pour continuer d'en profiter. Pendant la période d'essai, les fonctions du *shareware* sont généralement limitées, afin d'inciter l'usager a en payer les droits d'utilisation.

[484] On rappelle que le *chat* (traduction française : petite conversation, causette) est un mode d'utilisation d'Internet, qui permet à deux ou plusieurs personnes de « bavarder » par écrit et en temps réel. Appelé aussi « bavardoir » en France, un tel service nécessite l'emploi du protocole IRC (*Internet Relay Chat*).

Le fonctionnement d'un BBS peut varier considérablement selon les cas. Dénommés « babilleurs » ou « babillards électroniques » en France, ils sont, soit ouverts à tous, soit réservés à leurs abonnés, l'abonnement pouvant s'avérer payant. Ils peuvent être généralistes ou porter, au contraire, sur un thème spécifique.

On voit qu'un BBS permet une certaine interactivité. Très en vogue avant l'avènement d'Internet, ce type de système n'est plus trop utilisé aujourd'hui.

4.2 La responsabilité pour les contenus illicites

Il n'y a pas lieu de développer un régime de responsabilité propre aux exploitants de *bulletin board service*, tant il n'est pas question d'un service particulier, mais d'un melting-pot de services, dont nous avons déjà retiré les responsabilités éventuelles. Nous nous référons donc à ce qui a pu être développé ci-avant, notamment dans cette section H.
Il faut quand même noter l'existence de la seule loi régissant expressément le domaine. C'est en Suède que l'on trouve depuis 1998 cette loi sur les kiosques électroniques. Cette loi oblige l'exploitant à un contrôle périodique des messages. Si le nombre des *postings* est trop conséquent pour qu'un tel contrôle soit réellement efficace, le gérant du service doit au moins mettre en place un système d'alerte. Qu'il découvre lui-même un contenu manifestement illicite ou qu'il en soit informé, il doit l'effacer[485].

I. Le fournisseur de contenu (*content provider*)

1. Notions

On connaît deux types de fournisseurs de contenu : l'auteur et le *webmaster*.

L'auteur, parfois appelé éditeur de contenus en France[486], crée ou met à disposition sur Internet des informations, soit du texte, des images, des sons ou des vidéos. N'importe qui peut être auteur sur Internet : entreprises de presse, associations, fournisseurs d'accès, fournisseurs d'hébergement, simples particuliers, etc. On est déjà en présence d'un auteur à partir du moment où un cybernaute s'exprime au travers de son site *web*, d'un *e-mail*, d'un message dans un forum de discussion, etc. A la différence des médias traditionnels qui supputent généralement un certain professionnalisme, Internet permet à tout en chacun de s'« autopublier » très facilement et souvent gratuitement ou presque : Arnaud Hamon dit, des producteurs de contenu, qu'ils sont « *de plus en plus atomisés* »[487]. En fait, le nouveau médium permet à chacun de participer directement à la diffusion de l'information, en jouissant d'une grande liberté et sans être soumis à une autorisation ; il offre la possibilité « *à un individu isolé ou à un groupe sans moyens d'être plus médiatique qu'un Etat ou une multinationale* »[488].
Il faut noter que l'auteur d'une information disponible sur le net n'est pas forcément un accro de la toile. Il peut même ne pas avoir d'ordinateur. Le contenu qu'il a créé peut néanmoins se retrouver sur Internet avec ou sans son autorisation, chez un fournisseur de contenu professionnel ou amateur.

---

485 Bertil COTTIER, Impact, p. 6.
486 Cf. l'affaire Lynda Lacoste, où la société SPPI s'est reconnue seule responsable du contenu éditorial du site Parisvoyeur.
487 Arnaud HAMON, Expression, p. 159.
488 Sébastien CANEVET, Rapport.

Le *webmaster*[489] est l'administrateur du site *web*. Il s'attache surtout à l'aspect technique du site, qui doit toujours être accessible aux internautes. Mais le *webmaster* est aussi souvent un *webdesigner*, soit la personne qui conçoit le site au niveau « artistique ». Il transforme alors l'information brute en fichiers électroniques, qu'il agence et met en forme sur le site Internet, afin que ce dernier soit intuitif et d'utilisation aisée. En cas de problèmes, notamment si un lien hypertexte est rompu, c'est au *webmaster* que l'internaute doit envoyer un *e-mail* en guise d'avertissement. C'est aussi le *webmaster* qui doit assurer la maintenance et le suivi du site Internet.
Certains auteurs cataloguent le *webmaster* dans les fournisseurs de services[490]. Ils n'ont pas tort, mais l'important est que l'acteur en question répondra en tant fournisseur de contenu[491]. Nous comprenons donc cette dernière notion dans le sens que lui donne le *Communications Decency Act*, qui définit la notion d'*information content provider* comme « *any person or entity that is responsible, in whole or in part, for the creation or development of information provided through the Internet or any other interactive computer service* ». Une telle définition englobe évidemment le *webmaster*.

Il faut encore remarquer que, pour les sites non professionnels, l'auteur et le *webmaster* sont généralement les mêmes personnes et que le concept de fournisseur de contenu regroupe encore d'autres notions, telles que le propriétaire du site, le responsable du site, l'exploitant du site, etc, notions dont les contours sont flous. Des dispositions telles que l'art. 55 du CO risquent ainsi d'entrer en jeu.

2. La responsabilité pour le contenu illicite fourni

S'il est une certitude dans le domaine de la responsabilité en ligne, c'est que le fournisseur de contenu est le premier responsable pour le contenu illicite délivré ou mis en page sur Internet. A partir du moment où le droit s'appliquait aux communications électroniques, il n'y avait plus de place au moindre doute. La jurisprudence l'a d'ailleurs tout de suite confirmé[492].
La responsabilité du fournisseur de contenu sur Internet est pleine et entière. Il répond comme il répondrait d'un contenu illicite publié sur un autre support. Les régimes de responsabilité aquilienne ne font pas référence à des comportements, méthodes ou supports spécifiques. Le droit suisse ne fait pas exception : la problématique de la responsabilité des *content providers* ne change pas selon qu'ils aient rendu accessibles ou mis en circulation les informations illicites sur Internet ou ailleurs. L'important est que l'information illicite soit publiée[493] et que les conditions d'application de l'art. 41 du CO soient remplies. Il ne faut pas se demander comment, pourquoi, au travers de qui, ni si la publication a eu lieu avec ou sans son accord[494].

Les prestataires techniques répondent eux aussi des contenus informationnels qu'ils fournissent. Ils ne sauraient bénéficier d'un privilège à cet égard. L'art. 5 al. 1 du *Telediensgesetz* exprime bien ce principe : « *Dienstanbieter sind für eigene Inhalte, die sie für Nuztung bereithalten, nach den allgemeinen Gesetzen verantwortlich* ». La directive sur le commerce électronique ne contient pas ce type de disposition, car si une telle norme a le mérite de la clarté, elle n'en est pas moins superfétatoire.

---

489 Traduit en France par le terme « webmestre »…
490 Par exemple, Rolf H. WEBER, E-Commerce, p. 526.
491 Frédérique OLIVIER et Eric BARBRY, Hébergement, p. 1087.
492 Cf. par exemple TGI Paris, ord. réf. 12 juin 1996, UEJF c. Calvacom et autres.
493 David ROSENTHAL, Projekt, p. 189.
494 David ROSENTHAL, Projekt, p. 195.

On peut aussi ajouter que si la personne, dont l'activité principale est la fourniture d'information, est son propre hébergeur, elle ne profitera pas plus d'un *safe harbour*.

Si l'auteur et le *webmaster*, voire le propriétaire du site ou autres, sont des personnes différentes, la répartition des responsabilités et donc des dommages-intérêts, est régie par l'art. 50 du CO. Dans le contrat liant le *webmaster* au propriétaire du site, il y a sûrement des clauses d'exclusion ou de limitation de responsabilité, mais elles ne sont évidemment pas opposables aux tiers qui seraient lésés par le contenu du site. Le lésé peut donc intenter une action contre l'un ou l'autre de ces acteurs et obtenir la pleine réparation du dommage qu'il a subi.

Il faut encore préciser que la responsabilité d'un professionnel de l'information sera logiquement jugée de façon plus sévère que celle d'un amateur.

On le voit, la responsabilité du fournisseur de contenu sur Internet ne génère donc pas de question théorique particulière. Pour le lésé, les problèmes peuvent évidemment surgir dès qu'il souhaite prouver ce qu'il allègue. Mais bien avant d'en arriver là, il faut encore que le fournisseur soit connu.

3. L'anonymat

Une des raisons pour lesquelles le lésé tente de trouver réparation auprès du prestataire technique est l'anonymat du fournisseur de contenu. La probable insolvabilité de ce dernier est certes la première motivation de la victime dans son choix d'actionner un prestataire. Un tel fait est inéluctable. En revanche, l'anonymat peut être combattu, lorsqu'il mérite de l'être.

Force est de constater qu'aujourd'hui, une certaine clandestinité règne sur Internet. Les pseudonymes et les fausses identités sont légion dans le cyberespace. Mais sur Internet, l'identité décisive n'est pas celle du « surfeur », mais celle de la machine utilisée par celui-ci. Conformément au souhait des inventeurs d'Internet, chaque ordinateur connecté au réseau est identifiable par un numéro unique, nommé adresse IP. Pour découvrir l'adresse IP de l'ordinateur avec lequel le cyberdélinquant a agi, il faut déterminer le fournisseur d'accès qui a permis à la machine en question de se connecter sur Internet, en consultant « *les bases de données en ligne du RIPE, organisme chargé d'attribuer les blocs d'adresses IP en Europe* »[495]. Il ne reste alors qu'à demander poliment au fournisseur d'accès de livrer l'identité de son client, censé être le détenteur de la machine correspondante à l'adresse IP. Quant à l'obligation du fournisseur d'accès de conserver les *logs* de connexion, nous nous référons à ce qui a dit précédemment[496].

L'entrave à l'anonymat que constitue l'adresse Internet a titillé l'esprit de certains informaticiens, qui, sous le prétexte de la préservation de la vie privée, ont élaboré des solutions pour masquer cette adresse. Ainsi, on trouve sur Internet des « *anonymizers* », tiers de confiance qui substituent leur adresse IP à celle de l'internaute. Il est possible, soit de se rendre sur le site de l'*anonymizer*[497], puis d'entrer l'URL du site sur lequel on veut passer

[495] Alain STROWEL et Nicolas IDE, Responsabilité. L'acronyme RIPE signifie Réseaux IP Européens. Leurs registres se trouvent sous l'adresse http://www.ripe.net.

[496] Cf. Partie 3 B. 2.4.1 p. 49.

[497] La communauté Le Village offre ce service à l'adresse suivante : http://www.levillage.org/securite/securisurf. Il faut être membre pour bénéficier d'un tel privilège.

inaperçu, soit de lancer un logiciel « anonymisant », facile d'accès[498] et d'emploi, qui fera passer automatiquement l'internaute par le site de l'*anonymizer*. Certains sites permettent la pratique de l'« *anonymous remailing* », soit l'envoi de messages anonymes. Des logiciels[499] offrent aussi cette possibilité.

Il faut noter que le prétexte de la préservation de la vie privée évoqué ci-dessus n'en est parfois pas un. Il est en effet des circonstances, où le respect de la vie privée légitime entièrement l'usage de procédés d'« anonymisation », ou, du moins, le surf anonyme. Pensons en particulier aux utilisateurs des forums de discussion traitant, par exemple, de l'inceste, du SIDA ou de la toxicomanie. Pensons aussi aux dissidents politiques des pays soumis au diktat d'un tyran. Pensons simplement à ceux qui veulent éviter de futurs *spams*. L'anonymat n'est pas un mal en soi. C'est dans ce sens que la directive sur le commerce électronique « *ne peut pas empêcher l'utilisation anonyme de réseaux ouverts tels qu'Internet* »[500]. Même s'il n'est pas considéré comme un droit en tant que tel, on peut estimer que l'anonymat fait partie intégrante du droit au respect de la vie privée, au sens de l'art. 8 de la CEDH. Il est consacré dans quelques domaines, tels que celui de la téléphonie : pour une modique somme, les opérateurs de télécommunication empêchent l'indication du numéro appelant sur le téléphone récepteur possédant une telle fonction.

Selon Jean-Marc DINANT[501], les « *procédés d'anonymisation restent toutefois globalement peu fiables, ralentissent le fonctionnement du réseau et nécessitent en général un paiement* ». Il est juste de vivement relativiser les possibilités de clandestinité, en précisant qu'il existe de nombreux systèmes techniques permettant d'identifier un internaute. Il subsiste presque toujours une trace d'un « surf » sur le net[502]. Trace dont profitent les autorités, qui disposent d'équipements toujours plus perfectionnés et qui profitent de l'« expérience » des *hackers* repentis devenus d'heureux fonctionnaires, qui s'amusent désormais dans le rôle du policier. Les pirates et autres délinquants informatiques se font de plus en plus attraper[503] : il semblerait même que les enquêteurs n'ont rarement eu d'investigations plus simples. Mais la mise à disposition de tels moyens ne regarde pas le droit civil, mais seulement le droit pénal. Et le lésé n'investira pas des dizaines ou centaines de milliers de francs pour, éventuellement, mettre la main sur une société fantôme ou un cyberdélinquant sans le sou ou résident aux antipodes.

Même si l'anonymat sur Internet, accompagné de l'impunité qui en découlerait, n'est qu'un mythe, il n'en est pas moins problématique. Utilisé à outrance par les pornographes et les pirates, il est source de complications. C'est pourquoi le Conseil d'Etat français s'exprime ainsi : *« Si l'anonymat est une illusion sur les réseaux, il est souvent difficile de déceler l'identité réelle de la personne physique ayant commis l'infraction ; il parait donc essentiel*

---

498 De tels logiciels sont notamment disponibles aux adresses suivantes : http://www.stealth-anonymizer.com, http://www.anonymizer.com.

499 Comme exemples, on peut citer Ghost Mail et Potato.

500 Cf. considérant (14) de la directive.

501 Jean-Marc DINANT, Les risques majeurs de IPv6 pour la protection des données à caractère personnel, http://www.droit-technologie.org , 7 Novembre 2001, p. 6.

502 En réalité, la meilleur façon d'assurer son anonymat est l'utilisation d'un ordinateur « public », tel qu'on en trouve dans un cybercafé ou une haute école. Il sera alors difficile pour les enquêteurs de remonter à l'auteur. Mais dans de tels cas de figure, le champ d'action de l'auteur est limité.

503 A l'image de l'auteur de la menace de mort adressée au député-maire corse André Santini par le biais d'un message électronique anonyme.

d'améliorer la traçabilité des messages et l'identification des acteurs afin de pouvoir engager une action en responsabilité »[504].

Si l'anonymat complet est nuisible, il ne faut pas pour autant tomber dans l'autre extrême, comme le craignent actuellement les internautes belges. A ce propos, Etienne WÉRY s'inquiète d'une législation passée inaperçue, qui pourrait, dans le pire des cas, amener à considérer le surf anonyme comme illégal[505]. Sans aller jusque-là, on pourrait songer à imposer une obligation d'identification du fournisseur de contenu sur son site *web*. Sébastien CANEVET y est favorable, mais seulement en ce qui concerne les professionnels[506]. Il est vrai qu'il serait très préjudiciable pour la liberté d'expression que chaque auteur de site ait à supporter une telle tâche. A notre sens, il faut surtout se concentrer sur les obligations de l'hébergeur et du fournisseur d'accès d'identifier le fournisseur de contenu, notamment par l'entremise des fichiers *logs*.

[504] Conseil d'Etat (français), Etude Internet et les réseaux numériques, 2 juillet 1998, 4e Partie, 3.1, disponible à l'adresse suivante : http://www.internet.gouv.fr/francais/textesref/rapce98/sommaire.htm.

[505] Pour de plus amples renseignements, Etienne WÉRY, Surfer anonymement devient illégal en Belgique, http://www.droit-technologie.org, 18 mars 2002.

[506] Sébastien CANEVET, Rapport.

Partie 4 Conclusion : l'adaptation nécessaire du droit en matière de responsabilité

Dans l'introduction, nous avons clairement énoncé que l'avènement d'Internet rendait nécessaire une réforme de la législation suisse. Il reste à savoir si le changement doit aussi toucher le monde de la responsabilité civile.

Les quelques cas de responsabilité marginaux, que nous avons examinés, nous ont surtout montré que le droit pénal suisse devrait être modifié, afin d'ériger en infraction certains comportements aujourd'hui difficilement punissables. Indirectement, cela permettrait aux lésés de disposer d'une norme protectrice, pour obtenir réparation.

Quant à la responsabilité du fait de contenus illicites, les pays non membres de l'Union européenne qui se sont intéressés au problème n'ont pas toujours opté pour des modifications législatives, laissant le soin aux juges nationaux de se dépêtrer avec le droit à disposition. C'est notamment le cas du Canada. Le législateur canadien juge que les principes du droit commun sont assez souples pour régir la responsabilité des acteurs d'Internet. Comme leurs homologues étasuniens, les juges canadiens usent et abusent des métaphores et autres analogies, pour trouver des solutions aux litiges qui leur sont soumis[507]. On a pourtant vu que de telles pratiques n'étaient pas très adaptées aux réflexions liées au réseau des réseaux… C'est peut-être pourquoi le Québec a adopté le 21 juin 2001 la Loi concernant le cadre juridique des technologies de l'information[508], qui contient des clauses régissant la responsabilité des prestataires Internet.

En Suisse, le droit de la responsabilité, notamment l'art. 41 du CO, permet de trouver une solution acceptable à chaque cas présenté à un tribunal[509]. La responsabilité aquilienne est au centre du débat et c'est très bien ainsi. Mais peut-on se contenter d'une solution acceptable ?

Si la solution risque de n'être qu'acceptable, c'est en partie parce que les intérêts à prendre en compte dans la détermination de la responsabilité d'un prestataire technique sont nombreux. Les jugements risquent de partir dans tous les sens, certains juges accordant plus d'importance à tel ou tel intérêt. Même plusieurs décisions du Tribunal fédéral ne tueraient pas entièrement l'incertitude juridique, sachant que les sages de Mon-Repos ne prennent position que sur ce qui est nécessaire à la résolution du litige. Un débat démocratique serait de bon aloi pour la création d'un cadre générateur de sécurité juridique, concept primordial dans un environnement de justice.
De plus, on peut penser que l'application des normes existantes amènerait un régime de responsabilité trop sévère à l'égard des prestataires techniques d'Internet[510], comme cela a été le cas ailleurs, notamment en France. Un adoucissement serait nécessaire au bon développement d'Internet et de ses débouchés en Suisse.
Un autre argument en faveur d'une réglementation spécifique de la responsabilité délictuelle sur Internet est l'harmonisation nécessaire des solutions au niveau international quant aux problèmes liés à ce phénomène transfrontière. Les Etats-Unis et l'Union européenne ont

---

[507] Pierre TRUDEL, Le droit d'Internet au Canada, Colloque international, L'Internet et le droit, septembre 2000, la Sorbonne.
[508] L.Q. 2001, c. 32, disponible à l'adresse http://www.autoroute.gouv.qc.ca/loi_en_ligne/index.html.
[509] Dans ce sens, Jérôme BENEDICT, Responsabilité, p. 43.
[510] Charles PONCET (Intégration, p. 215) semble aller dans ce sens.

globalement des solutions semblables, en tout cas en matière de droit d'auteur grâce au *Digital Millenium Copyright Act*. Il faut s'en approcher, en attendant une hypothétique convention internationale, solution idéale du futur.

Dans le domaine de la responsabilité pénale des intermédiaires techniques, bien que le Conseil fédéral ait exprimé que le droit actuel permettait « *des solutions appropriées et différenciées* »[511], notre exécutif a choisi de suivre, en tout cas dans les grandes lignes, la voie montrée par la motion Pfisterer, qui prône la mise en place de dispositions quasi identiques à celles de la directive sur le commerce électronique. Dans sa prise de position du 28 février 2001, le Conseil fédéral souligne en effet qu'une « *harmonisation internationale de la législation relative à Internet est souhaitable, voire nécessaire* ». Mais le Conseil fédéral n'est pas encore passé aux actes. Notre exécutif a mis en avant l'état juridique et technique encore très mouvant du développement d'Internet. Voilà peut-être la raison de ce non-empressement. Mais, si la Suisse souhaite que le domaine soit calme comme un lac gelé pour légiférer, elle n'est pas sortie de l'auberge. Il ne faut pas attendre une affaire provoquant une levée de boucliers pour agir, mais plutôt suivre l'exemple donné par les Allemands, qui, dès 1997, possédaient une loi assurant le minimum nécessaire de praticabilité et de sécurité du droit, ou les Québécois, dont la province ne connaissait pas encore de jugements significatifs dans le domaine de la responsabilité des intermédiaires d'Internet[512]. De plus, le gros des principes de la directive sur le commerce électronique semble pouvoir tenir la route pendant quelques décennies, tant ils sont généraux.
La prise de position du Conseil fédéral a le mérite de montrer que l'exécutif ne souhaite pas modifier les choses uniquement dans le domaine pénal : il veut adopter des dispositions « *relevant de tous les domaines du droit concernés* ». Il souhaite, à terme, aussi harmoniser le régime suisse de responsabilité civile des prestataires techniques avec celui instauré à l'étranger - lorsqu'il sera moins en mouvement, bien évidemment. C'est heureux.

Oui. Il faut légiférer en matière civile. Mais comment ?

Formellement, il ne faut pas oublier que l'évolution d'Internet est telle que les dispositions législatives trop ciblées deviennent vite obsolètes. En ce sens, une loi formelle ne doit contenir que des principes et il faut utiliser la souplesse d'un outil tel que l'ordonnance et la flexibilité de la jurisprudence. Seule une régulation souple peut suivre l'évolution foudroyante de la technologie. Il ne faut pas cristalliser des règles dépendant de détails techniques.

Matériellement, l'important est que la loi spécifique à la responsabilité délictuelle relative à Internet concilie au mieux les intérêts contradictoires en présence - que nous avons eu de cesse de rappeler -, et ce pour tous les types d'activités développées en liaison avec Internet. Le premier intérêt à prendre en considération est la technique : il faut tenir compte de toutes les spécificités d'Internet. Ensuite, la liberté d'expression doit constituer un frein à certains idées tyranniques[513] : la réglementation spécifique doit garantir un minimum de liberté sur

---

[511] Motion Thomas Pfisterer, Cybercriminalité : modification des dispositions légales, disponible à l'adresse http://www.parlament.ch/afs/data/f/gesch/2000/f_gesch_20003714.htm. Le Conseil fédéral suit ainsi l'avis de droit de l'Office fédéral de la justice du 24 décembre 1999 (Gutachten zur Frage der strafrechtlichen Verantwortlichkeit von Internet-Access-Providern gemäss Artikel 27 und 322bis StGB, JAAC 2000, p. 820ss). A l'inverse, Marcel Alexander NIGGLI, Franz RICKLIN et Günter STRATENWERTH (Die strafrechtliche Verantwortlichkeit von Internet-Providern, Gutachten, octobre 2000, JAAC 2000, p. 820ss) pensent qu'une rapide modification législative est nécessaire pour assurer « *die notwendige Rechtssicherheit* ».

[512] Pierre TRUDEL, Responsabilité.

[513] Charles PONCET, Intégration, p. 217 : « *L'intégration de l'Internet dans l'ordre juridique suisse* […] *doit se faire sous l'angle de l'art. 10 CEDH* ».

Internet. En ce sens, aucune obligation générale de contrôle ne doit être imposée aux prestataires, afin d'éviter toute censure préjudiciable. Il faut également privilégier le développement d'Internet, plus précisément la croissance des activités des professionnels en Suisse. Sauvegarder l'attrait de la place économique suisse est primordial : si le régime de responsabilité à l'égard des intermédiaires est plus sévère en Suisse qu'à l'étranger, les opérateurs suisses risquent d'en pâtir et le monde suisse du travail par la même occasion. Il ne faut pas sous-estimer les futurs enjeux économiques qui se cachent derrière les activités liées à Internet. Par conséquent, le législateur suisse se doit de ne pas trop responsabiliser les prestataires et de ne pas leur imposer des devoirs trop astreignants : aider la justice, oui ; être l'esclave de la justice, non. S'il faut prendre en compte l'avis des professionnels, il ne faut pas se laisser guider par les lobbies, qui ont dominé les débats dans la construction de la directive européenne. En effet, il faut également tenir compte de la demande de sécurité vis-à-vis des contenus illicites et de la protection des droits des personnes. Le législateur doit favoriser la lutte les contenus illicites et, ainsi, ne pas trop épargner les prestataires, notamment le fournisseur d'hébergement.

La directive sur le commerce électronique incorpore ces intérêts, en tout cas en partie. En plus de l'harmonisation nécessaire des législations, la prise en compte de ces intérêts est une des raisons qui nous font dire que la réglementation spécifique suisse doit instaurer le même système de havres de sécurités et, par conséquent, créer des cas d'exonérations pour certaines activités bien définies et sous des conditions rigoureuses. Les *safes harbours* en question viendront ainsi se greffer sur les art. 41ss du CO. Mais le législateur doit profiter des fenêtres laissées béantes[514] par la directive, afin d'instaurer des obligations judicieuses à la charge des intermédiaires techniques. En tous les cas, l'hébergeur doit rester dans le viseur, car il est le seul à pouvoir faire disparaître le contenu illicite.

Il faut et il ne faut pas, le législateur doit et ne doit pas… Les nécessités sont nombreuses, agglutinées qu'elles sont derrière un seul impératif : la Suisse doit suivre la tendance dominante de la réglementation spécifique touchant à la responsabilité en ligne. Car seule l'adaptation du droit en matière de responsabilité offrira l'assurance d'une bonne solution à chaque cas.

[514] Cf. les art. 12 al. 3, 13 al. 2, 14 al. 3 et 15 al. 2 de la directive sur le commerce électronique.

Bibliographie

ABOUT, Carole	La responsabilité des personnes qui facilitent l'accès aux sites Internet en France et aux Etats-Unis, Intellex, 2000 (cité : Responsabilité)
BARBRY, Eric	Le droit du mail, 31 octobre 2000, journaldunet.com
BENEDICT, Jérôme	La responsabilité civile des prestataires techniques sur Internet, in Responsabilité civile et assurance : études en l'honneur de Baptiste Rusconi, Lausanne 2000, p. 11-43 (cité : Responsabilité)
BERNI, Markus	Sicherheit, Vetraulichkeit und Haftungsfragen, in E-Commerce : Rechtliche Aspekte einer neuen Geschäftsform, Zürich (sans date), p. 65-88 (cité : E-Commerce)
BERTRAND, André / PIETTE-COUDOL, Thierry	Internet et le droit, 1e éd., Paris 1999
BRAUN, Alexandre	Prescription des délits commis sur l'Internet : une impunité qui ne dit pas son nom ?, Juriscom.net, mars 1999
BREESE, Pierre	Guide juridique de l'Internet et du commerce électronique, Paris 2000
BRINER, Robert G.	Die Rechtsstellung des Access Providers, in Reto M. HILTY : Information Highway, Bern 1996, p. 489ss
BOCHURBERG, Lionel	Internet et commerce électronique, 2e éd., Paris 2001
CAHEN, Murielle	Responsabilité des hébergeurs, http://www.murielle-cahen.com, décembre 1999
CAHEN, Murielle	Les liens hypertexte, http://www.murielle-cahen.com, janvier 2001
CAHEN, Murielle	Responsabilité des moteurs et annuaires de recherche, http://www.murielle-cahen.com, janvier 2001 (cité : Moteurs)
CAHEN, Murielle	Les metas, http://www.murielle-cahen.com, février 2001
CAHEN, Murielle	Mémoire cache et responsabilité, http://www.murielle-cahen.com, avril 2001

CANEVET, Sébastien	La responsabilité des acteurs et des intermédiaires techniques, rapport au Premier Ministre, www.canevet.com (cité : Rapport)
CANEVET, Sébastien	FAQ sur le courrier électronique, www.canevet.com
CHEVALIER, Pierre-Ami	Les rapports éditeur-rédacteur et les tiers, in Aspects du droit des médias, tome I, Fribourg 1983, p. 179ss.
CLOUTIER, Jean-Pierre	Censure et liberté d'expression : recherche d'une solution politiquement raisonnable, socialement acceptable et techniquement réaliste, www.risq.qc.ca
COSTA-FORU, Irina	Les fournisseurs d'hébergement face à leurs responsabilités, Intellex, 2000
COTTIER, Bertil	Quelles responsabilités du fait de l'introduction de liens hypertextes sur une page web ? in Internet, actes illicites et responsabilités, 7e journée de droit des ingénieurs, 8 décembre 2000
COTTIER, Bertil	Impact des nouveaux médias sur la science et la pratique du droit, in Quelques facettes du droit de l'Internet, Neuchâtel 2001 (cité : Impact)
DESCHENAUX, Henri / TERCIER, Pierre	La responsabilité civile, 1e éd., Berne 1975
DIMEGLIO, Arnaud	La guerre contre les moteurs a commencé, Juriscom.net, 3 octobre 2001
DINANT, Jean-Marc	Les risques majeurs de IPv6 pour la protection des données à caractère personnel, http://www.droit-technologie.org, 7 novembre 2001
DOCQUIR, Pierre-François	Contrôle des contenus sur Internet et liberté d'expression au sens de la Convention européenne des droits de l'homme, http://www.droit-technologie.org, mai 2002
DUFOUR, Arnaud	Internet, 7e éd., Paris 1998 (cité : Internet)
ERNST, Stefan	Zivil- und strafrechtliche Verantwortlichkeit für Hyperlinks auf fremde Inhalte, www.rrzn.uni-hannover.de (cité : Hyperlinks)
FG Associés	Les incidences juridiques des liens hypertextes, Expertises, novembre 1998 et février 1999
FG Associés	A propos de la décision Estelle Hallyday, Expertises, avril 1999

FG Associés	Internet et les libertés publiques, Interview publiée dans le Monde Informatique, 7 juillet 2000
GIUSSANI, Bruno	Pas de cybersexe sans capote, Webdo, 24 avril 2001
HAAS, Gérard / DE TISSOT, Olivier	Remarques sur les problèmes posés par les atteintes aux droits individuels sur les forums Internet !, Juriscom.net, 20 décembre 1998 (cité : Atteintes)
HAAS, Gérard / DE TISSOT, Olivier	La mise à disposition de pages Web est-elle dangereuse ?, Juriscom.net, 5 juin 1999
HAMON, Arnaud	Une approche de la liberté d'expression sur Internet, Université Paris X Nanterre, année 1999/2000 (cité : Expression)
KALATHIL, Shanti / BOAS, Taylor C.	The Internet and State Control in Authoritarian Regimes : China, Cuba and the Counterrevolution, First Monday, volume 6, number 8 (August 2001)
KELTNER, Roman	Haftung für Hyperlinks am Beispiel der ersten höchstgerichtlichen Entscheidung in Österreich, www.it-law.at
KELTNER, Roman	Haftung und Überwachungspflicht der Suchmaschinenbetreiber und Hyperlinksetzer nach dem Entwurf zum ö. E-Commerce-Gesetz (ECG), www.it-law.at
KREMPL, Stefan	Netzsperre für Fritzchen Doof, heise.de, 22.11.2001
LABBÉ, Eric	Pourriel, pollupostage et référencement abusif : le spamming dans tous ses états, Juriscom.net, avril 1999
LARATE, Isabelle	Les liens hypertextes, Intellex, 2000
LATRIVE, Florent	Les hébergeurs priés de sévir. La loi va les obliger à la vigilance sur les contenus de leurs sites, Libération, 6 avril 2000
Lucas, André	La responsabilité des différents intermédiaires de l'Internet, Colloque international, L'Internet et le droit, septembre 2000, la Sorbonne (cité : Responsabilité)
MARZOUKI, Meryem	Quelques définitions, Après-Demain, Revue de la Ligue des droits de l'homme, n° 430-431, janvier-février 2001
MOLE, Arian	Cookies : des mouchards sur Internet, les Echos, 15 janvier 1998

MOREILLON, Laurent	Nouveaux délits informatiques sur Internet, Medialex 1/01, p. 21ss (cité : Délits)
NEUMANN, Andreas	Ordnungsrechtliche Sperrungsverfügungen und die Informationsfreiheit nach Art. 5 Abs. 1 S. 1 2. Alt. GG, www.artikel5.de
NIGGLI, Alexander / RICKLIN, Franz / STRATENWERTH, Günter	Die strafrechtliche Verantwortlichkeit von Internet-Providern, Gutachten, octobre 2000
Office fédéral de la justice (OFJ)	Internet. Le nouveau média interroge le droit. Rapport d'un groupe interdépartemental sur des questions relevant du droit pénal, du droit de la protection des données et du droit d'auteur suscitées par Internet, Bern 1996
Office fédéral de la justice (OFJ)	Gutachten zur Frage der strafrechtlichen Verantwortlichkeit von Internet-Access-Providern gemäss Artikel 27 und 322bis StGB, JAAC 2000, p. 820ss
OLIVIER, Frédérique / BARBRY, Eric	La responsabilité des prestataires d'hébergement sur l'Internet, JCP G 1999 II 10101, p. 1084ss (Hébergement)
OLIVIER, Frédérique / BARBRY, Eric	La responsabilité des professionnels de l'internet… une histoire sans fin, LEGICOM N^{o} 21/22, 2000/1 et 2, p. 79ss
PATIN, Jean-Claude	La responsabilité des hébergeurs n^{o}2, Juritel.com
PAUL, Christian	Du droit et des libertés sur Internet, rapport au Premier Ministre, http://www.internet.gouv.fr/rapportcpaul.htm (cité : Libertés)
POIDEVIN, Blandine	L'affaire Altern, Jurisexpert.com
Police fédérale suisse	La responsabilité pénale des fournisseurs de services Internet, Bern 2000 (cité : Responsabilité pénale)
PONCET, Charles	L'intégration de l'internet dans l'ordre juridique suisse, Medialex 4/1997, p. 207ss (cité : Intégration)
PROBST, Thomas	Quelle responsabilité pour les fournisseurs d'accès et d'hébergement ? in Internet, actes illicites et responsabilités, 7^{e} journée de droit des ingénieurs, 8 décembre 2000
ROJINSKY, Cyril	L'approche communautaire de la responsabilité des acteurs de l'Internet, Juriscom.net, 11 octobre 2000 (cité : Approche)
ROSENTHAL, David	Projekt Internet - Was Unternehmen über Internet und Recht wissen müssen, Zürich 1997 (cité : Projekt)

ROSENTHAL, David — Les risques d'Internet - De la croyance à la réalité, résumé de l'étude TA « Internet - schöne neue Welt ? Der Report über die unsichtbaren Risiken » , Conseil suisse de la science, Bern 1999

ROSENTHAL, David — Unverlangte Weber-E-Mail ohne Rechtsfolgen ?, Medialex 4/1999 p. 203ss

SCHMIDBAUER, Franz — Link ist nicht gleich Link, http://www.internet4jurists.at

SCHUHMACHER, Dirk — Sperrungsverpflichtungen für Access-Provider bezüglich des Zugangs zu Webseiten mit rechtswidrigen Inhalten, www.dfn.de (cité : Sperrungsverpflichtungen)

SÉDALLIAN, Valérie — 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 du Lamy droit de l'informatique et des réseaux 1999, supplément au n° 110, p. 1ss (cité : Responsabilité)

SÉDALLIAN, Valérie — A propos de la responsabilité des outils de recherche, Juriscom.net, 19 février 2000 (cité : Outils)

SEGOND, Francis — Affaire CompuServe Allemagne, résumé de la décision en appel, www.canevet.com.

SIRINELLI, Pierre — La responsabilité des intermédiaires de l'Internet, Colloque international, L'Internet et le droit, septembre 2000, la Sorbonne (cité : Responsabilité)

SPACENSKY, Vanina — Promotion d'un site web et risques encourus : quelle responsabilité pour les outils de recherche et les créateurs de liens hypertexte ?, Legipresse avril 1998 (cité : Promotion)

STADLER, Thomas — Sperrungsanordnungen gegenüber Access-Providern, 1999, www.afs-rechtsanwaelte.de

STADLER, Thomas — Die Verantwortlichkeit der Inhaltsanbieter nach der E-Commerce-Richtlinie und dem EGG, 2001, www.afs-rechtsanwaelte.de

STADLER, Thomas — Der derzeitige Stand der Diskussion zur Frage der Haftung für fremde Inhalte infolge der Setzung eines Links, 2002, www.afs-rechtsanwaelte.de (cité : Links)

STROWEL, Alain / IDE, Nicolas — Responsabilité des intermédiaires : actualités législatives et jurisprudentielles, http://www.droit-technologie.org, 10 octobre 2000 (cité : Responsabilité)

STROWEL, Alain / IDE, Nicolas	La responsabilité des intermédiaires sur Internet : actualités et question des hyperliens, http://www.droit-technologie.org, 8 février 2001 (cité : Hyperliens)
STROWEL, Alain / IDE, Nicolas / VERHOESTRAETE, Florence	La directive du 8 juin 2000 sur le commerce électronique : un cadre juridique pour l'Internet, Journal des tribunaux (Bruxelles), n° 6000, 17 février 2001, p. 133ss (cité : Directive)
SULLIVAN, Danny	How search engines work ?
THOUMYRE, Lionel	Liens hors-la-loi, Juriscom.net, septembre 1998
THOUMYRE, Lionel	Les hébergeurs dans les filets de la justice, Juriscom.net, octobre 1998
THOUMYRE, Lionel	Responsabilités sur le Web : une histoire de la réglementation des réseaux numériques, Lex Electronica, vol. 6, n° 1, printemps 2000 (cité : Réglementation)
THOUMYRE, Lionel	Responsabilité des hébergeurs : détours et contours de l'obligation de vigilance, Juriscom.net, 5 août 2000 (cité : Détours)
TRUDEL, Pierre	L'architecture technique comme élément régulateur du cyberespace, Medialex 4/2000, p. 187ss (cité : Architecture)
TRUDEL, Pierre	Le droit d'Internet au Canada, Colloque international, L'Internet et le droit, septembre 2000, la Sorbonne
TRUDEL, Pierre	La responsabilité civile sur Internet selon la Loi concernant le cadre juridique des technologies de l'information, Développements récents en droit de l'Internet, Service de formation permanente, Barreau du Québec, n° 160, 2001 (cité : Responsabilité)
VANHOOLANDT, Philippe	La désinformation sur Internet, vanho.com, octobre 1997
VERBIEST, Thibault	La responsabilité des outils de recherche sur Internet en droit français et droit belge, in Cahiers du Lamy droit de l'informatique et des réseaux 1999, supplément au n° 116
VERBIEST, Thibault	Quelle responsabilité pour les acteurs de l'internet ?, L'Echo, 21 janvier 1999 (cité : Acteurs)
VERBIEST, Thibault	Entre bonnes et mauvaises références. A propos des outils de recherche sur Internet, A&M, mars 1999, n°1 (cité : Références 1)

VERBIEST, Thibault	Entre bonnes et mauvaises références. A propos des outils de recherche sur Internet, 2ème partie, Cyberlex, 17 avril 1999 (cité : Références 2)
VERBIEST, Thibault	La Directive européenne sur le commerce électronique, Juriscom.net, 15 juin 2000
VERBIEST, Thibault / THOUMYRE, Lionel	Le mannequin et l'hébergeur, Juriscom.net, 25 février 1999
VERBIEST, Thibault / WÉRY, Etienne	La responsabilité des fournisseurs de services Internet : derniers développements jurisprudentiels, http://www.droit-technologie.org, 20 mars 2001 (cité : Responsabilité)
VERCKEN, G.	Responsabilité sur Internet, Revue Nov'Art, n° 21, octobre 1996 - janvier 1997, p. 34
VIVANT, Michel	La responsabilité des intermédiaires de l'Internet, JCP G 1999 I 180, p. 2021ss (cité : Responsabilité)
Vivre Le Net	Le créateur d'un forum peut être tenu responsable de son contenu, News Vivre Le Net, 11 mars 2002
Vivre Le Net	Defense-consommateur devra indemniser le Père-Noël(.fr), News Vivre Le Net, 29 mai 2002
WALDNER, Uwe	Zivilrechtliche Probleme der Internet-Nutzung, Hannover 2001 (cité : Internet-Nutzung)
WARDENBACH, Annecke	Nazi-Propaganda : Forscher suchen Filter, WDR, 14.02.02
WEBER, Rolf H.	Zivilrechtliche Haftung auf dem Information Highway, in Reto M. HILTY, Information Highway, Bern 1996, p. 531ss (cité : Haftung)
WEBER, Rolf H.	E-Commerce und Recht, Zürich 2001 (cité : E-Commerce)
WÉRY, Etienne	Internet hors-la-loi ? Description et introduction à la responsabilité des acteurs du réseau, Journal des Tribunaux (Bruxelles), n° 5846, 7 juin 1997
WÉRY, Etienne	Responsabilité des fournisseurs d'accès : la liste noire continue, http://www.droit-technologie.org, 12 avril 1999
WÉRY, Etienne	Affaire Skynet : la cour d'appel allège la responsabilité des hébergeurs, http://www.droit-technologie.org, 5 mars 2001 (cité : Skynet)

WÉRY, Etienne	La directive e-commerce devrait être transposée pour aujourd'hui au plus tard !, http://www.droit-technologie.org, 17 janvier 2002
WÉRY, Etienne	Surfer anonymement devient illégal en Belgique, http://www.droit-technologie.org, 18 mars 2002
WÉRY, Etienne	Le Parlement européen s'oppose au filtrage systématique du web comme moyen de protection des mineurs, http://www.droit-technologie.org, 15 avril 2002
WIDMER, Pierre / WESSNER, Pierre	Révision et unification du droit de la responsabilité civile, rapport explicatif, 1999 (cité : Rapport)
WIDMER, Pierre / WESSNER, Pierre	Révision et unification du droit de la responsabilité civile, commentaire abrégé, 1999
WIDMER, Ursula / BÄHLER, Konrad	Rechtsfragen beim Electronic Commerce, Sichere Geschäftstransaktionen im Internet, 2e éd., Zürich 2000