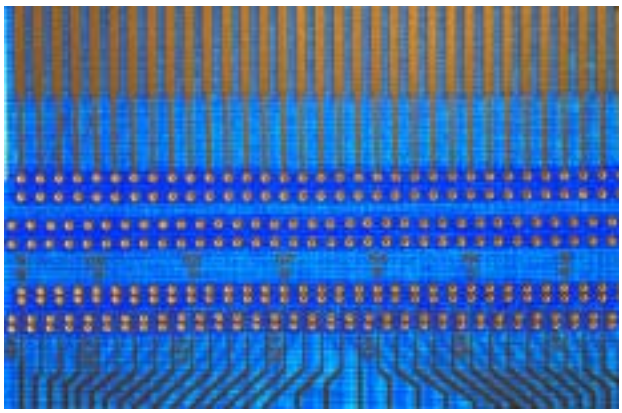
Cyber-



criminalité

Rapport de la commission d'experts

« Cybercriminalité »

Département fédéral de justice et police
Berne, juin 2003

Table des matières

Liste des abréviations et glossaire

a. v.	ancienne version
access provider	fournisseur ou prestataire d'accès
AP	avant-projet
ASDI	Annuaire suisse du droit international ((*manque dans liste version allemande* ; voir texte p. 73 : SJIR (Schw. Jahrbuch für Intern. Recht))
ATF	Arrêt du Tribunal fédéral
BGBl	Bundesgesetzblatt (Journal officiel de la République fédérale d'Allemagne)
BGH	Bundesgerichtshof (Cour fédérale suprême de la République fédérale d'Allemagne)
Bibl.	bibliographie du présent rapport (p.13))
BO	Bulletin officiel de l'Assemblée fédérale
browser	logiciel de navigation, navigateur : programme permettant de visualiser les contenus multimédias, reliés entre eux par les hyperliens (renvois électroniques).
Bull. sién.	Bulletin sténographique de l'Assemblée fédérale
cache	mémoire d'accès rapide aux données les plus fréquemment utilisées provenant d'une autre mémoire (stockage temporaire de données). Ces mémoires-caches sont utilisées sur Internet par les fournisseurs d'accès qui permettent ainsi à leurs clients d'accéder plus rapidement à des sites très demandés.
CC	Code civil suisse, RS 210
CEDH	Convention européenne des droits de l'homme, RS 0.101
ch. marg.	chiffre marginal
chat	discussion en ligne (texte, son, image) entre utilisateurs d'Internet
client	ordinateur participant à un réseau
CO	Code des obligations (RS 220)
content provider	fournisseur de contenus
CP	Code pénal suisse
CPP	code de procédure pénale
Cst.	Constitution fédérale, RS 101
DETEC	Département fédéral de l'environnement, des transports, de l'énergie et de la communication
DFJP	Département fédéral de justice et police
DNS	*domain name system (sy*stème d'adressage par domaine) : l '« annuaire » d'Internet traduit les noms symboliques des hôtes de l'Internet, par ex. www.bj.admin.ch, en adresse numérique.
download	téléchargement de données d'Internet vers son propre PC

e-com	commerce électronique ou commerce en ligne : possibilité d'acheter par l'intermédiaire d'Internet
EGG	Elektronisches Geschäftsverkehrgesetz (loi allemande sur le commerce électronique)
e-mail	courrier électronique
FF	Feuille fédérale
file sharing	partage de fichiers par plusieurs programmes : service d'Internet permettant aux utilisateurs finaux de mettre à la disposition d'autres utilisateurs d'Internet certaines données de leur disque dur (par ex. musique) pour que ceux-ci puissent les télécharger.
fournisseur d'hébergement (de sites)	prestataire mettant une capacité de mémoire à la disposition de ses clients sur un serveur.
FTP, ftp	*file transfer protocol* (protocole de transfert de fichier ou protocole FTP) : ensemble de règles permettant l'échange de données entre le client et le fournisseur d'accès.
GA	Goltdammer's Archiv für Strafrecht (Archives Goltdammer de droit pénal, Allemagne)
HTTP	*hypertext transfer protocol* (protocole de transfert d'hypertexte) : protocole utilisé sur la Toile, permettant au *navigateur* d'accéder à des sites.
IP	*internet protocol* (protocole Internet) : protocole à la base d'Internet permettant de contrôler au niveau mondial l'échange de données indépendamment du moyen physique de transmission utilisé.
ISP	*internet service provider* : prestataire de services Internet, c'est-à-dire fournisseur d'accès à Internet
JAAC	Jurisprudence administrative des autorités de la Confédération
JO	Journal officiel (Union européenne)
JO	Journal officiel de la République française
JZ	Juristenzeitung (Revue de jurisprudence, Allemagne)
LA	Loi fédérale du 21 décembre 1948 sur l'aviation, RS 748.0
LAN	*local area network* : réseau local clos d'une entreprise
LBI	Loi fédérale du 25 juin 1954 sur les brevets, RS 232.14
LCD	Loi fédérale du 19 décembre 1986 contre la concurrence déloyale, RS 241
LCR	Loi fédérale du 19 décembre 1958 sur la circulation routière, RS 741.01
LDA	Loi fédérale du 9 octobre 1992 sur le droit d'auteur, RS 231.1
LDIP	Loi fédérale du 18 décembre 1997 sur le droit international privé, RS 291
Lien	renvoi dans une page web à une autre page web ou à des contenus multimédias (musique, vidéo).
loc. cit.	*loco citato*, passage cité
LPM	Loi fédérale du 28 août 1992 sur la protection des marques, RS 232.11

LRTV	Loi fédérale du 21 juin 1991 sur la radio et la télévision, RS 784.40
LSCPT	Loi fédérale du 6 octobre 2000 sur la surveillance de la correspondance par poste et télécommunication, RS 780.1
LStup	Loi fédérale du 3 octobre 1951 sur les stupéfiants (RS 812.121)
LTC	Loi du 30 avril 1997 sur les communications RS 784.10
LTPF	Loi fédérale du 4 octobre 2002 sur le Tribunal pénal fédéral, RS 173.71 ((*manque en allemand*, voir p. 135 : Bundesgesetz über das Bundesstrafgericht / Strafgerichtgesetz SGG)
MMS	*multimedia messaging service* : service de messagerie multimédia permettant la transmission de données multimédias entre téléphones mobiles (enrichissant les SMS par son et images).
monitoring	contrôle et surveillance de l'offre Internet par un organe d'Etat.
n.	note
n.	note
n. v.	nouvelle version
network provider	fournisseur de réseau
newsgroup	forum de discussion sur le réseau Internet
op. cit.	*opere citato*, ouvrage cité
OST	Ordonnance du 31 octobre 2001 sur les services de télécommunication, RS 784.101.1
P2P ou *peer-to-peer*	protocole permettant l'échange direct d'informations entre des utilisateurs finaux (voir *file sharing*/partage de fichiers) sans instance de transmission centrale.
PJA	Pratique juridique actuelle
PPF	Loi fédérale du 15 juin 1934 sur la procédure pénale, RS 312.0 ((*manque dans la liste version allemande* = BStP voir p. 135))
protocole	convention composée de règles, de formats et d'indications techniques dont l'application permet le transport des données d'un ordinateur à l'autre.
proxy	les *proxies* ou, serveurs mandataires, sont des serveurs fonctionnant entre les réseaux locaux (LAN) et Internet. Evitant à chaque serveur d'envoyer ses propres requêtes, le serveur *proxy* envoie et reçoit des « paquets » de données à partir d'Internet et vers Internet. Les *proxies* permettent d'accélérer les échanges car ils jouent le rôle de *cache (espace de mémoire où sont enregistrées temporairement des données)*. Ils peuvent aussi être utilisés pour sécuriser ou contrôler l'accès au réseau dans la mesure où ils ne transmettent pas plus loin certaines requêtes en qualité de « pare-feu ».
RDS	Revue de droit suisse
routeur	dispositif qui assure la liaison entre des sections de réseaux et permet de transmettre des paquets de données via d'autres routeurs en établissant les itinéraires de

	transmission optimaux.
RPS	Revue pénale suisse
RS	Recueil systématique du droit fédéral
RSJ	Revue suisse de jurisprudence
serveur	ordinateur qui, dans un réseau, met ses données à la disposition des autres ordinateurs participant au réseau.
SMS	*short message service* : bref message envoyé par téléphone portable
TCP	*transmission control protocol :* règles de transmission de données de la couche transport assurant la sécurité du transfert de données sur Internet
TDG	Teledienstegesetz (loi allemande sur l'utilisation des téléservices)
URL	*universal resource locator* : adressage uniforme d'un document sur Internet avec indication du protocole d'accès à utiliser (accès avec FTP) : par ex. http://www.ibm.com (accès http) ou ftp://ftp.linksys.com (accès ftp).
WAP	*wireless access protocol* : standard (ou norme) du domaine de la téléphonie mobile permettant d'accéder à Internet à partir d'un téléphone portable. Un langage spécial (WML) a été mis au point pour permettre d'afficher des informations sur un petit écran de téléphone portable.
Web	réseau (abréviation de World Wide Web)
World Wide Web	littéralement « toile d'araignée mondiale », ou réseau mondial des sites utilisant le protocole http ; en français, la « Toile » (ou le « web »).
WWW	World Wide Web
ZStrW	Zeitschrift für die gesamte Strafrechtswissenschaft (revue allemande de droit pénal)

Bibliographie

La liste des ouvrages ci-dessous ne contient que les données bibliographiques ou la localisation des sources citées à plusieurs reprises dans le présent rapport. Dans un esprit de simplification, ces ouvrages sont cités sous leur forme abrégée (par ex. HÄFELIN/HALLER) accompagnée de l'indication « Bibl. » (Bibliographie).

CASSANI	Ursula Cassani, Die Anwendbarkeit des schweizerischen Strafrechts auf internationale Wirtschaftsdelikte (Art. 3 - 7 StGB), RPS 114 (1996), p. 237 ss
GUTACHTEN BJ	Bundesamt für Justiz, Gutachten vom 24. Dezember 1999 zur Frage der strafrechtlichen Verantwortlichkeit von Internet-Access-Providern gemäss Artikel 27 und 322bis StGB, JAAC 64.75
HÄFELIN/HALLER	Ulrich Häfelin/Walter Haller Schweizerisches Bundesstaatsrecht 5^{e} édition, Zurich 2001
HÄFELIN/MÜLLER	Ulrich Häfelin/Georg Müller, Allgemeines Verwaltungsrecht 4^{e} édition, Zurich 2002
HEINE	Günter Heine, Strafrechtlicher Schutz der Verbraucher vor Täuschungen und wettbewerbswidrigen Angeboten bei E-Commerce, in: Koller/Muralt Müller (Editeurs), Tagung 2001 für Informatikrecht vom 18./19. September 2001, Berne 2002
HILGENDORF	Eric Hilgendorf, Die Neuen Medien und das Strafrecht, ZStrW 2001, p. 650 ss
HÖSLI	Peter Hösli, Möglichkeiten und Grenzen der Verfahrensbeschleunigung durch informell-kooperatives Verwaltungshandeln, thèse, Zurich 2002
KOCH	Arnd Koch, Nationales Strafrecht und globale Internet-Kriminalität, GA 2002, p. 703 ss
LEHLE	Thomas Lehle, Der Erfolgsbegriff und die deutsche Strafrechtszuständigkeit im Internet, Constance 1999
MOREILLON/DE COURTEN	Laurent Moreillon/Frédérique de Courten, La responsabilité pénale du Cyber-Provider (fournisseur), Anwaltsrevue/Revue de l'avocat 8/2002, p. 12 ss
MÜLLER, GRUNDRECHTE	Jörg Paul Müller Grundrechte in der Schweiz, im Rahmen der Bundesverfassung von 1999, der UNO-Pakte und der EMRK 3^{e} édition, Berne 1999
NIGGLI, INTERNET-KRIMINALITÄT	Marcel Alexander Niggli Internet-Kriminalität Anwaltsrevue/Revue de l'avocat, 8/2002, p. 6 s.

NIGGLI, NATIONALES STRAFRECHT	Marcel Alexander Niggli, Nationales Strafrecht vs. globales Internet, in: Weber/Hilty/Auf der Maur (Editeurs), Geschäftsplattform Internet II, Zurich 2001, p. 144 ss
NIGGLI, RASSENDISKRIMINIERUNG	Marcel Alexander Niggli, Rassendiskriminierung, Kommentar, Zurich 1996
NIGGLI/SCHWARZENEGGER	Marcel Alexander Niggli/Christian Schwarzenegger, Strafbare Handlungen im Internet, RSJ 98 (2002), p. 61 ss
PFENNINGER	Hanspeter Pfenninger, Rechtliche Aspekte des informellen Verwaltungshandelns, thèse, Fribourg 1996
POPP	Peter Popp, in: Niggli/Wiprächtiger, Basler Kommentar zu Art. 7 STGB, Bâle 2003
REHBERG/DONATSCH	Jörg Rehberg/Andreas Donatsch, Strafrecht, Verbrechenslehre, 7e édition, Zurich 2001
DIRECTIVE	Directive européenne sur le commerce électronique. Directive 2000/31/CE du Parlement européen et du Conseil 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 (« directive sur le commerce électronique »). JO n° L. 178 du 17.7.2000, p. 1 à 16 http://europa.eu.int/eur-lex/pri/de/oj/dat/2000/l_178/l_17820000717de00010016.pdf
RIKLIN	Franz Riklin, Strafrecht, Allgemeiner Teil, 2e édition, Zurich 2002
RIKLIN/STRATENWERTH	Franz Riklin/Günter Stratenwerth, Medienstrafrecht/Kaskadenhaftung, in: Niggli/Riklin/Stratenwerth (Hrsg.), Die strafrechtliche Verantwortlichkeit von Internet Providern, medialex, édition spéciale 2000, p. 13 ss
SATZGER	Helmut Satzger Strafrechtliche Verantwortlichkeit von Zugangsvermittlern, Eine Untersuchung der Verantwortlichkeit für rechtswidrige Inhalte im Internet vor dem Hintergrund der neuen E-Commerce-Richtlinie der EG, Computer und Recht, 2/2001, p. 109 ss
SCHMID	Niklaus Schmid, in Schmid (Editeur), Einziehung, Organisiertes Verbrechen, Geldwäscherei, Kommentar, vol. 1, Zurich 1998
SCHULTZ, PRESSEDELIKT	Hans Schultz, Die unerlaubte Veröffentlichung - ein Pressedelikt, RPS 108 (1991) p. 273 ss
SCHWARZENEGGER, ABSTRAKTE GEFAHR	Christian Schwarzenegger, Abstrakte Gefahr als Erfolg im Strafanwendungsrecht - Ein Leading case grenzüberschreitenden Internetdelikten, sic! 2001, p. 240 ss
SCHWARZENEGGER, CRIMES	Christian Schwarzenegger Computer Crimes in Cyberspace, A comparative analysis of criminal law in Germany, Switzerland and Northern Europe

	Jusletter 14 octobre 2002 www.weblaw.ch/jusletter/jsp?ArticleNr=1957
SCHWARZENEGGER, E-COMMERCE	Christian Schwarzenegger, E-Commerce - Die strafrechtliche Dimension, in: Arter/Jörg (Editeurs), Internet-Recht und Electronic Commerce Law, Lachen et St-Gall 2001
SCHWARZENEGGER, GELTUNGSBEREICH	Christian Schwarzenegger, Der räumliche Geltungsbereich des Strafrechts im Internet, RPS 118 (2000), p. 109 ss
SEMKEN	Hartmut Semken (Un-)Möglichkeiten der Inhaltskontrolle mit technischen Mitteln im Internet, in: Cassani/Maag/Niggli (Editeurs), Medien, Kriminalität und Justiz, Schweizerische Arbeitsgruppe für Kriminologie, vol. 19. Choire/Zurich 2001, p. 249 ss
TRECHSEL	Stefan Trechsel, Schweizerisches Strafgesetzbuch, Kurzkommentar, 2e édition, Zurich 1997
TRECHSEL/NOLL	Stefan Trechsel/Peter Noll Schweizerisches Strafrecht, Allgemeiner Teil I, Allgemeine Voraussetzungen der Strafbarkeit, 5e édition, Zurich 1998
TSCHANNEN/ZIMMERLI/KIENER	Pierre Tschannen/Ulrich Zimmerli/Regina Kiener, Allgemeines Verwaltungsrecht, Berne 2000
WEBER	Rolf H. Weber E-Commerce und Recht, Rechtliche Rahmenbedingungen elektronischer Geschäftsformen, Zurich 2001
WIDMER/BÄHLER	Ursula Widmer/Konrad Bähler, Rechtsfragen beim Electronic Commerce, Sichere Geschäftstransaktionen im Internet, 2e édition, Zurich 2000
ZELLER	Franz Zeller, in: Niggli/Wiprächtiger, Basler Kommentar, zu Art. 27 STGB, Bâle 2003

Le flou juridique entourant la responsabilité pénale des fournisseurs d'accès Internet ainsi que diverses interventions parlementaires ont conduit à la création de la commission d'experts « Cybercriminalité ». Le présent rapport a certes pour objectif premier de clarifier certains points, mais aussi il entend formuler des recommandations ainsi que des propositions au niveau politique.

1. Introduction

1.1 Historique

1.11 Le projet-pilote des « flics du Net »

En janvier 1998, l'Office fédéral de la police (OFP) mettait sur pied un projet-pilote de surveillance d'Internet (monitoring Internet) : deux collaborateurs faisaient alors office de « flics du Net » et patrouillaient, pour ainsi dire, parmi les « offres » paraissant sur le réseau. Ils avaient néanmoins pour mission principale de recevoir et de traiter les communications du public sur des contenus Internet pénalement répréhensibles. Ce projet permit de constater que divers sites Internet présentaient des contenus susceptibles de contrevenir à l'art. 261bis du Code pénal (CP), Discrimination raciale.

1.12 La recommandation de blocage adressée aux fournisseurs d'accès

En juillet de la même année, la Police fédérale envoyait une circulaire aux fournisseurs de services Internet en Suisse (*Internet Service Providers*) leur demandant de tester le blocage des sites incriminés. Elle attirait notamment leur attention sur le fait que faciliter l'accès à de tels sites pouvait être qualifié de complicité à une infraction principale. Cette circulaire déclencha un tollé général parmi les fournisseurs de sites. Ils mettaient notamment en doute la faisabilité technique des blocages Internet et sa base légale. Cette réaction fut à l'origine de la mise sur pied d'un groupe de contact, composé de représentants des fournisseurs d'accès suisses et de représentants des offices fédéraux concernés. La tâche première de ce groupe était d'examiner en détail les questions techniques et juridiques qui se posaient en l'occurrence.

1.13 Un avis de droit...

Etant donné les réactions divergentes du groupe de contact à la première étude sur la question des blocages Internet, la Police fédérale demanda à l'Office fédéral de la justice (OFJ) d'établir un avis de droit sur la responsabilité pénale des fournisseurs d'accès Internet quant aux contenus illégaux.

Dans son avis de droit du 24 décembre 1999 [1], l'OFJ approuva fondamentalement la responsabilité subsidiaire du pur fournisseur d'accès selon le droit pénal des médias, à condition cependant que le fournisseur ait été clairement rendu attentif au contenu illégal par une autorité de poursuite pénale. En outre, l'avis précisait que pour les cas dans lesquels le droit pénal des médias n'est pas applicable, les fournisseurs peuvent être punis comme complice à l'infraction principale.

Sur la base des considérations figurant dans l'avis de droit de l'OFJ, la Police fédérale précisa alors sa position dans un avis rendu public [2].

1.14 ... et un second avis de droit

L'association Verband Inside Telecom (VIT), en qualité de représentante de la branche, rejeta les conclusions figurant dans l'avis de droit de l'OFJ comme étant inexactes et mandata les professeurs Marcel A. Niggli, Franz Riklin et Günter Stratenwerth d'examiner tout particulièrement la question de la responsabilité pénale des fournisseurs d'accès.

Les trois professeurs mandatés ont remis leur avis le 2 octobre 2000 [3]. Leurs conclusions sur la question centrale de la responsabilité pénale des purs fournisseurs d'accès contredisaient sur l'essentiel celles de l'OFJ. En outre, ils soulignaient expressément le manque de clarté de la situation juridique et s'appuyaient sur cette considération pour demander une révision du Code pénal.

1.2 Contexte politique

1.21 La motion Pfisterer

Le 14 décembre 2000, le conseiller aux Etats Thomas Pfisterer déposait avec 27 co-signataires la motion suivante :

> 1. Le Conseil fédéral est chargé de présenter rapidement et en première priorité une réglementation pénale - le cas échéant sous forme de dispositions isolées - satisfaisant aux critères de la sécurité juridique et de la praticabilité, et autant que possible coordonnée sur le plan international, afin de protéger le réseau Internet dans l'intérêt de l'économie et de la population.

---

[1] En allemand uniquement, in JAAC 64.75.

[2] Cf. http://internet.bap.admin.ch/d/archiv/berichte/weitere/2000-05-15-f-internet-isp.pdf

[3] Reproduit dans medialex, numéro spécial 1/2000.

2. Au besoin, il proposera d'autres modifications du droit à titre subsidiaire.

Dans son développement, le motionnaire soulignait les particularités techniques et juridiques des réseaux informatiques tel que le réseau Internet et en déduisait l'urgence de légiférer en la matière. Il recommandait par ailleurs une harmonisation avec la directive de l'Union européenne sur le commerce électronique. Enfin, le motionnaire présentait une proposition de législation prévoyant entre autres des compléments aux articles 27 et 340 CP (cf. libellé en annexe [A])

Dans sa prise de position, le *Conseil fédéral* soulignait que l'on ne pouvait pas dire qu'Internet évoluait dans un no man's land juridique même sans disposition y relative. Il s'appuyait notamment à ce propos sur l'avis de droit de l'Office fédéral de la justice. Par ailleurs, il réitérait sa volonté, déjà exprimée en 1996, d'harmoniser au niveau international la législation relative à Internet et estimait que la proposition de réglementation de l'auteur de la motion constituait dans cette optique un chemin en principe possible. Il mettait enfin l'accent sur la nécessité de mettre en place une politique criminelle cohérente et une réglementation ad hoc. Même s'il ne se considérait pas lié par le développement de la motion, le Conseil fédéral se déclarait prêt à *accepter* la motion.

Le *Conseil des Etats* a adopté la motion Pfisterer le 6 mars 2001 [4] et le *Conseil national* le 20 septembre 2001 [5].

1.22 Autres interventions parlementaires

Le 26 septembre 2002, la conseillère nationale *Regine Aeppli* déposait une initiative parlementaire rédigée sous la forme d'une demande conçue en termes généraux (02.452) [6]. Elle était ainsi *libellée*:

> Dans le but de coordonner et d'accroître l'efficacité de la poursuite pénale dans le domaine de la cybercriminalité, et notamment de la pédopornographie, une compétence fédérale semblable à celle que prévoit l'article 340bis du Code pénal en matière de crime organisé et de criminalité économique doit être créée.

Dans son développement, l'auteur de l'initiative rappelait la dissolution de la cellule de surveillance du réseau Internet par le Conseil fédéral à la fin de l'année 1999 et les difficultés de coopération avec les cantons. Elle soulignait l'augmentation des cas de cybercriminalité, particulièrement dans le domaine de la pornographie enfantine et de la pédophilie, et estimait « inacceptable » la « course aux compétences » qui durait depuis des années. Elle précisait en outre que la Convention du Conseil de l'Europe signée par la Suisse sur la cybercriminalité requérait la création d'une cellule d'investigation.

---

[4] BO 2001 p. 27 s.

[5] BO 2001 n. 1087 ss.

[6] Cf. la motion Aeppli Wartmann (01.3196) du 23 mars 2001 (Améliorer la procédure de lutte contre la cybercriminalité), qui va dans le même sens que l'initiative parlementaire de 2002.

1.3 La commission d'experts

1.31 Constitution et mandat

Dans le contexte de la motion Pfisterer (cf. ci-dessus ch. 1.21), et d'une manière générale dans le but d'examiner la situation dans le domaine de l'exploitation abusive des possibilités offertes par Internet, le DFJP a institué le 22 novembre 2001 une commission d'experts « Cybercriminalité » et lui a donné le *mandat* suivant :

> La commission d'experts « Cybercriminalité » examine quelles mesures d'ordre juridique, organisationnel et technique peuvent être appliquées pour prévenir et sanctionner les infractions commises par le biais d'Internet. Elle devra en particulier se pencher sur le problème de la réglementation de la responsabilité pénale dans le domaine d'Internet. De plus, si cela se révèle opportun, elle proposera également des règles relatives à la responsabilité civile et à la protection de la propriété intellectuelle. Ses travaux devraient déboucher sur un projet de loi prêt à être mis en consultation.

Le DFJP a demandé à la commission de rendre son rapport et l'avant-projet à la fin de 2003.

1.32 Composition

La commission d'experts était placée sous la *présidence* de Peter Müller, docteur en droit, vice-directeur de l'Office fédéral de la justice [7]. Elle se composait comme suit :

- Felix Bommer, docteur en droit, professeur assistant de droit pénal à l'Université de Lucerne
- Hans-Ulrich Bühler, avocat, Office fédéral de la police
- Lukas Bühler, docteur en droit, Institut fédéral de la Propriété Intellectuelle
- Maître Maurice Harari, avocat, Genève [8]
- Matthias Kaiserswerth, professeur, docteur en ingénierie, Zurich
- Laurent Moreillon, docteur en droit, professeur associé de droit pénal à l'Université de Lausanne
- Marcel Alexander Niggli, docteur en droit, professeur de droit pénal à l'Université de Fribourg
- Isabelle Romy, avocate, docteur en droit, professeure associée à l'Université de Fribourg
- Christian Schwarzenegger, docteur en droit, professeur assistant de droit pénal à l'Université de Zurich ; *vice-président de la commission d'experts*
- Bernhard Waldmann, professeur assistant de droit public à l'Université de Fribourg

[7] Depuis le 1er février 2003, secrétaire général du Département fédéral des affaires étrangères (DFAE).
[8] Jusqu'à octobre 2002.

- Ursula Widmer, docteur en droit, avocate et directrice du Verband Inside Telecom (VIT), Berne
- Franz Zeller, docteur en droit, Office fédéral de la communication

Le *secrétariat* de la commission a été assuré par Mme Dorrit Schleiminger (jusqu'à septembre 2002), Peter Ullrich (à partir d'octobre 2002, coordination du rapport), Grace Schild Trappe (depuis février 2003) ainsi que Stéphane Blanc et Patrick Gruber (procès-verbalistes), tous collaborateurs de l'Office fédéral de la justice.

1.33 Méthode de travail

De février 2002 à mars 2003, la commission a tenu en tout dix séances d'une demi-journée ou d'une journée entière.

Elle a invité à quelques séances Monsieur Philipp Kronig, lic. en droit, MPA, chef du Service national de coordination de la lutte contre la criminalité sur Internet (SCOCI) de l'Office fédéral de la police, en qualité d'expert extérieur.

Plusieurs chapitres du rapport final sont directement inspirés des travaux des membres de la commission d'experts :

- **Chapitre 2** (La communication sur les réseaux) : Ch. Schwarzenegger
- **Chapitre 3** (Les bases techniques) : M. Kaiserswerth
- **Chapitre 5** (Les conditions-cadres de droit constitutionnel) : B. Waldmann
- **Chapitre 6** (La cybercriminalité selon le droit pénal actuel) : F. Bommer, M. A. Niggli, Ch. Schwarzenegger
- **Chapitre 7** (Les ressources du droit administratif) : B. Waldmann
- **Chapitre 8** (La responsabilité civile): L. Bühler
- **Chapitre 9** (Le projet de loi) : F. Bommer, L. Moreillon, M. A. Niggli, Ch. Schwarzenegger
- **Chapitre 10** (La législation parallèle et autres tâches législatives): F. Bommer, M. A. Niggli, Ch. Schwarzenegger, H.U. Bühler, U. Widmer

1.4 Les questions essentielles

Formulée de manière très générale, la question à laquelle la commission avait à répondre était la suivante :

> Comment peut-on et doit-on lutter contre les contenus illégaux sur Internet, qui est responsable de ces contenus et à quel niveau ?

Il est possible de subdiviser cette question générale en plusieurs *questions partielles* :

- Comment *contrôler du point de vue technique* les contenus circulant sur les réseaux de communication, le cas échéant comment les *bloquer* ou les *éliminer*? (Cf. *chapitre 3* du présent rapport)

- A qui imputer la *responsabilité pénale* des violations du droit sur les réseaux de communication en Suisse et à quelles conditions ? (Cf. *chapitre 6, ch. 6.1 - 6.3 ; chapitre 9*).
- Dans quelle mesure est-il possible de poursuivre et réprimer pénalement en Suisse *les violations du droit commises depuis l'étranger* sur les réseaux de communication ? (Cf. *chapitre 6, ch. 6.4; chapitre 9*).
- La compétence de la poursuite pénale des violations du droit sur les réseaux de communication doit-elle être attribuée aux *cantons* ou à la *Confédération* ? (Cf. *chapitre 6, ch. 6.5; chapitre 9, ch. 9.4*).
- Le *droit administratif* offre-t-il des instruments permettant d'empêcher les violations du droit sur les réseaux de communication ? (Cf. *chapitre 7*).

Qui répond de quelle manière *en droit civi*l des dommages découlant des violations du droit sur les réseaux de communication et pour les dommages relatifs au blocage ou à l'élimination des contenus illégaux de réseau ? (Cf. *chapitre 8*).

Le nombre des services de communication et de leurs utilisateurs a fortement augmenté au cours des dernières années. Cette évolution n'a pas été sans influence sur la société. Avec pour corollaire une augmentation de la criminalité liée à Internet.

2. Communication sur les réseaux : faits et chiffres

2.1 Evolution des technologies de l'information et mutation sociale

L'évolution extrêmement rapide des technologies de l'information et de la communication au cours des vingt dernières années a influencé et modifié profondément les habitudes de vie et de communication des individus.

2.11 La nouvelle diversité des services de communication

Il n'y a pas si longtemps encore, lorsqu'on était en retard à un rendez-vous, il fallait chercher une cabine téléphonique et avoir la monnaie nécessaire pour pouvoir prévenir. Si la personne censée attendre était en route, on ne pouvait pas la joindre. Aujourd'hui, il suffit de l'appeler sur son *téléphone portable* ou de lui envoyer un *SMS* (*Short Message Service*) sur ce même *portable* (cf. l'encadré ci-dessous).

Véritable explosion du nombre des SMS

En 2001, les fournisseurs de téléphonie mobile ont enregistré un taux de progression des SMS allant jusqu'à 50 %. Ainsi, chez Orange, chaque client a reçu 1,8 SMS par jour. Swisscom, avec 7 millions de SMS par jour, présente une évolution similaire : chaque client Swisscom a reçu 2 SMS par jour. Chez Sunrise, les chiffres du troisième trimestre 2001 ont enregistré une progression de 66,7 % par rapport à la même période de l'année précédente. L'entreprise estime que chaque client reçoit par jour environ 1,8 à 2 SMS [9].

De même, lorsqu'un lecteur voulait écrire à la rédaction d'un journal, il devait poster une véritable lettre, au moins un jour avant la clôture de la rédaction. Aujourd'hui, il lui suffit d'envoyer un *e-mail* (courrier électronique), accompagné éventuellement d'un texte en fichier joint, le tout parvenant généralement à la rédaction en quelques secondes.

On était à la recherche d'un nouveau travail ou d'un appartement ? Il fallait alors attendre l'édition adéquate d'un ou de plusieurs journaux pour étudier les annonces. Aujourd'hui, on peut interroger à toute heure les *banques de données sur Internet* et établir les premiers contacts par courrier électronique.

[9] TAGES-ANZEIGER, SMS-Boom ungebrochen, 22.1.2002, p. 12.

Quant aux actualités, on peut pratiquement les suivre en direct sur les *sites web des diverses entreprises médiatiques*.

Nombre de tous les sites actifs [10] (au niveau mondial)	
Août 1995	18 957
Décembre 1996	603 367
Décembre 1997	1 681 868
Décembre 1998	3 689 227
Décembre 1999	9 560 866
Décembre 2000	25 675 581
Décembre 2001	36 276 252
Décembre 2002	35 543 105

Autrefois, lorsqu'on avait envie d'échanger des idées avec les autres membres d'un groupe, il fallait par exemple assister à des assemblées, à des rencontres ou encore se retrouver pour aller boire un verre. Aujourd'hui, on peut aller discuter ou bavarder en ligne sur Internet, dans des *chat rooms*. On peut y échanger en ligne et de manière anonyme idées ou nouvelles brèves. Pour les utilisateurs d'Internet possédant un accès rapide au réseau, il existe aussi la possibilité du *courrier vocal* (*voice mail*) ou de la *conférence vidéo*.

2.12 Un monde sans frontière grâce à Internet

Les services d'Internet décrit ci-dessus ont aussi contribué à la disparition des frontières géographiques. En effet, on peut exploiter ou appeler des informations de tous les coins du monde à partir de chaque raccordement au réseau. Que ce soit à la maison ou au travail, de plus en plus de personnes disposent d'une connexion. En comparaison européenne, la Suisse est l'un des pays où la proportion de ménages possédant un accès Internet compte parmi les plus élevées (cf. les tableaux ci-dessous).

Nombre de personnes disposant d'un accès Internet à leur domicile (4e trimestre 2001) [11]

	Nombre de personnes (en millions)	Croissance en comparaison avec le 3e trimestre 2001 (en %)	Part de la population mondiale ayant accès à Internet selon les régions (en %)
Etats-Unis/Canada	191,7	6,1	39
Europe/Israël/Afr. Sud*	134,7	6,3	27
Extrême-Orient, Austra-lie, Nouv. Zélande**	110,1	5,8	22
Amérique latine***	20,7	0,7	4
Autres pays	41,0	5,1	8
Total	498,2		100

* Allemagne, Autriche, Belgique, Danemark, Espagne, Finlande, France, Grande-Bretagne, Irlande, Italie, Luxembourg, Norvège, Pays-Bas, Suède, Suisse; Israël; Afrique du Sud

[10] BBC NEWS, Internet starts to shrink, 2.1.2002, adresse Internet : http://news.bbc.co.uk/1/hi/sci/tech/1738496.stm (état : 31.3.2003); source : Netcraft.

[11] ACNIELSEN ERATINGS.COM, adresse Internet: www.eratings.com/news/2002/20020306.htm (état : 7.10.2002).

** Australie, Corée du Sud, Hongkong, Inde, Japon, Nouvelle-Zélande, Singapour, Taiwan
*** Argentine, Brésil, Mexique

Ménages possédant un accès Internet et part des ordinateurs avec accès Internet en Europe (4e trimestre 2001) [12]

	Ménages possédant un accès Internet (en %)	Part des ordinateurs dans les ménages privés possédant un accès Internet (en %)
Suède	57	87
Pays-Bas	52	82
Danemark	51	82
Norvège	47	78
Suisse	**43**	**78**
Finlande	42	81
Autriche	38	70
Grande-Bretagne	38	78
Allemagne	35	72
Italie	34	80
Belgique/Luxembourg	32	68
France	20	53
Espagne	18	48

2.13 De plus en plus d'utilisateurs d'Internet - en Suisse aussi

Depuis 1997, l'utilisation d'Internet en Suisse a fortement augmenté : cette année-là, seulement quelque 7 pour cent de la population avait recours *régulièrement*, c'est-à-dire plusieurs fois par semaine, au réseau Internet. Au début de 2002, ils étaient déjà 42 pour cent à faire partie de ce cercle restreint des utilisateurs (CRU). Toujours en 1997, seulement 15 pour cent de la population faisait partie du cercle plus large des utilisateurs (CLU), c'est-à-dire du groupe de personnes utilisant *de temps en temps* Internet. Depuis, ce groupe d'utilisateurs s'est accru pour atteindre le chiffre de 57 pour cent [13].

2.14 Trois facteurs déterminants : sexe, formation et âge

Au début de 2002, le taux d'utilisation d'Internet chez les *hommes* était sensiblement plus élevé que chez les femmes : 52 % contre à peine 33 %. Néanmoins, la part des *femmes* parmi les utilisateurs d'Internet présente une nette tendance à la hausse. En 1997, plus de 3 % des femmes faisaient partie du CRU, en 2000 elles étaient plus de 22 % et en 2002 33 %. Alors que le taux de l'utilisation d'Internet chez les femmes a augmenté de plus de dix fois entre 1997 et 2001, le même taux chez les hommes ne s'est multiplié que par cinq [14].

Le *niveau de formation* a une influence considérable sur l'utilisation d'Internet : plus il est élevé, plus fréquente est l'utilisation d'Internet. Ainsi, en 2002, 22 pour cent des

[12] ACNielsen eRatings.com, adresse Internet : www.eratings.com/news/2002/20020306.htm (état : 7.10.2002).
[13] http://www.statistik.admin.ch/stat_ch/ber20/indic-soc-info/ind30106d_1_synth.htm
[14] http://www.statistik.admin.ch/stat_ch/ber20/indic-soc-info/ind30106d_4_synth.htm

personnes qui n'ont fréquenté que l'école obligatoire se raccordent régulièrement à Internet. Parmi les personnes qui ont fréquenté l'école secondaire, le taux d'utilisation est de 35 pour cent. Et il est de plus de 58 pour cent chez les personnes qui ont un niveau de formation plus élevé, pour atteindre environ 71 pour cent chez celles qui ont fait des études universitaires [15].

L'*âge* est un autre indicateur important. Les personnes de plus de 50 ans présentent un taux d'utilisation d'Internet nettement plus bas que les personnes plus jeunes. Au début de l'année 2002, l'utilisation d'Internet est la plus élevée parmi les tranches d'âge de 14 à 19 ans et de 20 à 29 ans : respectivement 56 et 60 pour cent de ces groupes faisaient partie du groupe restreint des utilisateurs. Ils n'étaient que 20 pour cent chez les personnes de plus de 50 ans [16].

2.15 Internet : un média de tous les jours

Il y a encore trois ans, l'utilisation d'Internet était plus élevée sur le lieu de travail qu'à la maison. Dans l'intervalle, Internet est utilisé plus souvent *à la maison* qu'au *travail*. En 2002, environ 42 pour cent de la population a eu recours à Internet à la maison ; sur le lieu de travail, ce taux était de quelque 31 pour cent. L'accroissement de l'utilisation d'Internet dans le domaine privé montre qu'Internet est devenu un média de tous les jours [17].

Des différences dans l'utilisation d'Internet apparaissent également en Suisse selon la *région linguistique* : elle est plus élevée en *Suisse alémanique* (43 %) qu'en *Suisse romande* (41 %) et qu'en *Suisse italienne* (34 %) [18].

En 2002, l'aspect *communication* a constitué le *motif d'utilisation* le plus fréquent : la messagerie électronique (e-mail) a été citée par plus de 91 pour cent des utilisatrices et utilisateurs. L'utilisation de *moteurs de recherche* arrive en seconde position (71 %) et le recours à Internet *à des fins d'information* en troisième position (53 %), notamment pour la consultation des articles de journaux et de revues. Par contre, en 2002 toujours, seulement 14 % des utilisateurs d'Internet ont fait usage de la *possibilité d'effectuer des achats en ligne* [19].

---

[15] www.infosociety-stat.admin.ch

[16] http://www.statistik.admin.ch/stat_ch/ber20/indic-soc-info/ind30106f_5_synth.htm

[17] http://www.statistik.admin.ch/stat_ch/ber20/indic-soc-info/ind30106f_311_synth.htm

[18] http://www.statistik.admin.ch/stat_ch/ber20/indic-soc-info/ind30106f_6_synth.htm

[19] http://www.statistik.admin.ch/stat_ch/ber20/indic-soc-info/ind30106f_319_synth.htm. Cf. également à propos de tous ces thèmes MAJA HUBER/FLORENT COSANDEY /VOLKER TÄUBE, Indicateurs de la société de l'information, in Société de l'information en Suisse, Etat des lieux et perspectives, Neuchâtel 2002, 22; cet ouvrage comprend de nombreuses informations sur la diffusion des ordinateurs, des modems, des téléphones portables ainsi que sur leur utilisation par les particuliers, les entreprises et les pouvoirs publics.

2.2 Cybercriminalité

2.21 Délits traditionnels et nouvelles catégories de délits

La face cachée de l'évolution décrite au point 2.1 se fait de plus en plus présente : d'une part il est plus facile de commettre des délits « traditionnels » [20] grâce aux nouveaux moyens et réseaux de communication; de l'autre, l'informatique et les réseaux ont conduit à l'apparition de nouvelles formes de criminalité [21] (voir les exemples ci-dessous).

Exemples de délits « traditionnels »

- Représentations de la violence (art. 135 CP),
- Faux renseignements sur des entreprises commerciales (art. 152 CP),
- Manipulation de cours (art. 161bis CP),
- Délits contre l'honneur (art. 173 ss CP),
- Violation du domaine secret ou du domaine privé au moyen d'un appareil de prises de vue (art. 179^{quater} CP),
- Utilisation abusive d'une installation de communication (art. 179^{septies} CP),
- Pornographie (art. 197 CP),
- Désagréments causés par la confrontation à un acte d'ordre sexuel (art. 198 CP),
- Indications permettant de fabriquer, dissimuler et transporter des explosifs ou des gaz toxiques (art. 226 CP),
- Provocation publique au crime ou à la violence (art. 259 CP),
- Atteinte à la liberté de croyance et des cultes (art. 261 CP),
- Discrimination raciale (art. 261bis CP),
- Publication de débats officiels secrets (art. 293 CP),
- Diffusion ou copie d'une œuvre protégée par des droits d'auteur (art. 67 et 69 LDA),
- Méthodes déloyales de publicité et de vente et autres comportements illicites (art. 3 LCD en rel. avec l'art. 23 LCD).

Exemples de nouvelles formes de criminalité

- Soustraction de données (art. 143 CP),
- Accès indu à un système informatique (art. 143bis CP),
- Détérioration de données, y compris la fabrication et la diffusion de virus informatiques (art. 144bis CP),
- Utilisation frauduleuse d'un ordinateur (art. 147 CP),
- Obtention frauduleuse d'une prestation informatique (« vol de temps machine », art. 150 CP),
- Contrainte due à l'envoi de courriers électroniques non demandés ou en quantités énormes ou due à des attaques par « déni de service » (art. 181 CP).
- Grave préjudice porté aux réseaux de communication : entrave aux services d'intérêt général (art. 239, ch. 1, al. 1 CP).

[20] C'est-à-dire de délits qui existaient certes auparavant, mais pour lesquels les technologies de l'information et les réseaux de communication constituent des moyens extrêmement efficaces et commodes.

[21] Pour une vue d'ensemble des formes de cybercriminalité, voir WIDMER/BÄHLER (Bibl.), p. 292 ss; SCHWARZENEGGER, E-COMMERCE (Bibl.), p. 333 ss; WEBER, (Bibl.), p. 538 ss.

2.22 Augmentation générale de la cybercriminalité

Les quelques enquêtes empiriques effectuées dans le domaine ont souligné la forte augmentation de la cybercriminalité depuis 1990 [22]. Selon une récente statistique de la *National Consumers League* (Etats-Unis), les consommateurs communiquent chaque année un nombre croissant de cas d'escroquerie commis à l'aide Internet. Différent selon les secteurs d'activités, le risque d'être victime d'une escroquerie est le plus élevé sur les sites de ventes aux enchères en ligne (87 % des cas communiqués au cours du premier semestre 2002). Six autres pour cent des dommages présumés par escroquerie relèvent des ventes courantes de marchandises. Le préjudice de fortune moyen s'élève à 484 $ US [23].

La *Commission européenne* a présenté en 2001 un rapport évaluant les revenus de l'escroquerie à 600 millions d'euros pour l'année 2000, ce qui représente une augmentation de 50 % environ. Les paiements par Internet y occupent une place prépondérante [24].

En 2001, la diffusion des *virus informatiques* a également fait un véritable bond en avant. Ces programmes pernicieux, qui se répandent principalement par l'intermédiaire de fichiers joints (*attachments*) à des messages électroniques, mais aussi parfois par l'intermédiaire de sites web infectés, recèlent un potentiel de dommages considérables [25]. Selon les relevés des fabricants de programmes anti-virus, un message électronique sur 370 était infecté par un virus en 2001, alors qu'en 2000, on recensait un virus pour 700 messages et en 1999, un virus pour 1400 messages [26].

2.23 Les limites de la poursuite pénale en Suisse

En Suisse, seul un petit nombre de cas sont enregistrés par la police, et quelques-uns d'entre eux à peine se soldent par une condamnation (voir les tableaux ci-

---

[22] Cf. OFFICE FÉDÉRAL DE LA POLICE, LA « CYBERCRIMINALITÉ », La face cachée de la révolution de l'information », Berne 2001, disponible à l'adresse Internet : www.isps.ch/site/fichiers/171.pdf (état au 7.10.2002); SCHWARZENEGGER, CRIMES (Bibl.), n. 3 ss et 42 s.

[23] NATIONAL CONSUMERS LEAGUE (Editeur), 2002 Internet fraud statistics, à consulter à l'adresse Internet : www.fraud.org/02intstats.htm (état au 10.10.2002). La somme totale des dommages communiqués s'élevait en 2000 à 3 387 530 dollars, au premier semestre 2002 elle était déjà de 7 209 196 dollars. Ces données statistiques ne sont toutefois pas représentatives de la totalité des utilisateurs d'Internet aux Etats-Unis. Il est probable que tous les cas communiqués ne correspondent pas à une escroquerie au sens de l'art. 146 CP.

[24] Commission de l'Union européenne, Communication du 9.2.2001 sur la prévention de la fraude et de la contrefaçon des moyens de paiement autres que les espèces, COM/2001/0011, à consulter à l'adresse Internet suivante :
http://europa.eu.int/comm/internal_market/en/finances/payment/fraud/cardfraud.htm (état au 10.10.2002).

[25] Le virus nommé « I Love You » qui s'est répandu dans le monde entier en mai 2000 aurait, selon les estimations de la Swiss Re, provoqué des dommages de l'ordre de plus de 1 milliard de dollars en quelques heures à peine ; cf. SWISS RE, National catastrophes and man-made disasters in 2000, sigma n° 2/2001, p. 7. Selon d'autres sources, les dommages économiques s'élèveraient même à 17 milliards de dollars.

[26] TAGES-ANZEIGER, Von Würmern und tanzenden CEOs, 24 décembre 2001, p. 49 : « Das Jahr des Wurms ».

dessous) [27]. Du reste, les condamnations pour abus frauduleux d'une installation de traitement de données ne concernent qu'une part minime des délits informatiques. La plupart des cas portent sur des abus ordinaires par cartes de paiement.

Ces chiffres soulignent clairement que la poursuite pénale dans le domaine de la criminalité informatique et de la cybercriminalité est encore très en retard. Cela surtout en comparaison avec les dommages et les dangers qui sont par exemple liés au piratage informatique (*hacking*) ou à la diffusion des virus informatiques [28]. On constate des carences similaires dans le domaine de la pornographie dure et douce, de la discrimination raciale ainsi que du piratage de musique, de films et de logiciels.

Délits informatiques recensés par la police (Zurich, 1996-2000)

Année	**1996**	**1997**	**1998**	**1999**	**2000**
Soustraction de données (art. 143), accès indu à un système informatique (art. 143bis), détérioration de données (art. 144bis, ch. 1), fabrication, etc. de programmes dans le but d'endommager des données (art. 144bis, ch. 2)	8	38	11	19	40
Utilisation frauduleuse d'un ordinateur (art. 147)	786	1 162	'612	1 673	2 100

Source : KRISTA 1996-2000 (Statistique criminelle du canton de Zurich)

Condamnations pour délits informatiques (Suisse, 1995-2000)

Année	1995	1996	1997	1998	1999	2000
Soustraction de données (art. 143)	1	2	2	2	4	3
Accès indu à un système informatique (art. 143bis)	0	1	0	1	1	2
Détérioration de données (art. 144bis, ch. 1)	14	18	111	21	10	2
Fabrication, etc. de programmes dans le but d'endommager des données (art. 144bis, ch. 2)	1	0	2	2	1	3
Utilisation frauduleuse d'un ordinateur (art. 147)	52	223	372	393	416	422

Source : Office fédéral de la statistique, Statistique suisse des condamnations pénales 2002 (non publiée).

2.24 La criminalité est techniquement neutre

La téléphonie mobile est également un domaine où l'on constate des phénomènes similaires de criminalité (par ex. désagréments causés par la confrontation à un acte

[27] La situation est identique en Allemagne ; cf. SCHWARZENEGGER, CRIMES (Bibl.), n. 3 ss.

[28] Cf. également les résultats de l'enquête publiée dans KPMG (Editeur) : 2001 global e.fr@ud.survey, 2001 (sans indic. du lieu de publication), à consulter à l'adresse Internet : www.kpmg.de/library/surveys/ (état au 9.10.2002).

d'ordre sexuel, atteinte à l'honneur par SMS, *flooding* par SMS - à savoir inonder une connexion de SMS dans le but de la gêner ou de la bloquer -, etc.) [29]. Suite à la mutation, pratiquement achevée, d'un simple moyen de communication oral en un réseau multifonctionnel d'échange de données numériques par ondes radio, permettant l'exécution d'un nombre de services de plus en plus grand grâce à de nouvelles capacités de transmission de données à larges bandes (nouvelles WAP, *chat* sur portable, jeux sur portable, transfert de données images, SMS, messagerie électronique), les possibilités d'utilisation criminelle se cumulent. Par ailleurs, grâce aux passerelles, ou *gateways* (dispositif qui connecte des réseaux de télécommunication différents), certains services du réseau de la téléphonie mobile sont reliés à Internet.

Bien que portant essentiellement sur les questions touchant la criminalité sur Internet, le présent rapport met en lumière la nécessité d'élaborer un cadre de réglementation neutre, cela en raison de la convergence des réseaux et services de communication électronique.

2.3 Les acteurs de la communication en réseau

La préparation, la mise à disposition et la transmission de contenus illégaux ou d'informations utilisées de manière illégale sur les réseaux de communication nécessitent plusieurs étapes. C'est la raison pour laquelle plusieurs personnes sont toujours impliquées comme auteurs ou participants chaque fois qu'un acte délictueux est commis.

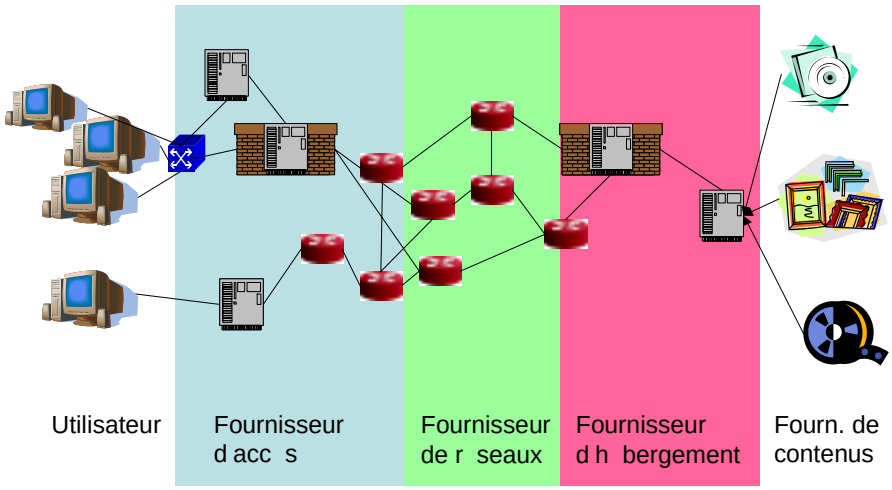
Dans l'exemple du World Wide Web (WWW) qui - outre la messagerie électronique - est le genre de transmission d'informations le plus utilisé via Internet (cf. ci-dessus 2.15), on peut différencier plusieurs groupes :

2.31 Les prestataires

Les prestataires, ou fournisseurs, se divisent en quatre groupes différents (voir le graphique ci-dessous). Certains fournissent les quatre prestations (par ex. America Online, Bluewin), d'autres se sont spécialisés uniquement dans une ou deux prestations de services.

[29] Voir à ce propos le site web des plaintes : www.handybetrug.ch (état : 9.10.2002)

Du fournisseur de contenus à l'utilisateur



2.311 Le fournisseur de contenus

Le fournisseur de contenus (*content provider*) diffuse sur Internet ses propres contenus ou des contenus repris de tiers. Il utilise au moins un fournisseur d'accès (cf. ci-dessous ch. 2.314) et diffuse ces contenus sur son propre ordinateur ou sur celui d'un fournisseur d'hébergement de sites (cf. ci-dessous ch. 2.312). Du fait de la diffusion croissante des protocoles *peer-to-peer*, des utilisateurs finaux normaux, qui n'apparaissent autrement que comme consommateurs de contenus, peuvent offrir leurs propres contenus. Dans ces cas, le fournisseur de contenus s'occupe lui-même de l'hébergement de ses données.

2.312 Le fournisseur d'hébergement de sites

Le fournisseur d'hébergement de sites (*hosting provider*) met à la disposition de ses clients - les fournisseurs de contenus - un serveur sur lequel ces derniers peuvent offrir leurs propres sites. Selon les possibilités, en ayant accès à une page web, le client peut aussi mettre à exécution ses propres programmes, qu'il y a hébergés. En fonction des circonstances, le fournisseur d'hébergement offre de l'espace à d'autres services, par ex. la messagerie électronique. Cette dernière prestation se caractérise par le fait que d'ordinaire, le fournisseur d'hébergement ne participe pas à la sauvegarde d'informations sur son serveur. Il s'agit dans ce cas de déroulements de programme automatisés que seul le fournisseur de contenus ordonne ou contrôle.

2.313 Le fournisseur de réseaux

Grâce à son réseau de communication, le fournisseur de réseaux (*network provider*) est relié avec divers fournisseurs d'accès, d'autres fournisseurs de réseaux ainsi qu'avec de gros clients potentiels qui n'ont pas besoin d'un propre fournisseur d'accès (voir ci-dessous ch. 2.314). Le transport des données se fait par

l'intermédiaire de ces réseaux ; il repose également sur l'automatisation des programmes.

2.314 Le fournisseur d'accès

Le fournisseur d'accès (*access provider*) permet aux utilisateurs finaux ou aux entreprises d'accéder à Internet par l'intermédiaire du téléphone ou par un accès à large bande (ADSL, Cablemodem, Wireless Local Loop, Satellit, ligne louée, etc.). En général, le fournisseur d'accès alloue dynamiquement à l'utilisateur final une adresse Internet qui n'est pas permanente (une nouvelle adresse est attribuée à chaque connexion). Les entreprises et les utilisateurs finaux qui veulent aussi fournir des contenus reçoivent toutefois d'ordinaire une adresse ou un bloc d'adresses fixes à partir du domaine d'adresses que gère le fournisseur d'accès. Ces processus se déroulent également de manière automatique, c'est-à-dire sans intervention manuelle du fournisseur d'accès.

En général, les fournisseurs d'accès gèrent aussi un serveur de nom de domaine (DNS, *Domain Name System*), qui permet la résolution de noms symboliques sur les adresses Internet [30]. Cela n'est toutefois pas absolument nécessaire car il existe aussi des serveurs DNS publics que l'on peut utiliser pour publier ou résoudre des noms symboliques.

2.32 L'utilisateur

L'utilisateur (*user*) est à l'autre extrémité du processus de communication. C'est la personne qui appelle à partir de la maison, du bureau, du cybercafé ou de son portable (ordinateur ou téléphone) les données mises à disposition sur un serveur.

2.33 Echangeabilité et multifonctionnalité

Les rôles décrits aux chiffres 2.31 et 2.32 sont interchangeables. Par exemple celui qui cherche des données musique dans un service *peer-to-peer* (voir ci-dessus ch. 2.311) et les charge sur son disque dur doit être qualifié d'*utilisateur*. Mais si cet utilisateur autorise en même temps l'accès en ligne à une partie de son disque dur, lequel contient des fichiers musique que l'on peut appeler et télécharger, il devient un *fournisseur de contenus* (ainsi que *fournisseur d'hébergement* de lui-même).

Les prestataires assument souvent plusieurs fonctions en parallèle. Une entreprise de médias peut par exemple offrir sur son site, outre ses propres contenus, un espace dans un forum pour les contenus de tiers. Pour ce qui est de leur propres contenus, ils agissent donc comme *fournisseur de contenus*, mais si l'on considère le forum, ils sont en règle générale de simples *fournisseurs d'hébergement*, le passage entre les deux fonctions s'effectuant *en permanence*.

Dans l'exemple mentionné ci-dessus, l'entreprise de médias peut aussi devenir un fournisseur de contenus du fait que des informations d'autrui sont fournies dans le

[30] Exemple : www.ofj.admin.ch correspond à l'adresse numérique 193.5.216.22.

forum lorsqu'un collaborateur responsable anime le forum ou publie des contributions dont seul le contenu a été contrôlé ; on considère qu'il s'est alors « approprié » les informations d'autrui. Souvent, la double fonction porte aussi sur l'accès et l'hébergement de sites.

2.34 Les participants à d'autres services d'Internet

Les fonctions décrites ci-dessus et assumées par les participants valent également pour les autres services mis en œuvre sur Internet. Mentionnons essentiellement la messagerie électronique, les forums de discussion, les transferts de fichiers (ftp), le bavardage en ligne (IRC, *Internet Relay Chat*), le *streaming web* (données tv, vidéo ou audio en flot continu), etc.

En principe, ces catégories de fournisseurs peuvent aussi être transférées sur la téléphonie fixe et mobile, ainsi que sur d'autres modes de communication (voir ci-dessous ch. 2.4).

2.4. Les réseaux

2.41 La télécommunication en général

La télécommunication est le processus technique permettant d'envoyer, de transmettre et de recevoir des informations de toutes sortes par le réseau électrique, magnétique, optique ou électromagnétique. La télécommunication permet donc de transférer des signes, des mots, des images, des sons ou encore des documents multimédias - qui sont sauvegardés ou traités dans la plupart des cas par des ordinateurs, des microprocesseurs ou autres appareils - de manière rapide et à peu de frais.

La transmission de données a encore lieu en partie sur la base de techniques analogiques : les données numériques sont d'abord transformées en signaux analogiques qui correspondent à des modifications continues de tensions électriques, ondes sonores ou magnétisations ; ces signaux sont ensuite transmis aux appareils-cibles qui les retransforment en données numériques.

2.42 Le réseau électronique de communication

On appelle réseau de communication, ou réseau de données, le regroupement en circuit d'ordinateurs ou d'autres appareils de télécommunication par des réseaux *câblés* terrestres ou des *réseaux radio* sans câble. Ces réseaux de communication utilisent diverses techniques de transmission et se différencient aussi par la manière dont ils assurent le transport logique des données.

Il est donc important de ne pas seulement parler « d'Internet » lorsque le débat s'engage sur les problèmes de droit pénal que pose la transmission d'informations. Une déclaration portant atteinte à l'honneur ou une image pornographique mettant en scène des enfants peut être transmise aussi bien par Internet (FTP, messagerie

électronique, WWW) que par le réseau de téléphonie mobile (SMS, MMS) ou par un réseau local d'entreprises (LAN) qui n'utilise pas nécessairement la technologie Internet.

2.43 Divers genres de réseaux de communication

Lorsqu'on parle de réseau électronique de communication, il est recommandé de prendre pour référence le modèle *Open Systems Interconnect* (modèle OSI) de l'ISO (Organisation internationale de normalisation). Selon ce modèle, *indépendamment de sa technologie*, un réseau se décompose en sept couches, chaque couche procurant des services à la couche immédiatement supérieure et requérant des services de la couche immédiatement inférieure. Au niveau de la couche inférieure (numérotée 1), la couche inférieure, on parle de transport physique des données qui peut avoir lieu à travers les médias les plus différents (transport électrique, optique, etc.). La couche supérieure (numérotée 7) procure à l'utilisateur des services tels que la téléphonie, la télévision, le courrier électronique et le World Wide Web.

Dans la pratique, on différencie souvent *divers genres de réseaux* qui tirent leur appellation des services offerts [31] ou du média physique de transmission [32]. L'important néanmoins est que *d'une part* des réseaux puissent être techniquement connectés entre eux indépendamment du moyen physique de transmission et que *de l'autre,* les services offerts puissent également l'être sur d'autres médias que ceux prévus à l'origine. Les protocoles Internet constituent une base [33] acceptée dans le monde entier permettant d'offrir des services d'utilisateur final indépendamment du média physique de transmission :

- **Le réseau de téléphonie fixe**
  Auparavant, le réseau téléphonique fixe reposait uniquement sur une technologie de transmission *analogique*. Il a été depuis réaménagé en réseau *numérique* à voix transmise en paquets [34]. Certains opérateurs se servent d'ores et déjà, du moins en partie, de la technologie Internet (*téléphonie sur IP*) et transmettent des conversations téléphoniques par le biais de la même infrastructure physique que celle permettant au réseau public d'Internet de fonctionner. Pour les entreprises ayant le projet d'aménager de nouvelles installations périphériques, cela constitue désormais une solution permettant de téléphoner sans câblage supplémentaire et de coupler leurs ordinateurs.
- **Le réseau de téléphonie mobile**
  Le réseau de téléphonie mobile est une extension du réseau téléphonique. Outre

[31] Par ex. le réseau de téléphonie mobile, le réseau câblé (pour la radio et la télévision).

[32] Wireless LAN (WLAN), réseau Ethernet, réseaux à fibres optiques.

[33] Jusqu'en 1994, plusieurs fabricants d'ordinateurs ainsi que l'ISO avaient l'intention de standardiser sur le marché d'autres protocoles de communication. Mais, grâce à la simplicité de leur structure et à leur disponibilité dans de nombreux systèmes d'exploitation, les protocoles concurrents d'Internet l'emportèrent et se sont depuis établis comme la norme de facto.

[34] Afin d'éviter les retards inopportuns dans la transmission de la voix, une ligne dédiée était jusqu'ici connectée entre l'appelant et l'appelé. Avec un inconvénient : cette liaison n'est jamais pleinement utilisée en raison des pauses vocales. Par contre, si la voix est désormais *mise sous paquets*, par exemple avec le protocole Internet (IP) - ces paquets étant individuellement transmis par le réseau -, il est possible à d'autres utilisateurs d'utiliser ces pauses, ce qui multiplie la capacité des lignes.

la transmission de la voix et les SMS (ainsi que les extensions multimédias), il offre encore d'autres services par rapport au réseau fixe. La transmission physique est en général assurée par des techniques numériques de transmission par paquets (par ex. GSM, CDMA), conçues avant tout pour le transport de la voix. Toutefois, il y a eu récemment aussi quelques tentatives visant à établir le réseau de téléphonie mobile (à nouveau sur la base de la *téléphonie sur IP*) sur des réseaux sans fil de données (WLAN ou IEEE 802.11).

- **Les réseaux câblés de télévision**
  Les réseaux TV câblés installés à l'origine pour la diffusion unilatérale de la radio et de la télévision ont été entre temps largement réorganisés du point de vue de leur structure physique pour permettre l'échange de données bilatéral. Ainsi, depuis un certain temps, le réseau câblé permet de se raccorder à la fois à Internet et au réseau téléphonique par la téléphonie sur IP.
- **Les réseaux câblés électriques**
  Les réseaux de distribution traditionnels destinés au courant électrique permettent également le transport de données. Quelques entreprises d'approvisionnement en énergie testent actuellement ce genre de possibilités et envisagent d'intervenir en qualité de fournisseurs de services Internet et d'opérateurs téléphoniques [35].

Il apparaît donc qu'*Internet* occupe une fonction de pont notamment entre les différents réseaux physiques mentionnés. Il offre à un niveau logique (couche 3 du modèle de référence OSI) un service universel permettant le transport de données pour les applications les plus diverses. En font partie - outre les données d'ordinateurs - la téléphonie, la radio, la télévision et la vidéo (pour plus de détails à ce propos, voir le chapitre 3 ci-dessous).

2.44 Nécessité d'une réglementation plus large

Etant donné la diversité des protocoles de communication et leur constante évolution, il ne conviendrait pas de considérer uniquement le protocole TCP/IP et Internet pour établir la réglementation légale de la responsabilité. En fait, le domaine d'application de cette réglementation devrait s'étendre à *tous les médias de transmission au niveau mondial* qui font de l'utilisateur final un acteur à part entière de cette transmission.

Du fait de cette large assise, la réglementation s'appliquerait ainsi à tous les acteurs de la transmission et de la fourniture d'informations, indépendamment des standards et protocoles utilisés.

2.5 Communication de masse et communication individuelle

Il importe en premier lieu de différencier les délits en matière de communication individuelle et les délits en matière de communication de masse. En effet, la

[35] Les Entreprises Electriques Fribourgeoises (EEF) et l'opérateur téléphonique Sunrise offrent, depuis septembre 2001, un accès à Internet par câble (par la prise électrique). La clientèle devrait bénéficier désormais d'une alternative à la connexion conventionnelle, alternative de surcroît plus avantageuse, plus souple et plus performante.

communication individuelle est soumise au *secret des télécommunications*. Les échanges d'informations y sont de ce fait plus *protégés* contre les interventions de tiers, y compris les fournisseurs d'accès, les fournisseurs d'hébergement et les fournisseurs de réseau.

2.6. Les réseaux électroniques de communication et les médias

2.61 Nécessité de différencier le droit des télécommunications et le droit des médias

Il est important de procéder à une *délimitation* nette du point de vue *dogmatique* entre

- les *prestations de télécommunication* concernant la « transmission d'informations pour le compte de tiers au moyen de techniques de télécommunication » (art. 3, let. b de la loi sur les télécommunications, LTC [36]) en tant que *prestation d'infrastructures* technique, largement automatisée,
- et la *diffusion d'informations par des médias de masse* - diffusion concernant les *contenus des informations*.

Par exemple si une émission d'information comme « 10 vor 10 » (DRS) est disponible en streaming vidéo sur Internet, il y a *recoupement* entre le droit des télécommunications et le droit des médias. Or, étant donné que le droit pénal différencie aussi ces deux domaines du droit en ce sens qu'il prévoit une réglementation spéciale pour les délits des médias (art. 27, 322bis CP), il est extrêmement important de ranger les prestations fournies dans les cadres réglementaires qui sont les leurs [37].

Ces recoupements (voir également le graphique ci-dessous) font également qu'on ne peut ni résoudre les problèmes uniquement dans le contexte de la loi sur les télécommunications, ni attribuer à tous les participants au transport des données dans les réseaux de communication le rôle de prestataires de services de télécommunication au sens de l'art. 3, let. b et c LTC [38].

---

[36] RS 784.10.

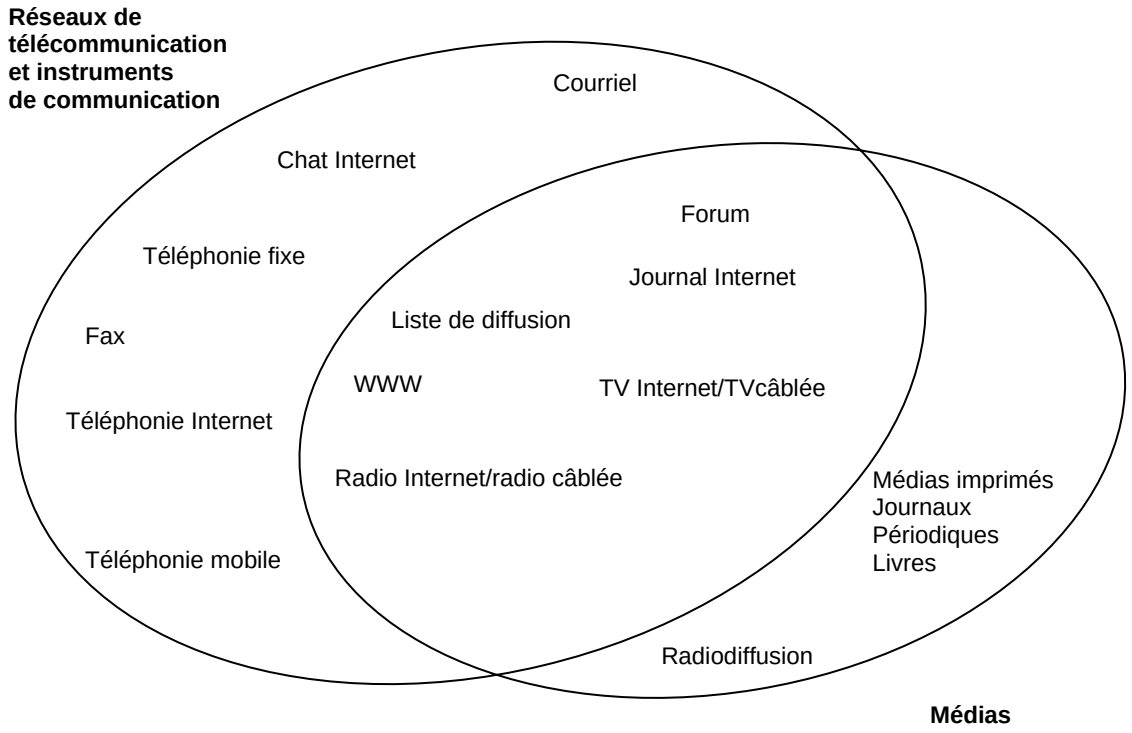
[37] Pour plus de détails voir : NIGGLI/SCHWARZENEGGER, (Bibl.), p. 61 ss.

[38] Art. 3 LTC

…

b. service de télécommunication : la transmission d'informations pour le compte de tiers au moyen de techniques de télécommunication;

c. transmission au moyen de techniques de télécommunication : l'émission ou la réception d'informations, sur des lignes ou par ondes hertziennes, au moyen de signaux électriques, magnétiques ou optiques ou d'autres signaux électromagnétiques;



Reprendre directement la notion de « fournisseur de services de télécommunication » poserait également un problème car cette notion recouvre uniquement la retransmission, mais pas la fourniture ou la préparation dans le but de transmettre des informations au moyen de techniques de télécommunication. Par ailleurs, l'art. 2 LTC prévoit une exception pour la diffusion et de la rediffusion de programmes au sens de la loi fédérale du 21 juin 1991 sur la radio et la télévision (LRTV) [39], qui couvrait également certaines émissions de radio et de télévision Internet. Enfin, la LTC s'applique uniquement aux services de communication, mais pas aux services d'information et de médias.

2.62 La technique a évolué plus rapidement que le droit

Le domaine du droit qu'il convient de clarifier recouvre un large domaine, à savoir les services de communication, d'information et de médias (c'est-à-dire les supports *et* le contenu de la communication). L'évolution de la technique a fait converger ces domaines alors que la réglementation juridique repose encore en grande partie sur une séparation entre communication individuelle et communication de masse.

2.63 Le réseau électronique de communication - une nouvelle notion centrale

Face aux infractions de plus en plus nombreuses commises sur les réseaux de communication, il est urgent de délimiter clairement les responsabilités entre les auteurs et les fournisseurs d'informations, les prestataires de services - qui mettent ces informations à la disposition de l'utilisateur sur un réseau de communication - et

[39] RS 784.40

les prestataires de services qui offrent uniquement l'accès technique aux informations sur les réseaux de communication. Il convient donc d'introduire pour la première fois dans ce rapport la notion de « réseau de communication électronique » (en abrégé « réseau de communication ») (cf. à ce propos ch. 9.21).

La même notion apparaît sous d'autres dénominations dans les publications spécialisées internationales :

- *Systèmes d'information* (notion de droit européen):

La notion de « système d'information » (Troisième Pilier, Décision-cadre relative aux attaques visant les systèmes d'information) est sciemment utilisée au niveau de l'Union européenne dans son acception la plus large possible afin de souligner l'imbrication croissante des réseaux électroniques et des différents systèmes reliés par ces réseaux. Cette notion englobe donc les ordinateurs, les organisateurs électroniques, les téléphones portables, les réseaux internes et externes, tout comme les réseaux, serveurs et autres infrastructures de l'Internet.

- *Réseau* (Convention relative à la lutte contre la cybercriminalité):

La Convention du Conseil de l'Europe relative à la lutte contre la cybercriminalité utilise comme notions générales les termes de 'réseaux' et de 'cybercriminalité'.

Si les contrôles des accès et des contenus sur Internet sont possibles dans certains cas, ils n'en demeurent pas moins extrêmement laborieux et très souvent lacunaires. Par ailleurs, il est possible de déjouer tous les dispositifs de contrôle.

3. Possibilités de contrôle technique

3.1 Objectif et principes de l'Internet

Internet a été créé dans l'optique de fournir un *réseau de communication* très décentralisé et immédiatement disponible. Même en cas de panne de certains nœuds ou de certaines liaisons (par ex. suite à une attaque militaire), ce réseau devrait demeurer à la disposition de ses utilisateurs. Son exploitation ne nécessite pas d'autorités centrales. Chaque nœud est autonome et aucun organisme n'a l'exclusivité du contrôle d'Internet.

Chaque individu disposant de l'infrastructure technique peut se raccorder à Internet. Les protocoles qui assurent la communication et le genre des prestations offertes sont établis selon un accord arrêté à l'unanimité par un organisme informel non étatique, l'« Internet Engineering Taskforce » (IETF), dont la tâche est de développer et de promouvoir les standards d'Internet. De ce fait, personne (ni fabricant, ni Etat) ne peut disposer de parties du réseau Internet. Etant donné la structure décentralisée de cette organisation associative, il n'existe que très peu de possibilités techniques de contrôler et, le cas échéant, de restreindre l'accès à certains services, à certains contenus ou à d'autres participants.

3.2 Contrôles

On distingue deux sortes de contrôles :

- *le contrôle de l'accès* : quel serveur ou quels services un utilisateur peut-il atteindre ?
- *le contrôle des contenus* : quels sont les contenus mis à disposition ? [40]

[40] L'ouvrage d'ULRICH SIEBER, Verantwortlichkeit im Internet, Munich 1999, donne une bonne vue d'ensemble de la question.

3.21 Contrôle de l'accès

3.211 News

Sur le réseau « News », un fournisseur d'hébergement (voir plus haut, ch. 2.312) peut bloquer l'accès à certains groupes de news (thématiques) en ne les copiant pas sur son infrastructure. Il décide, d'après les noms des groupes, si le nom permet de soupçonner d'éventuels contenus illégaux. Cette manière de trier les groupes est parfois une source de difficultés car il est possible que la majorité des contributions figurant dans ces groupes soient tout à fait conformes à la loi. Par ailleurs, il est très facile pour les utilisateurs de contourner un blocage en passant par d'autres serveurs de news accessibles au public.

3.212 World Wide Web

Dans le World Wide Web (WWW, Web), le fournisseur d'accès (voir plus haut ch. 2.314) peut prescrire à ses utilisateurs d'accéder au Web par l'intermédiaire d'un serveur mandataire (*serveur proxy*) afin de télécharger plus rapidement les sites Internet particulièrement populaires. Le serveur *proxy* intercepte les demandes de sites web et examine dans sa mémoire locale si l'un de ces sites a été appelé peu auparavant et a fait l'objet d'une sauvegarde intermédiaire. Si tel est le cas, il répond immédiatement à la demande sans aller de nouveau chercher le contenu désiré via Internet.

Si le fournisseur d'accès offre l'accès au web uniquement par l'intermédiaire d'un serveur *proxy*, ce dernier peut aussi être utilisé pour interdire des accès à certains sites (URL) ou serveurs (adresses IP) (voir par exemple dans l'encadré ci-dessous).

Le serveur proxy du monde arabe

Etisalat, le fournisseur d'accès Internet des Emirats arabes unis, exploite un serveur *proxy* constituant le seul accès au web. On trouve néanmoins de nombreuses descriptions sur la manière de contourner ce serveur proxy, permettant donc aussi dans les Emirats l'accès - qui y est *illégal* - à d'autres sites web [41].

Du fait que l'utilisation d'un serveur *proxy* doit être configurée directement par les utilisateurs dans le navigateur de réseau - donc dépend de l'utilisateur -, les fournisseurs d'accès occidentaux offrent d'ordinaire aussi l'accès direct au web. Les *proxies* dits *transparents* - qui ne doivent plus être configurés dans le *navigateur* (*browser)* de l'utilisateur - exploitent une technologie très récente : ils permettent un accès plus rapide à Internet et un contrôle éventuel de l'accès à certains URL [42].

Le fournisseur d'accès peut aussi configurer ses *routeurs* [43] ainsi que d'autres appareils [44] - par lesquels passent les flux de données - de manière à ce qu'ils filtrent

[41] Par ex. http://djsyndrome.homestead.com/proxies1.html
[42] Par ex. le Content Engine de Cisco http://www.cisco.com/warp/public/cc/pd/cxsr/ces/index.shtml
[43] Par ex. http://www.cisco.com/warp/public/44/jump/routers.shtml
[44] Par ex. *les pare-feux* http://www.checkpoint.com ou les appareils de gestion des réseaux à larges bandes, par ex. www.packeteer.com

et bloquent les paquets de données possédant des adresses cibles précises (ou adresses sources) ou même des paquets http avec des URL bien déterminés. Néanmoins, l'installation de ces contrôles d'accès signifie en général toujours que le flux des données qui passent par le routeur (ou par d'autres appareils) diminue car pour chaque paquet de données, la liste des adresses bloquées doit être fouillée.

Ce genre de filtrage ne pourra donc être utilisé que de manière très restrictive par les fournisseurs d'accès qui ont une grosse clientèle. Par ailleurs, les clients, qui se sont habitués à des vitesses de plus en plus élevées, n'accepteront pas un ralentissement de l'utilisation d'Internet dû à un filtrage. Cela irait aussi à l'encontre d'une diffusion rapide et avantageuse des accès Internet pour des raisons de politique technologique, sociale, éducative et économique.

En cas de blocage de l'accès aux serveurs ou aux sites, il convient, en outre, de tenir compte du fait qu'un grand nombre de contenus légalement autorisés sont souvent aussi touchés. Par exemple le blocage du serveur d'un fournisseur d'hébergement comme *geocities* pourrait toucher des milliers de sites Internet.

En outre, les utilisateurs suffisamment motivés et habiles ont, là aussi, diverses *possibilités de contourner* ces blocages : il existe par exemple des serveurs *proxies* publics qui sont rattachés à d'autres prestataires Internet (par ex. à l'étranger) et permettent d'accéder indirectement à des services bloqués [45].

Le fournisseur de contenus peut aussi modifier son adresse de serveur de sorte que les règles de filtrage en place deviennent obsolètes et que le blocage d'accès devienne inutile. Les expériences faites jusqu'ici montrent que les fournisseurs de contenus illégaux font rapidement usage de cette possibilité.

3.22 Contrôle des contenus

Le contrôle des contenus requiert du fournisseur d'hébergement qu'il contrôle régulièrement les contenus mis à disposition sur ses serveurs (textes et données multimédias). Etant donné les très importants volumes de données (de nombreux tera bytes de données) et les taux de modifications élevés, le contrôle des contenus pose les fournisseurs de services devant des problèmes souvent insolubles.

Il est *impossible* de procéder à une recherche entièrement automatisée et fiable de contenus dont les droits d'auteurs sont protégés, ou même de contenus illégaux. Il existe des algorythmes d'analyse de textes et d'images, mais ils sont très longs et en outre sujets aux erreurs ; la recherche dans ce domaine est en cours.

On peut certes chercher rapidement des textes ou des données multimédias repérables grâce aux « empreintes digitales électroniques » [46]. Mais en modifiant les données - un *bit* suffit - un fournisseur peut aisément éviter que ses contenus soient identifiables. Etant donné la multitude des fournisseurs d'hébergement, un

[45] Une liste de ces serveurs figure par ex. sous http://tools.rosinstrument.com/proxy/

[46] Une « empreinte digitale électronique » est fréquemment un nombre binaire long de 32 à 130 bits que l'on peut calculer par procédé mathématique à partir d'un document ou d'une image électronique ; elle caractérise ce document ou cette image. Si un seul bit est changé dans le document, l'empreinte digitale est également modifiée.

fournisseur de contenus peut en général recourir à un autre fournisseur d'hébergement (également dans un autre pays) lorsqu'il pense que ses contenus pourraient être censurés.

Les services *peer-to-peer* (P2P) rencontrent de plus en plus de succès. Ils permettent l'échange direct de données entre des utilisateurs finaux sans instance de transmission centrale. Pour ces services, le contrôle de contenu ne peut être effectué que par l'utilisateur final. En cas de *services de file sharing*, par exemple Gnutella ou Morpheus, il peut décider quels fichiers il veut offrir. Mais s'il participe à un service comme *Freenet* [47], il ne peut pas procéder à un contrôle du contenu sur la base du projet spécifique étant donné que les données sont fournies sous forme cryptée sur son ordinateur et qu'il ne connaît pas la clé.

3.3 Efficacité

Il convient de retenir pour conclure que du fait de sa constitution, Internet *ne se prête pas à un contrôle ou une surveillance centralisé/ée*. Toutes les mesures de contrôles que nous connaissons peuvent être contournées par des utilisateurs plus moins habiles et même par les fournisseurs de contenus illégaux.

Toute nouvelle mesure de contrôle envisagée est immédiatement suivie d'une mise au point technique permettant de la contourner [48]. De ce fait, les mesures de contrôle prescrites peuvent certes accroître le seuil d'accès à des contenus illégaux, mais la possibilité de les contourner demeure.

Globalement, il ne semble *pas judicieux*, ne serait-ce que du point de vue technique, d'obliger les fournisseurs d'accès à bloquer l'accès à des contenus illégaux ou d'obliger les fournisseurs d'hébergement à contrôler à titre préventif la conformité légale de tous les contenus mis à disposition chez eux par des tiers.

---

[47] http://freenetproject.org/ , description en allemand à l'adresse suivante : http://archiv.tu-chemnitz.de/pub/2002/0050/data/vortrag.html

[48] La menace de fermer des *Napster* a été l'une des raisons du développement de services de *file sharing* entièrement décentralisés comme Gnutella ne possédant plus aucun ordinateur central assumant une fonction d'intermédiaire.

La diffusion d'informations au niveau mondial, que la Toile notamment a permise, nécessite une coordination internationale du droit. Les principes que les pays de l'UE ont formulés dans la « directive sur le commerce électronique » ont, de ce fait, une importance majeure pour la Suisse.

4. La directive de l'UE sur le commerce électronique et son application dans les Etats voisins de la Suisse

4.1 Généralités à propos de la directive 2000/31 du Parlement européen et du Conseil (directive sur le commerce électronique) du 8 juin 2000

Le Parlement européen et le Conseil de l'Union européenne ont arrêté le 8 juin 2000 la directive 2000/31/CE relative à certains aspects juridiques des services de la société de l'information, et notamment du commerce électronique dans le marché intérieur (« Directive sur le commerce électronique »)[49].

Cette directive rassemblant 24 articles est précédée de 65 *considérants*. Selon ceux-ci, la directive sur le commerce électronique a pour but d'assurer que le commerce électronique puisse *bénéficier dans sa globalité du marché intérieur*. Pour y parvenir, il convient d'*éliminer les obstacles juridiques* qui découlent d'une part de la divergence des législations et, de l'autre, de l'insécurité juridique des régimes nationaux applicables à ces services.

Pour garantir, à l'avenir aussi, la *sécurité du droit* et la confiance du consommateur, la directive doit établir un cadre juridique clair, pour le marché intérieur, réglant certains aspects du commerce électronique.

L'objectif de la directive est de créer un cadre juridique pour assurer la libre circulation des services de la société de l'information entre les Etats membres, *et non d'harmoniser le domaine du droit pénal en tant que tel* [50,51]. Notamment, la directive

[49] Directive sur le commerce électronique, en abrégé : DIRECTIVE (Bibl.).

[50] Cf. DIRECTIVE (Bibl.), p. 2 s., ch. 5 à 8. A l'art. 1, al. 2 de la directive, il est dit d'une manière générale que la directive *rapproche* (uniquement) certaines dispositions nationales applicables aux services de la société de l'information et qui concernent le marché intérieur, notamment aussi pour ce qui est de la responsabilité des intermédiaires et des fournisseurs.

[51] La Convention du Conseil de l'Europe sur la cybercriminalité, STE n° 185, (« Convention sur la cybercriminalité ») signée à Budapest le 23 novembre 2001, entre autres par la Suisse, a pour but *une harmonisation du droit pénal et du droit de procédure pénle* . Le texte de cette convention peut être consulté sur le site Internet suivant : http://conventions.coe.int. Pour plus de détail sur son contenu, se reporter au chiffre 10.21. - Cf. en outre la « *Déclaration sur la liberté de la communication sur l'Internet »,* du comité ministériel du Conseil de l'Europe du 28 mai 2003 qui rassemble les principes centraux de la directive sur le commerce électronique. Ce texte est disponible sur le site Internet

n'entend pas porter atteinte aux règles et principes fondamentaux nationaux en matière de liberté d'expression [52].

Selon le *principe de la proportionnalité*, les mesures prévues par la directive se limitent strictement au minimum requis pour atteindre l'objectif du bon fonctionnement du marché intérieur. Là où il est nécessaire d'intervenir au niveau communautaire, la directive sur le commerce électronique doit, par contre, assurer un haut niveau de protection des objectifs d'intérêt général, en particulier la protection des mineurs, de la dignité humaine, du consommateur et de la santé publique [53].

4.2 Les articles 12 à 15 de la directive sur le commerce électronique (responsabilité des intermédiaires)

4.21 Remarques préliminaires

La *responsabilité des « prestataires »* [54], c'est-à-dire des fournisseurs, est *l'un des domaines de réglementation majeurs* de la directive sur le commerce électronique. Il se trouve de ce fait au cœur de la directive, aux articles 12 à 15, sous le titre « Responsabilité des prestataires intermédiaires ».

Afin de répondre à l'objectif fixé dans les considérants de la directive, à savoir l'élimination de l'insécurité juridique [55], les articles 12 à 15 définissent essentiellement les cas ou conditions dans lesquelles *les prestataires ne sont pas responsables*.

Les notions utilisées ici sont celles de « dérogations », de « limitation de responsabilité » [56]. La directive part donc implicitement du *principe de la responsabilité des prestataires.* Néanmoins, les principes généraux sur lesquels repose cette responsabilité et la manière dont elle est fondée sont formulés de manière relativement large ; elle peut au besoin - même si cela devait être peu approprié - être déduite a contrario des dérogations [57].

---

suivant :
http://www.coe.int/T/F/Droits_de_l%27Homme/media/5_Ressources_documentaires/1_Textes_de_base/2_%20Textes_du_Comite_des_Ministres/PDF_D%E9claration%20libert%E9%20de%20communication%20sur%20Internet%20%20(f).pdf

[52] DIRECTIVE (Bibl.), p. 2, ch. 9.

[53] DIRECTIVE (Bibl.), p. 2, ch. 10.

[54] Ce terme est défini à l'art. 2, let. b de la directive (Bibl.) Selon cette définition, est « prestataire » toute personne physique ou morale qui fournit un service de la société de l'information.

[55] DIRECTIVE (Bibl.), p. 6, ch. 40.

[56] DIRECTIVE (Bibl.), p. 6, ch. 42 à 46.

[57] Selon SATZGER (Bibl.), p. 109 ss, 111, les articles 12 à 15 de la directive auraient donc une fonction de « filtre » ; en d'autres termes, la directive viserait ainsi une « generelle Einschränkung der Verantwortlichkeit für unerlaubte Netz-Aktivitäten Dritter, ohne dabei materiellrechtliche Vorschriften der nationalen Rechtsordnungen, die eine Rechtsverletzung begründen, als solche zu modifizieren » (N.d.T. « une restriction générale de la responsabilité des activités non autorisées de tiers sur la Toile, sans modifier en tant que telles les prescriptions de droit matériel des législations nationales qui fondent une violation du droit »).

Les considérants ne précisent pas non plus sur quelle base la responsabilité des prestataires doit reposer. Par contre, ils soulignent que les dérogations établies dans la directive concernant la responsabilité ne couvrent que « les cas où l'activité du prestataire de services est limitée au processus technique d'exploitation et de fourniture d'un accès à un réseau de communication sur lequel les informations fournies par des tiers sont transmises ou stockées temporairement, dans le seul but d'améliorer l'efficacité de la transmission. Cette activité revêt un caractère purement technique, automatique et passif, qui implique que le prestataire de services de la société de l'information n'a pas la connaissance ni le contrôle des informations transmises ou stockées. » [58]

Aux articles 12 à 15, la directive sur le commerce électronique réglemente la responsabilité de manière généralement uniforme. En d'autres termes, elle soumet tous les domaines du droit à une *réglementation horizontale* (droit pénal, droit de la responsabilité, droit d'auteur, droit de la concurrence, etc.) [59]. Ce large dispositif de réglementation explique aussi pourquoi la directive ne fournit aucune base légale, couvrant les différents domaines du droit, à une responsabilité des prestataires de services. Si les Etats membres de l'UE ne possèdent pas de base légale couvrant la responsabilité d'une partie de ces prestataires de services, la directive sur le commerce électronique n'a aucun impact

Il convient, en outre, de souligner que conformément au Traité instituant la communauté européenne (TCE), l'UE ne possède *pas de compétence législative dans le domaine du droit pénal des Etats membres*. La modification des conditions de la punissabilité constitue donc une répercussion indirecte de l'harmonisation du droit sur le marché intérieur, qui ne peut concerner en principe que des prestations fournies contre rémunération. Afin d'obtenir la sécurité du droit visée, les Etats membres sont invités à procéder à une mise en application dépassant le marché intérieur, donc le champ d'application géographique du droit européen [12].

4.22 Art. 12 : pas de responsabilité pour un simple transport

Art. 12 - Simple transport

1. Les États 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 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

[58] DIRECTIVE (Bibl.), p. 6, ch. 42.

[59] Voir à ce propos NIGGLI/SCHWARZENEGGER (Bibl.), p. 63 ss, 66 ss. A propos des principaux inconvénients de ce système de réglementation - contrairement à la réglementation spécifique à un domaine - qui touchent surtout le droit pénal, voir entre autres op. cit., p. 66 ss.

[61] DIRECTIVE (Bibl.), p. 6, ch. 43.

c) ne sélectionne et ne modifie pas les informations faisant l'objet de la transmission.

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 États membres, d'exiger du prestataire qu'il mette un terme à une violation ou qu'il prévienne une violation.

En résumé, l'art. 12 de la directive sur le commerce électronique libère les prestataires de la responsabilité du « simple transport » (al. 1). Les prestataires ne seront pas tenus responsables, même en cas de stockage automatique, intermédiaire et limité dans le temps dont le seul but est la transmission de données (al. 2). Dans les deux cas, il est supposé qu'ils ne sont impliqués en aucune manière dans l'information transmise. Cela suppose notamment qu'ils ne modifient pas l'information qu'ils transmettent [61].

4.23 Art. 13 et 14 : pas de responsabilité pour le caching et l'hébergement

Art.13 - Forme de stockage dite "caching"

1. Les États 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 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.

Comme précédemment dans le cas du simple transport [62], l'exclusion de la responsabilité n'est applicable que si le prestataire de service dit de « caching » *n'est impliqué en aucune manière* dans l'information transmise. Par contre le prestataire de service de « caching » qui collabore délibérément avec un fournisseur de contenu afin de commettre des actes illicites fournit nettement plus de prestations, raison pour laquelle il ne peut bénéficier de l'exclusion de la responsabilité [63].

Art.14 *Hébergement*

1. Les États membres veillent à ce que, en cas de fourniture d'un service de la société de l'information consistant à stocker des informations fournies par un destinataire du service, le prestataire ne soit pas responsable des informations stockées à la demande d'un destinataire du service à condition que :

a) le prestataire n'ait pas effectivement connaissance de l'activité ou de l'information illicites et, en ce qui concerne une demande en dommages et intérêts, n'ait pas connaissance de faits ou de circonstances selon lesquels l'activité ou l'information illicite est apparente ou
b) le prestataire, dès le moment où il a de telles connaissances, agisse promptement pour retirer les informations ou rendre l'accès à celles-ci impossible.

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 États 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 États membres, d'instaurer des procédures régissant le retrait de ces informations ou les actions pour en rendre l'accès impossible.

Le fournisseur d'hébergement ne peut revendiquer une limitation de responsabilité que lorsqu'il agit promptement, dès qu'il prend connaissance ou conscience du caractère illicite des activités, pour retirer les informations concernées ou en rendre l'accès impossible [64].

4.24 Art. 15 : pas d'obligation générale de surveillance

Art. 15 Absence d'obligation générale en matière de surveillance

1. Les États membres ne doivent pas imposer aux prestataires, pour la fourniture des services visée aux articles 12, 13 et 14, 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.

2. Les États membres peuvent instaurer, pour les prestataires de services de la société de l'information, l'obligation d'informer promptement les autorités publiques

[62] Voir plus haut ch. 4.22 in fine.
[63] DIRECTIVE (Bibl.), p. 6, ch. 44.
[64] DIRECTIVE (Bibl.), p. 6, ch. 46.

compétentes d'activités illicites alléguées qu'exerceraient les destinataires de leurs services ou d'informations illicites alléguées que ces derniers fourniraient ou de communiquer aux autorités compétentes, à leur demande, les informations permettant d'identifier les destinataires de leurs services avec lesquels ils ont conclu un accord d'hébergement

Conformément à l'art. 15 de la directive sur le commerce électronique, les prestataires mentionnés ci-dessus ne doivent pas se voir imposer d'obligation générale de surveiller les informations qu'ils transmettent et qu'ils stockent, ou de rechercher activement les circonstances révélant des activités illicites. La directive n'empêche néanmoins pas les Etats membres d'établir des procédures permettant de retirer les informations ou de bloquer l'accès à ces dernières [65].

4.3 La mise en application des art. 12 à 15 de la directive sur le commerce électronique dans les Etats voisins de la Suisse, membres de l'Union européenne [66]

4.31 Allemagne

En édictant le 22 juillet 1997 une loi intitulée « Gesetz über die Nutzung von Telediensten » [67], en abrégé : *Teledienstegesetz* (TDG) [loi sur l'utilisation des téléservices] - comparable à la directive européenne sur le commerce électronique, mais la précédant de quelques années - , l'Allemagne s'est dotée d'une *réglementation horizontale*. En d'autres termes, elle avait déjà harmonisé la réglementation de la responsabilité dans le domaine des services d'information et de communication.

En vertu de cette réglementation horizontale du droit national, le prestataire qui remplit les conditions de l'exclusion de la responsabilité ne peut être poursuivi en justice ni sur le plan civil ni sur le plan pénal. A quel échelon des conditions de la responsabilité ou punissabilité convient-il d'examiner cette question ? La réponse demeure extrêmement floue (état de fait, illicéité, faute ou élément d'examen extérieur à cette structure, cf. ci-dessous 9.121). Par contre, il est établi que si les conditions mentionnées ne sont pas remplies, la responsabilité ou la punissabilité doivent être examinées à la lumière des états de fait prévus dans les domaines du droit entrant en considération.

En vue de la mise en application de la directive, le législateur allemand a édicté le 14 décembre 2001 la loi intitulée « Gesetz über die rechtlichen Rahmenbedingungen für den elektronischen Geschäftsverkehr, en abrégé *Elektronisches Geschäftsverkehrsgesetz*, EGG » [loi relative aux conditions-cadres applicables aux

---

[65] DIRECTIVE (Bibl.), p. 6, ch. 45.

[66] Au *Liechtenstein*, Etat voisin non membre de l'UE mais faisant partie de l'EEE et de l'AELE, la directive sur le commerce électronique n'a, à ce jour, pas encore été mise en application ; autrement dit, il n'existe pas de règles spéciales légales de responsabilité dans ce domaine. - Pour des informations plus détaillées, cf. l'avis établi en 2002 par l'Institut suisse de droit comparé sur mandat de l'Office fédéral de la justice à propos des législations dans les 15 Etats de l'UE et des Etats-Unis (état au 23 août 2002).

[67] In : BGBl I 1997, 1870.

commerce électronique, en abrégé « loi sur le commerce électronique »]. Cette loi est entrée en vigueur le 21 décembre 2001.

L'art. 1 EGG a introduit *dans la TDG* [68] de *nouvelles règles relatives à la responsabilité* [69]: les §§ 8 à 11 TDG (nouvelle version) se trouvent au chapitre 3 de la TDG sous le titre « Verantwortlichkeit ».

> **§ 8 Allgemeine Grundsätze**
>
> (1) Diensteanbieter sind für eigene Informationen, die sie zur Nutzung bereithalten, nach den allgemeinen Gesetzen verantwortlich.
>
> (2) Diensteanbieter im Sinne der §§ 9 bis 11 sind nicht verpflichtet, die von ihnen übermittelten oder gespeicherten Informationen zu überwachen oder nach Umständen zu forschen, die auf eine rechtswidrige Tätigkeit hinweisen. Verpflichtungen zur Entfernung oder Sperrung der Nutzung von Informationen nach den allgemeinen Gesetzen bleiben auch im Falle der Nichtverantwortlichkeit des Diensteanbieters nach den §§ 9 bis 11 unberührt. Das Fernmeldegeheimnis nach § 85 des Telekommunikationsgesetzes ist zu wahren.

Le § 8, al. 1 réglemente de manière explicite la responsabilité du prestataire de services à l'égard de ses propres informations. Le § 8, al. 2 met en application l'art. 15, al. 1 (Absence d'obligation générale en matière de surveillance) de la directive sur le commerce électronique. Par contre, le législateur allemand n'a fait aucun usage de la possibilité donnée par l'art.15, al. 2 de la directive aux Etats membres d'instaurer une obligation générale de rechercher activement des faits révélant des activités illicites.

> **§ 9 Durchleitung von Informationen**
>
> (1) Diensteanbieter sind für fremde Informationen, die sie in einem Kommunikationsnetz übermitteln oder zu denen sie den Zugang zur Nutzung vermitteln, nicht verantwortlich, sofern sie
> 1. die Übermittlung nicht veranlasst,
> 2. den Adressaten der übermittelten Informationen nicht ausgewählt und
> 3. die übermittelten Informationen nicht ausgewählt oder verändert haben.
>
> Satz 1 findet keine Anwendung, wenn der Diensteanbieter absichtlich mit einem der Nutzer seines Dienstes zusammenarbeitet, um rechtswidrige Handlungen zu begehen.
>
> (2) Die Übermittlung von Informationen nach Absatz 1 und die Vermittlung des Zugangs zu ihnen umfasst auch die automatische kurzzeitige Zwischenspeicherung dieser Informationen, soweit dies nur zur Durchführung der Übermittlung im

[68] In: BGBl I 2001, 3721. Lien vers la TDG nouvelle version : http://bundesrecht.juris.de/bundesrecht/tdg/index.html

[69] Les dispositions de l'ancienne TDG réglementant la responsabilité, notamment le § 5, avaient été une source de problèmes - notamment pour ce qui est de la question de la responsabilité pénale des fournisseurs d'accès. Voir à ce propos entre autres SATZGER (Bibl.), p. 113 ss, notamment les renvois et le ch. 9.121.

Kommunikationsnetz geschieht und die Informationen nicht länger gespeichert werden, als für die Übermittlung üblicherweise erforderlich ist.

Le simple transport et la simple fourniture d'accès sont ici - sous certaines conditions toutefois - exclues de la responsabilité.

§ 10 Zwischenspeicherung zur beschleunigten Übermittlung von Informationen

Diensteanbieter sind für eine automatische, zeitlich begrenzte Zwischenspeicherung, die allein dem Zweck dient, die Übermittlung der fremden Information an andere Nutzer auf deren Anfrage effizienter zu gestalten, nicht verantwortlich, sofern sie
1. die Informationen nicht verändern,
2. die Bedingungen für den Zugang zu den Informationen beachten,
3. die Regeln für die Aktualisierung der Information, die in weithin anerkannten und verwendeten Industriestandards festgelegt sind, beachten,
4. die erlaubte Anwendung von Technologien zur Sammlung von Daten über die Nutzung der Information, die in weithin anerkannten und verwendeten Industriestandards festgelegt sind, nicht beeinträchtigen und
5. unverzüglich handeln, um im Sinne dieser Vorschrift gespeicherte Informationen zu entfernen oder den Zugang zu ihnen zu sperren, sobald sie Kenntnis davon erhalten haben, dass die Informationen am ursprünglichen Ausgangsort der Übertragung aus dem Netz entfernt wurden oder der Zugang zu ihnen gesperrt wurde oder ein Gericht oder eine Verwaltungsbehörde die Entfernung oder Sperrung angeordnet hat.

§ 9 Abs. 1 Satz 2 gilt entsprechend.

Le § 10 TDG nouvelle version reprend presque mot pour mot l'art. 13 de la directive sur le commerce électronique et *libère de ce fait de la responsabilité le prestataire dit « proxy-cache »*.

§ 11 Speicherung von Informationen

Diensteanbieter sind für fremde Informationen, die sie für einen Nutzer speichern, nicht verantwortlich, sofern
1. sie keine Kenntnis von der rechtswidrigen Handlung oder der Information haben und ihnen im Falle von Schadensersatzansprüchen auch keine Tatsachen oder Umstände bekannt sind, aus denen die rechtswidrige Handlung oder die Information offensichtlich wird, oder
2. sie unverzüglich tätig geworden sind, um die Information zu entfernen oder den Zugang zu ihr zu sperren, sobald sie diese Kenntnis erlangt haben.

Satz 1 findet keine Anwendung, wenn der Nutzer dem Diensteanbieter untersteht oder von ihm beaufsichtigt wird.

Le § 11 TDG nouvelle version réglemente enfin les conditions auxquelles les fournisseurs d'hébergement sont exclus de la responsabilité (mise en application de l'art. 14 de la directive sur le commerce électronique).

4.32 Autriche

L'Autriche a réglementé la responsabilité des prestataires de services au chapitre 5 de la loi intitulée *E-Commerce-Gesetz (ECG)* [70] [loi sur le commerce électronique]. Les art. 13 à 19 ECG ont permis à l'Autriche, d'une part, de mettre en application dans une large mesure les articles 12 à 15 de la directive sur le commerce électronique et, de l'autre, *d'aller encore un peu plus loin* quant à l'exclusion de la responsabilité en ce sens qu'elle exclut aussi expressément la responsabilité des moteurs de recherche (§ 14) et des liens (§ 17). Les §§ 13 ss ECG constituent - tout comme les dispositions de la directive européenne sur le commerce électronique et de la loi allemande TDG - une *réglementation horizontale.*

§ 13 Ausschluss der Verantwortlichkeit bei Durchleitung

(1) Ein Diensteanbieter, der von einem Nutzer eingegebene Informationen in einem Kommunikationsnetz übermittelt oder den Zugang zu einem Kommunikationsnetz vermittelt, ist für die übermittelten Informationen nicht verantwortlich, sofern er

1. die Übermittlung nicht veranlasst,
2. den Empfänger der übermittelten Informationen nicht auswählt und
3. die übermittelten Informationen weder auswählt noch verändert.

(2) Die Übermittlung von Informationen und die Vermittlung des Zugangs im Sinn des Abs. 1 umfassen auch die automatische kurzzeitige Zwischenspeicherung der übermittelten Informationen, soweit diese Zwischenspeicherung nur der Durchführung der Übermittlung im Kommunikationsnetz dient und die Information nicht länger gespeichert wird, als es für die Übermittlung üblicherweise erforderlich ist.

§ 14 Verantwortlichkeit bei Suchmaschinen

(1) Ein Diensteanbieter, der Nutzern eine Suchmaschine oder andere elektronische Hilfsmittel zur Suche nach fremden Informationen bereitstellt, ist für die abgefragten Informationen nicht verantwortlich, sofern er

1. die Übermittlung der abgefragten Informationen nicht veranlasst
2. den Empfänger der abgefragten Informationen nicht auswählt und
3. die abgefragten Informationen weder auswählt noch verändert.

(2) Abs. 1 ist nicht anzuwenden, wenn die Person, von der die abgefragten Informationen stammen, dem Diensteanbieter untersteht oder von ihm beaufsichtigt wird.

[70] Le titre intégral de cette loi est : *Bundesgesetz, mit dem bestimmte rechtliche Aspekte des elektronischen Geschäfts- und Rechtsverkehrs geregelt werden* [loi fédérale permettant de réglementer certains aspects juridiques du commerce électronique et des échanges électroniques de données juridiques]) ; voir BGBl. (autrich.) I n° 152/2001. L'ECG est entrée en vigueur le 1.1.2002 et peut être consultée sur le site Internet suivant : http://www.ris.bka.gv.at/bundesrecht/

§ 15 Ausschluss der Verantwortlichkeit bei Zwischenspeicherungen (Caching)

Ein Diensteanbieter, der von einem Nutzer eingegebene Informationen in einem Kommunikationsnetz übermittelt, ist für eine automatische, zeitlich begrenzte Zwischenspeicherung, die nur der effizienteren Gestaltung der auf Abruf anderer Nutzer erfolgenden Informationsübermittlung dient, nicht verantwortlich, sofern er

1. die Information nicht verändert,
2. die Bedingungen für den Zugang zur Information beachtet,
3. die Regeln für die Aktualisierung der Information, die in allgemein anerkannten und verwendeten Industriestandards festgelegt sind, beachtet,
4. die zulässige Anwendung von Technologien zur Sammlung von Daten über die Nutzung der Information, die in allgemein anerkannten und verwendeten Industriestandards festgelegt sind, nicht beeinträchtigt und
5. unverzüglich eine von ihm gespeicherte Information entfernt oder den Zugang zu ihr sperrt, sobald er tatsächliche Kenntnis davon erhalten hat, dass die Information am ursprünglichen Ausgangsort der Übertragung aus dem Netz entfernt oder der Zugang zu ihr gesperrt wurde oder dass ein Gericht oder eine Verwaltungsbehörde die Entfernung oder Sperre angeordnet hat.

§ 16 Ausschluss der Verantwortlichkeit bei Speicherung fremder Inhalte (Hosting)

(1) Ein Diensteanbieter, der von einem Nutzer eingegebene Informationen speichert, ist für die im Auftrag eines Nutzers gespeicherten Informationen nicht verantwortlich, sofern er

1. von einer rechtswidrigen Tätigkeit oder Information keine tatsächliche Kenntnis hat und sich in bezug auf Schadenersatzansprüche auch keiner Tatsachen oder Umstände bewusst ist, aus denen eine rechtswidrige Tätigkeit oder Information offensichtlich wird, oder,
2. sobald er diese Kenntnis oder dieses Bewusstsein erhalten hat, unverzüglich tätig wird, um die Information zu entfernen oder den Zugang zu ihr zu sperren.

(2) Abs. 1 ist nicht anzuwenden, wenn der Nutzer dem Diensteanbieter untersteht oder von ihm beaufsichtigt wird.

§ 17 Ausschluss der Verantwortlichkeit bei Links

(1) Ein Diensteanbieter, der mittels eines elektronischen Verweises einen Zugang zu fremden Informationen eröffnet, ist für diese Information nicht verantwortlich,

1. sofern er von einer rechtswidrigen Tätigkeit oder Information keine tatsächliche Kenntnis und sich in Bezug auf Schadenersatzansprüche auch keiner Tatsachen oder Umstände bewusst ist, aus denen eine rechtswidrige Tätigkeit oder Information offensichtlich wird, oder,
2. sobald er Kenntnis oder dieses Bewusstsein erlangt hat, unverzüglich tätig wird, um den elektronischen Verweis zu entfernen.

(2) Abs. 1 ist nicht anzuwenden, wenn die Person, von der die Informationen stammen, dem Diensteanbieter untersteht oder von ihm beaufsichtigt wird oder der Diensteanbieter die fremden Informationen als seine eigenen darstellt.

§ 18 Umfang der Pflichten der Diensteanbieter

(1) Die in den §§ 13 bis 17 genannten Diensteanbieter sind nicht verpflichtet, die von ihnen gespeicherten, übermittelten oder zugänglich gemachten Informationen allgemein zu überwachen oder von sich aus nach Umständen zu forschen, die auf rechtswidrige Tätigkeiten hinweisen.

(2) Die in den §§ 13 und 16 genannten Diensteanbieter haben auf Grund der Anordnung eines dazu gesetzlich befugten inländischen Gerichtes diesem alle Informationen zu übermitteln, an Hand deren die Nutzer ihres Dienstes, mit denen sie Vereinbarungen über die Übermittlung oder Speicherung von Informationen abgeschlossen haben, zur Verhütung, Ermittlung, Aufklärung oder Verfolgung gerichtlich strafbarer Handlungen ermittelt werden können.

(3) Die in § 16 genannten Diensteanbieter haben auf Grund der Anordnung einer Verwaltungsbehörde dieser den Namen und die Adressen der Nutzer ihres Dienstes, mit denen sie Vereinbarungen über die Speicherung von Informationen abgeschlossen haben, zu übermitteln, sofern die Kenntnis dieser Informationen eine wesentliche Voraussetzung der Wahrnehmung der der Behörde übertragenen Aufgabe bildet.

(4) Die in § 16 genannten Diensteanbieter haben den Namen und die Adresse eines Nutzers ihres Dienstes, mit dem sie Vereinbarungen über die Speicherung von Informationen abgeschlossen haben, auf Verlangen dritten Personen zu übermitteln, sofern diese ein überwiegendes rechtliches Interesse an der Feststellung der Identität eines Nutzers und eines bestimmten rechtswidrigen Sachverhalts sowie überdies glaubhaft machen, dass die Kenntnis dieser Informationen eine wesentliche Voraussetzung für die Rechtsverfolgung bildet.

(5) Sonstige Auskunfts- und Mitwirkungspflichten der Diensteanbieter gegenüber Behörden oder Gerichten bleiben unberührt.

§ 19 Weitergehende Vorschriften

(1) Die §§ 13 bis 18 lassen gesetzliche Vorschriften, nach denen ein Gericht oder eine Behörde dem Diensteanbieter die Unterlassung, Beseitigung oder Verhinderung einer Rechtsverletzung auftragen kann, unberührt.

(2) Abs. 1 sowie §§ 13 bis 18 sind auch auf Anbieter anzuwenden, die unentgeltlich elektronische Dienste bereitstellen.

4.33 France

La France a procédé à une importante modification du droit touchant les conditions de la punissabilité des prestataires ou fournisseurs. A cette date, la *Loi du 1er août 2000 relative à la liberté de communication*[71,72]) s'est vue rajouter l'art. 43-8, al. 1. Cette disposition figure au chapitre VI (Dispositions relatives aux services de communication en ligne autres que de correspondance privée).

L'art. 43-8, al. 1a introduit le *principe de la responsabilité limitée.* Selon cet article, le prestataire n'est responsable que s'il ne bloque pas l'accès à un site Internet illicite

[71] Voir égal. ci-dessous ch. 9.121.

[72] Lien : http://www.foruminternet.org/texte/documents/lois/lire.phtml?id=22

bien qu'il ait été saisi par une autorité judiciaire. L'art. 48-8, al. 2 établit, en outre, qu'un fournisseur d'hébergement peut également être punissable lorsqu'il a été informé par un utilisateur et n'a pas réagi. Cette disposition a néanmoins été déclarée *anticonstitutionnelle* par le Conseil constitutionnel avant même son entrée en vigueur [73].

Les dispositions du droit français quant à la responsabilité des prestataires sont désormais les suivantes :

> **Art. 43-7.** - Les personnes physiques ou morales dont l'activité est d'offrir un accès à des services de communication en ligne autres que de correspondance privée sont tenues, d'une part, d'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.
>
> **Art. 43-8.** - Les personnes physiques ou morales qui assurent, à titre gratuit ou onéreux, le stockage direct et permanent pour mise à disposition du public de signaux, d'écrits, d'images, de sons ou de messages de toute nature accessibles par ces services, ne sont pénalement ou civilement responsables du fait du contenu de ces services que :
> - si, ayant été saisies par une autorité judiciaire, elles n'ont pas agi promptement pour empêcher l'accès à ce contenu;.[...]
>
> **Art. 43-9.** - Les prestataires mentionnés aux articles 43-7 et 43-8 sont tenus de détenir et de 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.
> Ils sont également tenus de fournir aux personnes qui éditent un service de communication en ligne autre que de correspondance privée des moyens techniques permettant à celles-ci de satisfaire aux conditions d'identification prévues à l'article 43-10.
> Les autorités judiciaires peuvent requérir communication auprès des prestataires mentionnés aux articles 43-7 et 43-8 des données mentionnées au premier alinéa. Les dispositions des articles 226-17, 226-21 et 226-22 du code pénal sont applicables au traitement de ces données.
> Un décret en Conseil d'Etat, pris après avis de la Commission nationale de l'informatique et des libertés, définit les données mentionnées au premier alinéa et détermine la durée et les modalités de leur conservation.
>
> **Art. 43-10.** - I. - Les personnes dont l'activité est d'éditer un service de communication en ligne autre que de correspondance privée tiennent à la disposition du public :
> - s'il s'agit de personnes physiques, leurs nom, prénom et domicile ;
> - s'il s'agit de personnes morales, leur dénomination ou leur raison sociale et leur siège social ;
> - le nom du directeur ou du codirecteur de la publication et, le cas échéant, celui du responsable de la rédaction au sens de l'article 93-2 de la loi no 82-652 du 29 juillet 1982 sur la communication audiovisuelle ;
> - le nom, la dénomination ou la raison sociale et l'adresse du prestataire mentionné à l'article 43-8.
> II. - Les personnes éditant à titre non professionnel un service de communication en

[73] Cf. Décision du Conseil constitutionnel n° 2000-433 DC du 27 juillet 2000, JO du 2 août 2000, 11922 ss, 11926. Pour plus de détails, voir MOREILLON/DE COURTEN, (Bibl.), p. 12, avec d'autres renvois. A propos de l'évolution de cette législation en France suite à la décision du Conseil constitutionnel, voir ci-dessous, ch. 9.121.

ligne autre que de correspondance privée peuvent ne tenir à la disposition du public, pour préserver leur anonymat, que le nom, la dénomination ou la raison sociale et l'adresse du prestataire mentionné à l'article 43-8, sous réserve de lui avoir communiqué les éléments d'identification personnelle prévus au I.

4.34 Italie

Le parlement italien a délégué au gouvernement, entre autres, la mise en application de la directive sur le commerce électronique dans le droit italien en adoptant, le 1er mars 2002, le texte de loi n. 39 intitulé « *Disposizioni per l'adempimento di obblighi derivati dall'appartenenza dell'Italia alle Comunità europee - Legge comunitaria 2001* » ; l'article déterminant est l'art. 31 : *Attuazione della direttiva 2000/31/CE, relativa a taluni aspetti giuridici dei servizi della società dell'informazione, in particolare il commercio elettronico, nel mercato interno*) [74].

La norme de délégation de l'article 1 de la loi communautaire 2001 prescrit au gouvernement d'édicter l'ordonnance requise dans le délai d'un an à partir de l'entrée en vigueur de la loi. Ce délai est depuis écoulé sans qu'aucune démarche n'ait été effectuée [75].

La lutte contre la cybercriminalité découle du mandat constitutionnel visant à empêcher la violation d'un bien juridique. Ce faisant, l'Etat est néanmoins lié par les principes de la constitution et doit en particulier respecter les principes fondamentaux de la libre communication.

[74] Lien : http://www.parlamento.it/parlam/leggi/02039l.htm#31.1

[75] C'est-à-dire après la publication de la loi dans la Gazzetta Ufficiale n° 72 du 26 mars 2002 – Supplemento Ordinario n° 54 .

La lutte contre la cybercriminalité découle du mandat constitutionnel visant à empêcher la violation d'un bien juridique. Ce faisant, l'Etat est néanmoins lié par les principes de la constitution et doit en particulier respecter les principes fondamentaux de la libre communication.

5. Conditions-cadres découlant de la constitution

5.1 Le mandat constitutionnel visant la protection des biens juridiques

5.11 Objet du mandat constitutionnel

Les *libertés* et *droits à l'intégrité* conférés par les *droits fondamentaux* sont des biens juridiques centraux auquel l'Etat est tenu de veiller de par la constitution. Dans un Etat constitutionnel démocratique moderne tel que la Suisse, ils constituent l'un des piliers qui soutiennent l'ensemble de l'ordre juridique et étatique [76].

Cette acception a été expressément concrétisée par l'art. 35, al. 1 de la nouvelle constitution (Cst.) [77] (« Les droits fondamentaux doivent être réalisés dans l'ensemble de l'ordre juridique »). Il n'est actuellement plus question de comprendre les droits fondamentaux comme de simples droits donnés à l'individu pour se défendre contre l'Etat ; bien plus, ils obligent aussi l'Etat à veiller à la protection effective des droits et des libertés qui y sont consignés.

Ainsi, l'art. 10 Cst. (intégrité physique et psychique) ou l'art. 8, al. 2 Cst. (protection contre la discrimination) obligent aussi l'Etat à exercer une protection effective contre les préjudices causés par des particuliers. Le mandat de protection découlant de la constitution *est axé sur le résultat* : il existe indépendamment de l'endroit où la violation du bien juridique a eu lieu et des moyens (techniques) utilisés pour cela. Donc la protection des droits fondamentaux que doit assurer l'Etat couvre aussi la lutte contre les atteintes aux biens juridiques protégés par les droits fondamentaux, notamment lorsque ces atteintes ont comme vecteur les réseaux électroniques de communication.

[76] JÖRG PAUL MÜLLER, Grundrechte, in: Kälin/Bolz (Editeurs), Handbuch des bernischen Verfassungsrechts, Bern/Stuttgart/Wien 1995, p. 29.
[77] RS 101.

5.12 Réalisation du mandat de protection

Un certain nombre de *questions* se posent au législateur confronté au mandat de protection imparti par la constitution (cf. ci-dessus ch. 5.11) :

- Quel *arsenal de mesures législatives* doit-on mettre en place pour empêcher et lutter contre les atteintes portées à des biens juridiquement protégés ? Les recommandations administratives sont-elles suffisantes ou faut-il établir des prescriptions de droit civil, de droit pénal ou de droit administratif ?
- *Contre qui* les dispositions de protection étatiques doivent-elles être dirigées ? Dans quelle mesure doit-on poursuivre (notion de « responsabilité ») les fabricants, propriétaires et exploitants d'installations techniques ?
  - *Droit privé* : doit-on parer au potentiel de préjudice inhérent à toute mesure étatique de protection par l'établissement d'une responsabilité délictuelle, causale ou à raison du risque ?
- *Droit pénal* : doit-on concevoir un élément constitutif d'infraction ayant le caractère de délit intentionnel ou celui délit par négligence ? Dans ce dernier cas, quelle est la portée des devoirs de vigilance ou bien dans quelle mesure est-il possible de présumer des mesures de protection ?
- *Droit administratif* : les mesures de police visant la protection de biens juridiques protégés par les droits fondamentaux ne doivent-elles viser que les personnes qui sont à l'origine de leur mise en danger ou de leur entrave par leur comportement propre ou par celui de tiers placés sous leur responsabilité (« perturbateur par comportement ») [78] ? Ou bien les mesures de police doivent-elles aussi s'appliquer aux personnes qui possèdent la puissance légale ou de fait sur la chose qui provoque l'état non conforme aux règles (« perturbateur par situation ») [79] ? Dans quelle mesure doit-on également inclure les personnes dont l'action ou la négligence font que d'autres mettent en danger ou portent atteinte à des biens juridiques protégés par les droits fondamentaux (« auteur indirect ») [80] ?

5.2 Le cadre constitutionnel de la protection des biens juridiques

A première vue, les questions formulées ci-dessus (ch. 5.12) semblent être de nature purement politique et nécessiter des réponses en conséquence. Dans la réalité, le législateur n'a pas toute liberté pour concevoir les mesures visant à empêcher les atteintes aux biens juridiques. En effet, il est lié par la *constitution* à plusieurs égards.

---

[78] Cf. notamment ATF 122 II 70; 118 Ib 415. – par exemple, dans ce contexte, un fournisseur de contenu pourrait être un « *perturbateur par comportement* ».

[79] Cf. notamment ATF 122 II 70; 118 Ib 415. – par exemple, dans ce contexte, un fournisseur d'hébergement pourrait être un « *perturbateur par situation* ».

[80] Cf. à ce propos ATF 99 Ia 511; HÄFELIN/MÜLLER (Bibl.), ch. marg. 2497 ss; DANIEL THÜRER, Das Störerprinzip im Polizeirecht, in : RDS 102 (1983) I 463 ss, 477 s. – dans le cas présent, on pourrait éventuellement qualifier un fournisseur d'accès d'« auteur indirect ».

5.21 Protection efficace des droits fondamentaux

De par la constitution (art. 35, al. 1 Cst.), le législateur est tenu de veiller à une protection *effective* et *efficace* des droits fondamentaux [81]. Ce précepte doit guider son choix des moyens de réglementation.

5.22 Répartition des compétences de la Confédération

Les droits fondamentaux ne permettent pas de déduire de nouvelles compétences de la Confédération. La protection des droits fondamentaux doit être réalisée en vertu du régime de répartition des compétences telle qu'il résulte de la Constitution (art. 42 ss Cst.) [82]. Les mesures de droit fédéral visant la protection des biens juridiques protégés par les droits fondamentaux ne sont donc admises dans le présent contexte que si la constitution fédérale établit à cet effet une compétence fédérale pour le domaine des réseaux de télécommunication [83].

5.23 L'assise institutionnelle des droits fondamentaux

Le législateur doit concevoir les mesures de protection requises dans le respect des droits des libertés, dans le cas présent *des droits fondamentaux de la libre communication* [84] .

A ce propos, il convient de souligner en premier lieu leur rôle fondamental au sein des institutions démocratiques. La *doctrine* [85] et la *jurisprudence* [86] considèrent les droits fondamentaux de la libre communication non seulement comme un élément indispensable à l'épanouissement de l'individu ; ils leur attribuent aussi une *fonction primordiale dans une société démocratique*.

Néanmoins, le débat démocratique doit être protégé non seulement des atteintes directes, mais aussi des atteintes indirectes. Il peut, par exemple, y avoir atteintes indirectes lorsque des mesures entravent concrètement la libre communication par la menace de sanctions *frappant des déclarations illicites* ; ces atteintes indirectes ont

---

[81] DFJP, Réforme de la Constitution fédérale, Exposé des motifs du projet de Constitution de 1995, Berne 1995, p. 64; RENÉ RHINOW, Die Bundesverfassung 2000, Eine Einführung, Basel/Genf/München 2000, p. 152; PETER SALADIN, Grundrechte im Wandel, 3e paragraphe, Berne 1982, p. 294 ss, PETER SALADIN, Die Funktion der Grundrechte in einer revidierten Verfassung, in: Die Kunst der Verfassungsrevision, Schriften zur Verfassungsreform 1968-1996, Basel/Frankfurt a. M. 1998, p. 47 ss, 57 ss

[82] Voir notamment JEAN-FRANÇOIS AUBERT, Bundesstaatsrecht der Schweiz, version de 1967, supplément remanié jusqu'à 1990, vol. I, Basel/Frankfurt a. M. 1991, ad n. 699; HÄFELIN/HALLER (Bibl.), ch. marg. 1070.

[83] Cf. à ce propos ci-dessous ch. 7.12.

[84] Art. 16 et 17 Cst.; cf. égal. art. 10 CEDH.

[85] ANDREAS AUER/GIORGIO MALINVERNI/MICHEL HOTTELIER, Droit constitutionnel suisse, Volume II: Les droits fondamentaux, Berne 2000, ch. marg. 486; HÄFELIN/HALLER (Bibl.), ch. marg. 447; MÜLLER, GRUNDRECHTE (Bibl.), p. 183 s.; JÖRG PAUL MÜLLER, § 39 Allgemeine Bemerkungen zu den Grundrechten, in: Thürer/Aubert/Müller (Editeurs), Verfassungsrecht der Schweiz/Droit constitutionnel suisse, Zurich 2001, ch. marg. 16, p. 628.

[86] ATF 96 I 592.

donc un effet dissuasif sur les citoyennes et les citoyens [87]. Pour la même raison, les atteintes aux droits fondamentaux de la libre communication nécessitent une *base légale suffisamment précise* [88].

5.24 Respect des droits fondamentaux protégés

La mise en place des mesures de protection par le législateur doit tenir compte des positions protégées en vertu des droits fondamentaux des *destinataires* de ces mesures, ainsi de celles des *tierces personnes*. Les atteintes à ces droits fondamentaux nécessitent une base légale suffisante [89], doivent pouvoir être justifiées par un intérêt public ou par la protection des droits fondamentaux de tiers; en outre, elles doivent être proportionnées. L'essence des droits fondamentaux est inviolable (art. 36, al. 1 à 4 Cst.).

5.241 Destinataires

En qualité de principaux destinataires des mesures de protection dont il est ici question, les *fournisseurs Internet* sont protégés en premier lieu par le droit fondamental générique de la *liberté d'opinion* (art. 16, al. 1 Cst.). Ils peuvent à ce propos invoquer notamment le droit fondamental de la *liberté des médias* (art. 17 Cst.) qui abrite dans son essence inviolable *l'interdiction de la censure préalable* (art. 17, al. 2 en rel. avec l'art. 36, al. 4 Cst.). Outre la libre transmission d'informations par la presse, la radio et la télévision, la liberté des médias protège aussi d'autres formes de diffusion de productions et d'informations ressortissant aux télécommunications publiques, notamment l'Internet [90].

Les fournisseurs peuvent invoquer par ailleurs la *liberté économique* (art. 27 Cst.). Par contre, lorsqu'ils assurent des services dit universels [91] et assument ainsi une tâche de l'Etat au sens de l'art. 35, al. 2 Cst., ils ne peuvent invoquer l'art. 27 Cst. [92].

---

[87] Cf. à ce propos essent. JÖRG PAUL MÜLLER/MARKUS SCHEFER, Grundrechtliche Fragen zum Internet, Medialex 1997, p. 198 ss, 203 : « Eine Verpflichtung von Anbietern (Systembetreiber, Diensteanbieter oder Inhaltsanbieter), nur legale Publikationen zu verbreiten, dürfte u.E. daher aus grundrechtlicher Sicht nur soweit gehen, als dadurch keine substantiellen Einbussen der Auseinandersetzung über Fragen von gesellschaftlichem Interesse am Internet zu befürchten sind. »

[88] Cf. MÜLLER, GRUNDRECHTE (Bibl.), p. 210 s.

[89] Par ailleurs, le principe de la légalité sert notamment à concrétiser le principe constitutionnel de la *sécurité du droit* (art. 5 Cst.). Celui-ci oblige également le législateur à établir des normes connues à l'avance et de portée générale. Cf. sur l'ensemble de la question YVO HANGARTNER, art. 5 Cst., in: Ehrenzeller/Mastronardi/Schweizer/Vallender (Editeurs), Die schweizerische Bundesverfassung, Kommentar, Zurich/Bâle/Genève 2002, n. 8; HÄFELIN/MÜLLER, (Bibl.), n. 372.

[90] Cf. sur l'ensemble de la question DENIS BARRELET, § 45 Les libertés de la communication, in: Thürer/Aubert/Müller (Editeurs), Verfassungsrecht der Schweiz/Droit constitutionnel suisse, Zurich 2001, p. 721 ss, ch. marg. 40 ss; voir égal. MÜLLER, GRUNDRECHTE (Bibl.), p. 275. – A propos de la communication qui ne s'adresse pas au public en général, le Tribunal fédéral permet aussi aux fournisseurs de courrier électronique d'invoquer le droit fondamental du *secret des télécommunications* (art. 13, al. 1 Cst.); ATF 126 I 50 ss, 57.

[91] Cf. art. 92, al. 2 Cst., art. 1, al. 2, let. a et art. 14 ss LTC.

[92] Cf. à ce propos égal. GIOVANNI BIAGGINI, § 49 Wirtschaftsfreiheit, in : Thürer/Aubert/Müller (Editeurs), Verfassungsrecht der Schweiz/Droit constitutionnel suisse, Zurich 2001, p. 779 ss, ch. marg. 11 avec renvois ; ISABELLE HÄNER, Grundrechtsgeltung bei der Wahrnehmung staatlicher Aufgaben durch Private, in : AJP/PJA 2002, p. 1144 ss, 1146, 1150.

5.242 Tierces personnes

La *liberté d'information* des *utilisateurs* d'Internet doit être protégée (art. 16, al. 1 et 3 Cst.). Cette liberté couvre, entre autres, le droit de recevoir librement des informations. Sont considérées comme « librement recevables » notamment les émissions de radio qui sont diffusées par voie hertzienne ou par le câble [93], ainsi que les informations diffusées par Internet [94].

5.25 Proportionnalité

5.251 En général

Chargé d'accomplir le mandat de protection qui a pour objet la lutte contre la discrimination et les violations de l'intégrité, jusqu'où le législateur peut-il intervenir dans les droits fondamentaux de la libre communication ? La réponse à cette question doit être envisagée sous l'angle du *principe de la proportionnalité* (art. 36, al. 3 Cst.; art. 5, al. 2 Cst.)[95]. Pour être considérées comme proportionnées, les mesures doivent être *aptes* à concrétiser le but visé et, de plus, *nécessaires* et *raisonnablement exigibles*.

5.252 Adéquation

Le principe de la proportionnalité interdit les mesures limitant les droits fondamentaux lorsqu'elles ne contribuent pas à atteindre le but visé et sont de ce fait inadéquates. Outre sa dimension politique, l'objection formulée contre la prise en compte dans le droit des activités des fournisseurs d'accès - selon laquelle il serait facile, du point de vue technique, de contourner les blocages d'accès - reçoit de ce point de vue une assise juridique. Il en va de même des prescriptions qui obligent les fournisseurs à installer des programmes de filtrage. En effet, il est aujourd'hui possible de contourner pratiquement tous les filtres [96].

5.253 Nécessité

Le principe de la proportionnalité interdit par ailleurs les mesures qui - de par leur champ d'application à raison des personnes ou de la matière, ou encore de leur champ d'application géographique et temporel - vont au-delà de ce qui est nécessaire pour atteindre le but visé par la réglementation (donc la protection des biens juridiques menacés).

---

[93] Cf. ATF 120 Ib 64 ss ; MÜLLER, GRUNDRECHTE (Bibl.), p. 292 s.
[94] Cf. à ce propos RAIMUND KROPP, Zensur im Internet, in : perspektive 21, Brandenburgische Hefte für Wissenschaft und Politik, Informationsgesellschaft, Heft 3/1998, p. 28 ss, 29.
[95] Le législateur demeure lui aussi lié par ce principe, cela malgré l'art. 191 Cst.
[96] Cf. à ce propos SEMKEN (Bibl.), p. 249 ss, 269.

5.254 Exigibilité

Pour être proportionnées, les mesures de protection doivent en outre pouvoir être raisonnablement exigées de la personne concernée. La « responsabilité » personnelle [97] de la cybercriminalité trouve donc sa limite dans le caractère exigible de sa prise en compte dans le droit pour les prestataires ou fournisseurs.

En *droit pénal*, la responsabilité (hormis les délits intentionnels) ne peut aller que jusqu'à la limite de ce qui semble exigible comme mesure de protection, de sorte que le non-respect de celle-ci doit être simplement qualifié de manquement au devoir de diligence et, de ce fait, de négligence.

En *droit privé* aussi, la critère de l'exigibilité est pris en compte lorsqu'il s'agit d'introduire une responsabilité causale simple ou stricte.

En *droit administratif* également, l'auteur indirect n'est considéré comme perturbateur que lorsqu'on peut équitablement lui imposer l'intervention de la police, en d'autres termes lorsque cette intervention apparaît proportionnée dans la perspective de la protection du bien juridique.

5.26 Egalité devant la loi et arbitraire

Indépendamment de la portée des positions protégées par les droits fondamentaux du fournisseur d'Internet, le législateur demeure lié par *le principe de l'égalité devant la loi* (art. 8 Cst.) et par *l'interdiction de l'arbitraire* (art. 9 Cst.).

Ainsi, le fait de considérer que l'illicéité d'une représentation sur Internet va plus loin que s'il s'agissait d'une publication dans un autre média (par ex., dans la presse écrite) [98] peut être problématique au regard du droit constitutionnel. Le principe de l'égalité devant la loi n'empêche certes pas le législateur de tenir compte du potentiel de danger spécifique à chaque média par une différenciation des prescriptions. Néanmoins, un traitement inégal doit reposer sur des raisons objectives. Dans ce sens, il peut se justifier d'établir des réglementations différentes pour les différents médias qui ont, chacun, un impact différent sur le public [99] ou un public cible différent, ainsi que - par voie de conséquence - un mode de diffusion différent [100].

La mise en place de réglementations plus sévères - comparativement à celles qui ont cours dans les autres pays (voisins) - peut se traduire par un désavantage pour le prestataire suisse, désavantage qui peut se révéler problématique du point de vue du droit constitutionnel.

---

[97] La notion de responsabilité s'entend ici au sens large et englobe les acceptions spéciales en droit pénal, droit civil et droit constitutionnel ; la *directive de l'UE sur le commerce électronique* semble aussi comprendre la responsabilité dans ce sens ; cf. en particulier le titre de sa Section 4 (voir à ce propos ci-dessus chapitre 4).

[98] Cf. MÜLLER, GRUNDRECHTE (Bibl.), p. 246 s.

[99] Ainsi, l'interdiction de la violence prescrite par l'art. 135 CP ne porte que sur les enregistrements sonores ou visuels, et non sur le mot écrit.

[100] L'interdiction de la pornographie figurant à l'art. 197, ch. 1 CP traite les déclarations de caractère pornographique à la radio et à la télévision de manière plus sévère que les écrits pornographiques, enregistrements pornographiques sonores ou visuels qui peuvent être offerts aux personnes de moins de 16 ans.

Le droit pénal actuel ne répond ni clairement ni de manière satisfaisante aux questions majeures en rapport avec la poursuite et la répression des infractions commises sur les réseaux.

6. Cybercriminalité et droit pénal actuel

6.1 Généralités

6.11 Exposé de la question

Contrairement à d'autres activités criminelles, l'auteur d'une infraction relevant de la cybercriminalité doit nécessairement recourir à *l'infrastructure technique* fournie par un grand nombre de participants (souvent des personnes morales) [101]. Une autre caractéristique essentielle des prestations offertes par les fournisseurs d'hébergement, de réseaux et d'accès [102] est le *déroulement* largement *automatisé* de ces processus.

En raison du parallélisme [103] avec le *droit pénal des médias*, il convient en premier lieu de déterminer si les éléments constitutifs de la cybercriminalité tombent sous le coup de l'art. 27 et de l'art. 322 [bis] CP [104] ou s'ils doivent être appréciés à la lumière des *règles générales du code pénal*, à savoir plus particulièrement celles concernant la complicité (art. 25 CP) [105].

En outre, l'infraction, les prestations d'infrastructure des autres participants ainsi que la consultation des informations par les utilisateurs peuvent être situées en des lieux géographiques tout à fait différents. De ce fait, la cybercriminalité est souvent *internationale* et soulève la question de savoir dans quels cas la Suisse possède une compétence juridictionnelle et quels sont les comportements qui y sont soumis [106].

S'ajoutent à cela la question des *compétences en matière d'enquête* (délimitation de la compétence fédérale et de la compétence cantonale, art. 340 ss CP) et la question du for (compétence locale, art. 346 ss CP).

---

[101] A propos des participants et de leurs fonctions, voir ci-dessus chapitre 2, ch. 3.

[102] A savoir la mise à disposition et la transmission d'informations sur les réseaux.

[103] Là aussi, il s'agit de la publication (préparation), diffusion et consommation (utilisation) d'informations. En outre, un grand nombre de personnes participent à leur publication et à leur diffusion.

[104] Voir à ce propos ci-dessous ch. 6.2.

[105] Voir à ce propos ci-dessous ch. 6.3.

[6] Voir à ce propos ci-dessous ch. 6.4.

6.12 La notion de cybercriminalité

La notion de cybercriminalité englobe un grand nombre de délits [107] qui obéissent à des définitions très diverses et que l'on peut soumettre à des types de classification très différents. Le *tableau* ci-dessous contient une sélection des délits majeurs les plus courants liés à l'utilisation du réseau informatique, dits *cyberdélits* (première colonne). Elle est basée sur le *type de délit*, dont dépend la question de la localisation du délit en Suisse (2e colonne). Dans la plupart des cas, la compétence judictionnelle de la Suisse repose sur ce critère de rattachement. Elle est la condition fondamentale à toute poursuite pénale en Suisse. Enfin, les éléments constitutifs du délit sont classés selon leur appartenance, ou non, aux *délits de média* et tombent, ou non, sous le coup des réglementations spéciales des art. 27 et 322bis CP (3e colonne). Cette répartition correspond à la jurisprudence actuelle du Tribunal fédéral - si tant est qu'il y en ait déjà une - et tente de donner une image de la situation juridique actuelle. Quelques-unes de ces classifications n'ont toutefois pas encore été clarifiées sur le plan juridique et sont contestées dans la doctrine.

Les principaux types de cyberdélits et leur rapport avec le droit pénal des médias [108]

ELÉMENTS CONSTITUTIFS DU DÉLIT	TYPE DE DÉLIT	DÉLITS DE MÉDIA [109]
Représentation de la violence, art. 135 CP	Délit de mise en danger abstraite	Pas de délit de média
Soustraction de données, art. 143 CP	Délit matériel [110] (classif. litigieuse. Autre interprétation : délit formel)	Pas de délit de média
Accès indu à un système informatique (« piratage informatique »), art. 143bis CP	Délit matériel [111] (litigieux. Autre interprétation : délit formel)	Pas de délit de média
Détérioration de données, art. 144bis, ch. 1 CP (effacer, modifier, mettre hors d'usage)	Délit matériel	Pas de délit de média
Détérioration de données, art. 144bis, ch. 2 CP (état de fait « virus informatique »)	Délit de mise en danger abstraite (ch. 2)	Pas de délit de média (hormis évent. dans la variante consistant à fournir des indications)
Escroquerie, art. 146 CP	Délit matériel	Pas de délit de média
Utilisation frauduleuse d'un ordinateur, art. 147 CP	Délit matériel	Pas de délit de média

[107] Cf. ci-dessus chapitre 2, ch. 2.2.

[108] Cf. SCHWARZENEGGER, E-COMMERCE (Bibl.), p. 342 et 350.

[109] Cf. ATF 125 IV 206 ss, qui ne s'exprime toutefois de manière explicite qu'à propos de la classification des représentations de la violence (art. 135 CP), de la pornographie dure (art. 197, ch. 3 CP) et du négationnisme (art. 261bis, al. 4 CP). Les autres classifications n'ont donc pas (encore) été clarifiées par le Tribunal fédéral. Pour une classification selon le point de vue du Tribunal fédéral, voir TRECHSEL/NOLL, (Bibl.), p. 229 avec renvois; AVIS OFJ (Bibl.), p. 834 s.

[110] SCHWARZENEGGER, GELTUNGSBEREICH (Bibl.), p. 122, selon lesquels un résultat dissociable du point de vue spatial et temporel est établi; autre avis NIKLAUS SCHMID, Criminalité découlant de l'utilisation des ordinateurs, des chèques et des cartes de crédit, Zurich 1994, CP 143, n. 17 et CP 143bis, n. 11; CASSANI, (Bibl.), p. 253.

[111] Voir note précédente.

Manipulation de cours, art. 161bis CP	**Délit de mise en danger abstraite**	Cas incertain, probablement délit de média (dans la variante de la diffusion de l'information)
Délits contre l'honneur, art. 173 ss CP	Délits matériels	Délits de média
Pornographie douce, art. 197, ch. 1 CP (protection de la jeunesse)	Délit de mise en danger abstraite	Cas incertain, probablement pas un délit de média
Pornographie douce, art. 197, ch. 2 CP (protection des adultes de la confrontation involontaire avec la pornographie)	Délit de mise en danger concrète	Pas un délit de média
Pornographie dure, art. 197, ch. 3 CP	Délit de mise en danger abstraite	Pas un délit de média
Fabrication, dissimulation, transmission à autrui d'explosifs et de gaz toxiques, art. 226, al. 3 CP (fournir des indications pour la fabrication)	Délit de mise en danger abstraite	Cas incertain, probablement pas un délit de média car le délit n'est pas consommé sous forme de publication (nécessité de fournir des indications à certaines personnes)
Menace alarmant la population, art. 258 CP	Délit matériel	Pas un délit de média
Provocation publique au crime ou à la violence, art. 259 CP	Délit de mise en danger abstraite	Délit de média
Discrimination raciale, art. 261bis CP	Délit formel	Pas un délit de média (al. 4, négationnisme), de même pour l'al. 1-3
Service de renseignements économiques, art. 273 CP	Délit de mise en danger abstraite	Cas incertain, probablement délit de média
Provocation et incitation à la violation des devoirs militaires, art. 276 CP	Délit de mise en danger abstraite	Délit de média
Publication de débats officiels secrets, art. 293 CP	Délit de mise en danger abstraite	Délit de média
Violation du secret de fonction, art. 320 CP	Délit formel	Délit de média
Violation du secret professionnel, art. 321 CP	Délit formel	Délit de média
Violation du droit d'auteur Confectionner des exemplaires d'une oeuvre, art. 67, al. 1, let. e LDA Proposer, aliéner ou mettre en circulation des exemplaires d'une œuvre, art. 67, al. 1, let. f LDA	Délit formel Délit formel	Pas un délit de média Pas un délit de média (sauf évent. dans la variante de la proposition)
Violation de droits voisins notamment art. 69, al. 1, let. c et f LDA	Délit formel	Pas un délit de média
Méthodes déloyales de publicité et de vente, notamment art. 3 en liaison avec art. 23 LCD	Délit de mise en danger abstraite	Délit de média

6.2 Punissabilité selon le droit pénal des médias ?

6.21 Les nouvelles dispositions du droit pénal des médias

Pour qu'il y ait délit de média, il faut que l'infraction soit commise et *consommée sous forme de publication par un média*. Conformément aux art. 27 et 322bis CP, ces délits sont soumis à un régime spécial de responsabilité quant à la participation au processus de publication [112]. En principe, seul l'auteur de la publication illégale est punissable (art. 27, al. 1 CP). Si ce dernier ne peut être découvert ou ne peut être traduit en Suisse devant un tribunal (art. 27, al. 2 CP), il découle de l'art. 322bis une punissabilité subsidiaire et exclusive du rédacteur responsable ou, à défaut, de la personne responsable de la publication en cause.

Selon cette disposition pénale en vigueur depuis le 1er avril 1998, le fait de ne pas s'opposer *intentionnellement* à une publication incriminée peut être puni de l'emprisonnement ou de l'amende. Le caractère punissable de l'infraction a néanmoins été renforcé par rapport à l'ancien droit pénal de la presse en ce sens que le fait de ne pas empêcher *par négligence* la publication est désormais aussi punissable. L'art. 27 CP ne contenant pas d'énumération des délits de média, la liste des éléments constitutifs du délit concernés par cette réglementation doit être établie par l'interprétation de ceux-ci (cf. tableau ci-dessus, 3^{e} colonne ; des incertitudes demeurent dans certains cas).

6.22 Un nouvel arrêt du Tribunal fédéral sur la notion de délit de média

La situation s'est compliquée depuis un arrêt rendu par le Tribunal fédéral en 1999, selon lequel toute publication faite dans un média et consommée sous forme de publication ne constitue pas nécessairement un délit de média [113]. Dans cet arrêt, le Tribunal fédéral mentionne explicitement les représentations de la violence (art. 135 CP), la pornographie dure (art. 197, ch. 3 CP) et le négationnisme (notamment par le « mensonge d'Auschwitz », art. 261bis, al. 4 CP) comme n'étant pas à compter parmi les délits de média.

Le Tribunal fédéral *motive* en premier lieu sa position par le fait que le législateur, pour ce qui est des délits qui ne sont pas délits de média, entendait *empêcher* précisément la publication des contenus incriminés et, de ce fait, ne voulait guère mettre un groupe déterminé de responsables au bénéfice d'un régime de faveur. Par ailleurs, toujours dans les cas de délits « non médiatiques », il estimerait tout à fait contraire au but poursuivi par le législateur d'accorder un traitement privilégié à la diffusion par les médias. Enfin, le Tribunal fédéral a estimé qu'en matière de discrimination raciale, la Suisse *est tenu, en vertu du droit international public*, de poursuivre sans exception toute diffusion de propos raciste [114] depuis la ratification de la Convention internationale contre la discrimination raciale.

---

[112] A propos de la genèse et du sens de la réglementation spéciale en droit des médias, voir RIKLIN, (Bibl.), p. 243 ss; ZELLER (Bibl.) n. 3 et 10 ss.

[113] ATF 125 IV 211 s., de même que SCHULTZ, PRESSEDELIKT (Bibl.), p. 278 et TRECHSEL/NOLL (Bibl.), p. 229. Cf. AVIS OFJ (Bibl.), p. 832 ss.

[114] TRECHSEL/NOLL (Bibl.), p. 230.

La question fondamentale qui se pose ici est de savoir si le *traitement privilégié* de la responsabilité des médias n'équivaut pas à une violation du *principe de l'égalité de traitement* (art. 8, al. 1 Cst.), ce qui le rendrait contraire à la constitution. Il convient d'y objecter que le droit pénal de la presse avait été introduit dans l'idée que le droit pénal ordinaire ne tenait pas suffisamment compte des besoins d'une presse libre et que la satisfaction de ces besoins passait obligatoirement par une limitation de la punissabilité des participants au produit de la presse [115]. La libre circulation des informations et le libre échange des opinions ne constituent pas seulement un élément indispensable au *développement de l'être humain*; ils représentent également le fondement de tout Etat démocratique. Dans la nouvelle réglementation du droit pénal des médias, le législateur suisse a décidé de conserver le régime de faveur - il avait notamment en vue la *protection de la liberté des médias* (cf. art. 17 Cst.). Il convient donc d'admettre que *toutes les publications par un média devraient être appréciées à la lumière des art. 27 et 322bis CP* dans les cas où l'infraction a été consommée sous forme de publication.

Pour cette raison, la classification des délits de média selon les critères de l'ATF 125 IV 206 ss demeure *discutable* (cf. plus haut tableau, 3^{e} colonne). Cette décision a également suscité de nombreuses *critiques* [116]. En fait, les arguments invoqués par le Tribunal fédéral permettent d'exclure du domaine d'application du droit pénal des médias tous les délits d'expression et de diffusion car les normes pénales visent dans tous les cas l'interdiction de déclarations non autorisées dans toutes les variantes de diffusion - que le contexte soit celui des médias ou non. Cela vaudrait par exemple aussi pour *les délits contre l'honneur* qui englobent les modes de commission les plus divers (verbe, écriture, image, geste ou tout autre moyen, cf. art. 176 CP).

6.23 Trois essais d'interprétation

6.231 Les prestataires sont responsables de la publication - applicabilité du droit pénal des médias

Un premier essai d'interprétation de l'art. 27 CP [117] considère Internet comme moyen de communication de masse, ce qui induit, en principe, l'applicabilité des art. 27 et 322bis CP aux publications sur le web. Dans ce cas, seul le *fournisseur de contenu* est punissable s'il peut être découvert ou s'il peut être traduit en Suisse devant un tribunal.

Si le fournisseur de contenu ne peut pas être déterminé, le fournisseur d'hébergement est subsidiairement responsable aux conditions prévues par l'art. 27, al. 2 CP. C'est lui qui permet à l'auteur ou au fournisseur de contenu d'apparaître sur

---

[115] Sten Bull SR 1931, p. 68 et 76; pour plus de détail, voir ZELLER (Bibl.), n. 10 ss

[116] FRANZ RIKLIN, Kaskadenhaftung – quo vadis?, Medialex 2000, p. 208; RIKLIN/ STRATENWERTH, (Bibl.), p. 13 ss; DORRIT SCHLEIMINGER/CHRISTOPH METTLER, Strafbarkeit der Medienverantwortlichen im Falle der Rassendiskriminierung, art. 27, art. 261bis, al. 4 CP, remarques relatives à l'ATF 125 IV 206 ss, AJP 2000, p.1039 ss; REHBERG/ DONATSCH (Bibl.), p. 166; SCHWARZENEGGER, E-COMMERCE (Bibl.), p. 349 ss; RIKLIN (Bibl.), p. 245; ZELLER (Bibl.), n. 32.

[117] Message concernant la modification du code pénal suisse et du code pénal militaire (droit pénal des médias et droit de procédure), FF 1996 IV 535 et 558; AVIS OFJ (Bibl.), p. 832 ss avec renvoi.

Internet avec ses contenus et constitue donc, selon cette conception, le responsable de la publication. Sa punissabilité est régie par l'art. 322bis CP – dans la mesure où il y a délit de média.
En outre, selon cette conception, le *fournisseur d'accès* est également considéré comme responsable subsidiaire de la publication au sens de l'art. 27, al. 2 CP, au cas où ni le fournisseur de contenu ni le fournisseur d'hébergement ne peuvent être découverts ou ne peuvent être traduits devant un tribunal. La punissabilité du fournisseur d'accès découle donc aussi de l'art. 322bis CP [118].

6.232 Les prestataires ne sont pas responsables de la publication - applicabilité des règles générales

La *seconde tentative d'interprétation* reproche au point de vue exprimé plus haut de négliger la différence entre la fonction de média de la Toile, fonction qui s'exerce exclusivement dans le cadre du processus électronique de publication (préparation), et sa fonction de télécommunication, fonction qui englobe tous les aspects techniques du stockage et de la transmission des données (mise à disposition, transmission proprement dite) [119]. Cette opinion ne se vérifie que pour les entreprises de médias qui publient leurs contenus parallèlement en ligne et hors ligne sur un serveur qui leur appartient (préparation = publication)[120].

Normalement toutefois, le *fournisseur d'hébergement* ne participe pas activement au processus de publication du fournisseur de contenu, pas plus qu'il ne surveille passivement les transmissions d'informations. Les données sont mises en mémoire par le fournisseur de contenu, au moyen d'un logiciel de *web publishing,* directement et automatiquement par un serveur du fournisseur d'hébergement. En d'autres termes, le fournisseur d'hébergement exploite *uniquement l'infrastructure technique* permettant de mettre à disposition les informations et ne constitue donc pas - sauf pour ce qui est de l'exception mentionnée au paragraphe précédent - une personne responsable de la publication [121]. Assumant cette fonction, il ne tombe pas du tout dans le domaine de réglementation du droit pénal des médias, bien qu'il faille néanmoins, selon cette conception, considérer une punissabilité conformément aux conditions générales de la complicité (cf. à ce propos ci-dessous ch. 6.3) [122].

---

[118] Avis OJF (Bibl.), p. 841 ss

[119] Explicité par NIGGLI/SCHWARZENEGGER (Bibl.), p. 65 s.

[120] Exemple : un quotidien publie un article simultanément dans son édition du matin (imprimée) et sur son site Internet, qu'il exploite lui-même. Il y a également participation directe au processus de publication lorsque le fournisseur d'hébergement reçoit les informations sur un support de données afin de les publier ensuite sur son serveur pour le fournisseur de contenu.

[121] Cf. REHBERG/DONATSCH (Bibl.), p. 167: « [es] muss … sich dabei um Personen handeln, die einerseits eine medienspezifische Tätigkeit ausüben und denen andererseits Verantwortung für den Inhalt der Publikation innerhalb des betreffenden Mediums zukommt. »

[122] Ce point de vue rejette une extension du droit pénal des médias aux diffuseurs techniques du contenu. Voir RIKLIN/STRATENWERTH (Bibl.), p. 19 s.; SCHWARZENEGGER, E-COMMERCE (Bibl.), p. 351; NIGGLI/SCHWARZENEGGER (Bibl.), p. 62; RIKLIN (Bibl.), p. 251. Cf. la réglementation explicite à ce propos en vigueur aux Etats-Unis, section 230(c) (2) Communications Decency Act: « 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. »

Le *fournisseur d'accès*, lui non plus, ne participe pas à la publication de contenus interdits sur des serveurs d'autrui. Sa prestation se limite à fournir un accès à Internet. La transmission de données déclenchée par l'utilisateur se déroule automatiquement et sans surveillance. S'agissant ici d'une sorte de « complicité » en faveur de l'utilisateur qui cherche et interroge les informations sur Internet, le fournisseur d'accès ne relève en aucune manière du domaine de réglementation des art. 27, al. 2 et 322bis CP [123].

6.233 Les prestataires ne sont pas responsables de la publication — Applicabilité du droit pénal des médias

A l'instar de la conception précédente, ce *troisième essai d'interprétation* exclut les fournisseurs d'hébergement et d'accès de la responsabilité au sens de l'art. 27, al. 2 CP. Mais du fait que le cercle des personnes responsables à titre subsidiaire selon l'art 27, al. 2 CP ne recouvre pas le cercle des personnes qui ne sont pas exposées à une sanction pénale, cette troisième conception n'exclut pas que les fournisseurs d'hébergement et les fournisseurs d'accès tombent tout de même sous le coup de la réglementation spéciale de l'art. 27 CP. Les personnes rendant concrètement accessible au public un écrit (ci-après les *diffuseurs*) qui ne figurent pas dans l'énumération légale des personnes responsables à titre subsidiaire peuvent, selon ce point de vue, être exclues de toute responsabilité pénale indépendamment de leur contribution à l'infraction [124].

Le *Tribunal fédéral* a statué dans ce sens récemment, dans un cas relevant du droit pénal de la pressele contexte d'un état de faits touchant le droit pénal de la presse (Campagne d'affiches diffamatoires, ATF 128 IV 53). Cet arrêt dénie la responsabilité pénale des personnes qui, dans le cadre de leur fonction dans la chaîne de production et de diffusion, se limitent à diffuser dans le public un écrit constitutif d'une infraction. Conformément à cet arrêt, le *diffuseur* d'un contenu illicite ne peut être considéré comme punissable que s'il agit en dehors du cadre de l'activité de la presse, c'est-à-dire en dehors de la chaîne de production et de diffusion (ATF 128 IV 68).

Si l'on soumet la publication et la diffusion sur Internet à cette interprétation, les fournisseurs d'hébergement tout comme les fournisseurs d'accès font partie des *diffuseurs* qui devraient *demeurer impunis* [125]. Les résultats choquants pouvant découler de cette situation de privilège considérable [126] doivent être contrecarrés par une limitation du champ d'application du droit pénal des médias [127].

---

[123] RIKLIN/STRATENWERTH (Bibl.), p. 21; REHBERG/DONATSCH (Bibl.), p. 169; SCHWARZENEGGER, E-COMMERCE (Bibl.), p. 351 s.; WEBER (Bibl.), p. 547; NIGGLI/SCHWARZENEGGER (Bibl.), p. 62.

[124] ZELLER (Bibl.), n. 32. Cf. égal. à ce propos RIKLIN (Bibl.), p. 250 s.

[125] Cf. ZELLER (Bibl.), n. 35 ss et 56 s. (point encore en suspens).

[126] On peut penser aux domaines sensibles tels que la pornographie (art. 197 CP), l'incitation au crime ou à la violence (art. 259 CP) ou la discrimination raciale (art. 261bis CP).

[127] Le Tribunal fédéral s'est déjà engagé dans cette direction dans l'ATF 125 IV 206 ss.

6.24 L'art. 27 CP n'est pas adapté à l'Internet

Les différences d'interprétation soulignées au ch. 6.23, mettent en évidence que le champ d'application du droit pénal des médias *manque de clarté*. En effet, d'une part, le groupe des délits de média (« délit consommé sous forme de publication » ; cf. tableau ci-dessus, ch. 6.12, 3e colonne) est imprécis et, d'autre part, l'applicabilité des dispositions en question aux fournisseurs d'hébergement et aux fournisseurs d'accès est entachée d'incertitudes.

Abstraction faite des différents essais d'interprétation, il est manifeste que l'art. 27 CP est taillé pour la coopération entre auteurs, rédacteurs et autres responsables de la publication et n'est guère approprié aux circonstances entourant le réseau mondial, les forums de discussion, les listes de diffusion (*mailing lists*), etc. Pour la plupart, les fournisseurs d'informations publient dans ces services Internet de manière autonome et selon des processus d'automatisation, *sans intervention intermédiaire d'une rédaction*, d'une autorité de contrôle, d'un imprimeur, etc. Il est donc difficile de comparer la position du fournisseur d'hébergement ou du fournisseur d'accès à celle des acteurs des médias de masse classiques tels que la presse écrite ou la radio.

Une nouvelle réglementation de la punissabilité des divers participants doit donc viser une *séparation explicite entre la fonction de médias et la fonction de télécommunication* de la Toile et des autres services de réseaux (cf. à ce propos ci-dessus chapitre 2).

6.3 Punissabilité selon les règles générales du Code pénal ?

Si l'on applique les règles générales de responsabilité aux auteurs et aux participants de délits qui ne constituent pas des délits de média (cf. tableau des délits, ci-dessus ch. 6.12, 3e colonne) ainsi qu'aux personnes qui y participent, toute une série de questions supplémentaires se posent quant aux fournisseurs d'accès et d'hébergement - questions dont les réponses demeurent entourées d'incertitude [128]. Une seule chose est claire : est responsable, en tant qu'auteur du délit, celui dont dépend directement l'existence du site et le contenu de celui-ci (fournisseur de contenu). Dès qu'il s'agit du fournisseur d'hébergement dont la fonction est de mettre de l'espace à la disposition d'autrui (contre rémunération) - espace que cette tierce personne peut utiliser à sa guise -, la controverse porte sur la manière dont ce fournisseur participe par l'intermédiaire d'un tiers au délit perpétré sur la Toile ; il en va de même du fournisseur d'accès. Cela pour *diverses raisons* :

Le fournisseur d'hébergement est qualifié soit *d'auteur* soit *seulement de complice* du délit en question selon la description de cet acte dans la norme pénale applicable. L'*auteur* est celui dont on doit dire qu'il a exécuté (en personne) l'acte, ce que le *complice* justement ne fait pas. Mais précisément dans le cas des éléments constitutifs examinés ici, la frontière entre ces deux rôles est très floue car ils excluent des modes d'action qui constituent un lointain *prélude à la violation du bien*

[128] En cas d'exclusion des diffuseurs techniquesdu champ d'application du droit pénal des médias, cela s'applique d'une manière tout à fait générale aux fournisseurs d'accès et d'hébergement (voir ci-dessus ch. 6.2).

juridiquement protégé. Ainsi, conformément à l'art. 197, ch. 1 CP, le seul fait de mettre des écrits pornographiques à la disposition de personnes de moins de 16 ans suffit (égal. art. 197, ch. 3 CP « pornographie dure », art. 135 CP « Représentations de la violence »), ce qui ferait du fournisseur d'hébergement l'auteur du délit. Néanmoins, lorsque le fournisseur d'hébergement passe avec l'utilisateur (fournisseur de contenu) le contrat lui remettant une certaine capacité de mémoire, il ne sait pas quel genre d'informations l'utilisateur veut et va mettre sur le réseau. C'est là une caractéristique de la position du fournisseur d'hébergement qui, en l'occurrence, donne *carte blanche* ; celle-ci porte sur les futures informations du fournisseur de contenu, non pas sur la pornographie, la discrimination raciale et autres sujets. Par exemple, le fournisseur d'hébergement ne permet pas l'accès à des prises de vue pornographiques (art. 197, ch. 1 CP), mais en premier lieu uniquement à un site - encore - vide. Ce site ne deviendra pornographique que par l'action de celui qui lui affectera un contenu. En conséquence, le fournisseur d'hébergement ne réunirait pas les éléments *objectifs* de l'infraction.

Par ailleurs, si l'on argumente à partir de *l'aspect subjectif de l'infraction*, le fournisseur d'hébergement peut n'avoir aucunement connaissance des informations que le fournisseur de contenu veut et va mettre sur le réseau. Certes, il sait d'expérience qu'on trouve aussi des contenus illégaux sur Internet ; mais savoir cela d'une manière générale ne peut fonder une intention quant aux délits dont la commission et, à plus forte raison, la constitution détaillée relèvent totalement de l'indéfini. On ne peut donc parler d'intention au moment où le fournisseur d'hébergement [129] commet l'acte en question ; ce qui éliminerait sa punissabilité pour comportement actif.

Ce n'est qu'*après* la conclusion du contrat que le fournisseur d'hébergement peut éventuellement avoir connaissance de la présence de contenus illicites sur son serveur. En règle générale, ce sont des *utilisateurs* de la Toile qui *attirent son attention* sur ce genre de contenus et peuvent même le mettre en demeure de bloquer ou de supprimer un site pour illicéité (au titre du droit pénal) des informations qui y figurent. Si le fournisseur d'hébergement se penche sur ce qui lui a été signalé, il peut réaliser qu'il y a infraction - par ex., selon l'art. 135 ou 197 CP. Mais il est douteux dans ce cas qu'il se rende punissable par comportement actif ou, le cas échéant, par négligence.

La jurisprudence *du Tribunal fédéral* ne permet pas de tirer des conclusions absolues ; les constatations figurant dans *l'arrêt* « *du 156 »* [130] ne peuvent pas être appliquées telles quelles au cas des fournisseurs d'hébergement [131]. Dans cet arrêt, le Tribunal fédéral avait considéré qu'il y avait eu « action » de la part de l'ancien directeur du département des télécommunications PTT en ce sens que celui-ci avait ordonné l'introduction du télékiosque 156 et que les prestations nécessaires à son exploitation avaient été fournies sur ses instructions. La mise à disposition de ces installations avait été considérée comme prestation active [132] et le directeur général

[129] Celui-ci existe au moment de la conclusion du contrat d'hébergement qui a en général lieu automatiquement lorsque le formulaire est rempli en ligne.

[130] ATE 121 IV 109 (l'arrêt dit du « 156 »).

[131] Pour plus de détails, cf. RIKLIN/STRATENWERTH, (Bibl.), p. 23 s.

[132] ATE 121 IV 109, 120 cons. 3b.

avait été condamné pour complicité de publications obscènes et de pornographie (art. 204 a CP et art. 197, ch. 1 CP).

La *différenciation entre action et omission,* fondamentale en droit pénal, n'est pas claire dans le cas couvrant le fait de « laisser, remettre », et surtout le fait de « rendre accessible ». Le Tribunal fédéral considère aussi comme action le fait de laisser se poursuivre les répercussions d'une action entreprise autrefois de manière licite lorsque cette action sert à appuyer une action de tiers intentionnellement illicite. Il est largement permis de douter de la pertinence de ce point de vue [133]. En effet, lorsque le fournisseur d'hébergement ignore simplement la remarque qui lui a été faite à propos d'un site punissable selon le droit pénal, il est difficile de reconnaître où il y aurait eu action en relation avec le site incriminé, même si la remarque est juste et si le fournisseur d'hébergement s'en est lui-même convaincu. Il convient de lui faire ici grief d'omission d'intervention. Ce comportement ne serait punissable que si le fournisseur était soumis à une obligation légale particulière d'agir (s'il avait l'obligation de se "porter garant" de la licéité du site dont il assure l'hébergemen) [134].

Selon la jurisprudence et la doctrine reconnues, une *position de garant* peut découler d'un agissement antérieur menaçant (responsabilité pour ingérence). Celui qui, de manière prévisible, produit, par ses actions, un danger pour les biens juridiques de tiers, est tenu de tout entreprendre pour que ce danger ne se concrétise pas. L'action du fournisseur d'hébergement consiste à fournir des capacités de mémoire aux personnes qui le demandent. Or il s'agit là d'un *acte légal* en soi et absolument quotidien, qui ne produit pas de danger particulier [135].

Le danger ou l'infraction résulte seulement de l'utilisation abusive de cette espace de mémoire par un tiers (le fournisseur de contenu) qui commet un délit de manière intentionnelle au moyen des informations mises sur le réseau [136].
On peut comparer cette situation à la question de savoir si un restaurateur est tenu d'empêcher ses clients, auxquels il a prêté des cartes à jouer, de s'adonner aux jeux de cartes interdits, ou si le propriétaire d'une maison doit veiller à ce que les personnes qui l'occupent n'y commentent pas de délits. Le Tribunal fédéral a

---

[133] En outre : dans le cas de l'arrêt « du 156 », *un seul* fournisseur de cette prestation était concerné (parce qu'il n'y en avait qu'un) ; dans le cas des fournisseurs d'hébergement, la question concerne quelque 100 entreprises.

[134] La doctrine estime qu'il y a omission ; cf. FRANZ RIKLIN: Information Highway und Strafrecht, in: Reto M. Hilty (Editeur): Information Highway. Beiträge zu rechtlichen und tatsächlichen Fragen, Berne/Munich 1996, p. 578; cette question a été débattue en détail dans le droit allemand avant l'entrée en vigueur de la TDG (Teledienstegesetz // loi sur les téléservices) ; cf. Ulrich SIEBER: Strafrechtliche Verantwortlichkeit für den Datenverkehr in internationalen Computernetzen, Teil 2, JZ 1996, p. 494 ss.

[135] Cette situation fait l'objet d'une controverse sous l'appellation de « complicité innocente » ; cf. entre autres GRACE SCHILD TRAPPE: Harmlose Gehilfenschaft, Berne 1995; WOLFGANG WOHLERS: Gehilfenschaft durch „neutrale" Handlungen, RPS 1999, p. 425 ss; MARC FORSTER: Der Wirtschaftsalltag als strafrechtsdogmatischer „Hort des Verbrechens", Festschrift Niklaus Schmid, Zurich 2001, p. 127 ss.

[136] Et, ce faisant, enfreint aussi le contrat conclu avec le fournisseur d'hébergement parce que le contrat interdit l'offre d'informations pénalement punissables.

répondu oui à la première question [137], et non à la seconde [138]. Ce point n'est donc également *pas clarifié* [139].
Les constatations faites à propos du fournisseur d'hébergement sont également applicables, par analogie, au *fournisseur d'accès*. La seule différence est que ce dernier se situe encore plus loin de l'auteur (principal) de l'acte. En effet, il n'entretient avec celui-ci aucun lien contractuel - automatisé -, mais est lié par contrat uniquement avec l'utilisateur final.

6.4 Le problème de la compétence juridictionnelle

L'une des questions les plus controversées dans le domaine du droit pénal d'Internet est celle de savoir à quel Etat revient le pouvoir de réprimer pénalement les cyberdélits internationaux [140]. Le droit de l'application des peines (art. 3 ss CP) définit de manière autonome et sans tenir compte des prétentions concurrentes d'autres Etats, le lieu où le droit pénal suisse est applicable et quelle est la personne soumise à l'autorité pénale suisse. Si la compétence jurdictionnelle de la Suisse est fondée, le tribunal doit appliquer le droit suisse [141].

Le *droit international public* pose, le cas échéant, des limites à ce pouvoir national de définition car lui aussi va très loin dans la reconnaissance de points de rattachement « judicieux » [142]. Il se peut donc, en droit pénal, qu'un même délit fasse l'objet de plusieurs poursuites et sanctions pénales. Ce risque concerne surtout les cyberdélits qui, du fait de la diffusion de contenus punissables sur la Toile, ont une portée qui ignore les frontières.

Le droit suisse de l'application des peines connaît un grand nombre de *règles de rattachement*. Hormis le *principe de la territorialité* [143] - celui qui est invoqué dans la plupart des cas - les délits transfrontaliers peuvent aussi être soumis au pouvoir pénal de la Suisse [144] en vertu du principe du pavillon [145], du principe de la protection

---

[137] ATF 81 IV 201.

[138] ATF 79 IV 147.

[139] En résumé du débat allemand, voir MARTIN POPP: Die strafrechtliche Verantwortung von Internet-Providern, Berlin 2002, p. 121 ss, qui admet une position de garant due à une souveraineté effective sur une chose dangereuse (positon de garant de surveillance) et approuve fondamentalement une punissabilité pour omission. Celle-ci est néanmoins limitée par la réglementation explicite du § 11 TDG.

[140] Pour une vue d'ensemble, voir SCHWARZENEGGER, GELTUNGSBEREICH (Bibl.), p. 109 ss.

[141] Exceptions : les art. 5, al. 1, 6, ch. 1, 6bis, ch. 1 CP obligent le juge suisse à appliquer le droit pénal étranger si celui-ci est plus clément.

[142] COUNCIL OF EUROPE, European Committee on Crime Problems: Extraterritorial criminal jurisdiction, Criminal Law Forum 1992, p. 441 ss. Voir égal. à ce sujet Cour Permanente de Justice Internationale [CPJI], Recueil des Arrêts, Sér. A, No 10, 1927 (« Affaire du Lotus »).

[143] Actes commis en Suisse, art. 3, ch. 1, al. 1 CP.

[144] Les art. 3 à 7 CP sont applicables dans les conditions prévues à l'art. 333, al. 1 CP (Réserve de réglementations divergentes) également pour ce qui est du droit pénal accessoire.

[145] Actes commis à bord d'un navire ou d'un aéronef soumis au droit suisse, art. 97 de la loi fédérale du 21 décembre 1948 sur l'aviation (LA, RS 748.0) ; art. 4, al. 2 à 3 de la loi fédérale du 23 septembre 1953 sur la navigation maritime sous pavillon suisse (RS 747.30).

de l'Etat [146], du principe de la personnalité active [147] et passive [148], ainsi que du principe de la compétence universelle [149].

Le rattachement selon le principe de la territorialité est concrétisé par le *principe* restreint *d'ubiquité* [150] : l'acte est réputé commis en Suisse lorsque soit le lieu où l'auteur a agi, soit le lieu où le résultat s'est produit se trouve en Suisse. En conséquence, les actes commis à l'étranger, mais menaçant ou violant des biens suisses juridiquement protégés peuvent être classés parmi les actes commis en Suisse [151].

6.41 Le lieu de commission des cyberdélits

Le lieu où *séjourne physiquement l'auteur* au moment où l'acte est perpétré est toujours l'élément déterminant quant au lieu de commission. Si le code pénal interdit, par exemple, de promouvoir, d'offrir, de montrer, d'exposer, de diffuser ou de rendre accessibles certaines informations [152], le lieu de commission est là où l'auteur a procédé à l'ordre de transmission ou de stockage grâce auquel le traitement de données est mis en marche par les processus automatisés du programme.

Si l'infraction doit être *« publique »,* il faut alors se fonder sur le lieu où se trouvait l'auteur au moment où est donné l'ordre permettant aux données d'être transférées, par les processus automatisés du programme, *dans le domaine public* du disque dur d'un ordinateur (serveur web, serveur Usenet) [153]. Le transport des données vers le serveur et leur stockage ne sont plus le fait de l'auteur, mais résultent d'un processus automatique. Par conséquent, le *lieu du serveur n'est pas le lieu de commission* [154].

---

[146] Actes dirigés contre l'existence et le crédit de la Suisse, art. 4, al. 1 CP, avec liste des délits.

[147] Actes commis par des ressortissants suisses, art. 6, ch. 1 CP.

[148] Actes dirigés contre des biens juridiquement protégés en droit pénal de ressortissants suisses, art. 5, al. 1 CP.

[149] Tout acte dirigé contre des biens universels juridiquement protégés , cf. art. 6bis CP, art. 19, ch. 4 de la loi fédérale du 3 octobre 1951 sur les stupéfiants (LStup, RS 812.121).

[150] Art. 7 CP.

[151] En fait, ce ne sont pas les biens juridiquement protégés qui sont menacés ou lésés, mais les objets de l'acte ou de l'atteinte dans lesquels ces biens sont concrétisés.

[152] Cf. art. 135 CP (Représentations de la violence), art. 173, ch. 1 et art. 174, ch. 1 CP (Délits contre l'honneur), art. 179, al. 2 CP (Violation de secrets privés), art. 197 ch. 1 à 3 CP (Pornographie), art. 259 CP (Provocation publique au crime ou à la violence), art. 261bis (Discrimination raciale) etc.

[153] A propos de la notion que recouvre l'adjectif « publique » - ou l'adverbe « publiquement » - dans le CP et spécialement à l'art. 261bis CP (Discrimination raciale), voir NIGGLI, RASSENDISKRIMINIERUNG, (Bibl.), n. 691 ss; GERHARD FIOLKA/ MARCEL ALEXANDER NIGGLI, Der Begriff der Öffentlichkeit im Strafrecht am Beispiel der Bundesgerichtsentscheide vom 21. Juni 2000 und vom 23. August 2000 betreffend Rassendiskriminierung, AJP 2001, 533 ss avec renvois.

[154] Cf. l'arrêt non publié de la Chambre d'accusation du Tribunal fédéral du 11 août 1999 (8G.43/1999), p. 5. Dans certains cas, en référence à la théorie dite « de la main à distance », l'emplacement du serveur-cible est aussi désigné comme lieu de commission de l'acte, cf. POPP (Bibl.), n. 6 avec renvois. A l'encontre de cette théorie, nous trouvons néanmoins l'intention manifeste du législateur suisse qui a sciemment limité le principe d'ubiquité de l'art. 7 CP au lieu où l'auteur agit (lieu de commission de l'infraction) et au lieu où le résultat s'est produit afin d'exclure les potentialités électroniques (« main à distance ») utilisées ou enclenchées par l'auteur ; cf. EMIL ZÜRCHER, Erläuterungen zum Vorentwurf vom April 1908, Berne 1914, p. 25 s. Cette interprétation permettrait le cas échéant de parvenir à des rattachements totalement fortuits au lieu du serveur-cible

Les cyberdélits se caractérisent notamment par le fait que le lieu de commission (celui où l'auteur agit) , qui fournit d'ordinaire le point de rattachement standard, demeure souvent inconnu aux autorités de poursuite pénale et est, dans certains cas, absolument impossible à déterminer.

6.42 Lieu de production du résultat dans le cas des cyberdélits

Souvent commis à l'étranger, les cyberdélits ont néanmoins des répercussions en Suisse. Se pose donc à cet endroit la question centrale de savoir ce que recouvre exactement la notion de « résultat » au sens de l'art. 7, al. 1 CP [155]. La controverse porte ici sur le fait de savoir si tous les délits présentent un résultat (faisant partie des éléments constitutifs de l'infraction) ou si tel n'est pas le cas pour certains types de délits comme les délits de mise en danger abstraite et les simples délits formels. *Deux essais d'interprétation* se dégagent de cette controverse :

6.421 Notion technique de résultat

Selon *la doctrine*[156] *et la jurisprudence dominantes* [157], la notion de résultat au sens de l'art. 7 CP est interprétée d'après la classification des différents genres de délits, à savoir les simples délits formels, ou délits matériels, et les délits de mise en danger concrète et abstraite. Cette classification est, pour sa part, fondée sur les différentes conditions qui doivent être remplies, selon la doctrine générale, pour que les différents éléments constitutifs soient réunis. Du fait que selon ce point de vue, la notion de « résultat » au sens de l'art. 7 CP correspond à un résultat « extérieur » (résultat au sens technique) défini dans les éléments constitutifs de l'infraction et dissociable dans le temps et l'espace du lieu de l'acte, on ne peut s'y rattacher dans le cas des simples délits formels et des délits de mise en danger abstraite (cf. tableau ci-dessus ch. 6.12, 2e colonne).

Ces délits s'accomplissent par la commission de l'action de sorte que, dans leur cas, il ne peut pas y avoir de lieu - distinct du lieu de l'action - où se produit le résultat. En conséquence, si une infraction commise par le biais d'Internet relève des simples délits formels ou des délits de mise en danger abstraite, elle ne peut ensuite être poursuivie en Suisse que si l'auteur a agi en Suisse. Par contre, si l'auteur a agi à

---

qui peut se situer dans un pays qui, sinon, n'a absolument rien à voir avec l'acte en question ; cf. SCHWARZENEGGER, E-COMMERCE (Bibl.), p. 339 s.

[155] Jusqu'à présent, le Tribunal fédéral n'a pas eu la possibilité de se prononcer sur la question du rattachement du résultat en cas de cyberdélits transfrontaliers ; cf. néanmoins à propos de l'Allemagne BGHSt 46, 212 (Volksverhetzung). A propos de l'opinion actuelle au niveau de la doctrine, voir SCHWARZENEGGER, GELTUNGSBEREICH (Bibl.), p. 120 s.; SCHWARZENEGGER, ABSTRAKTE GEFAHR (Bibl.), p. 240 ss; NIGGLI, NATIONALES STRAFRECHT (Bibl.), p. 144 ss; WEBER (Bibl.), p. 536 ss. Cf. à propos de la situation juridique en Allemagne : LEHLE (Bibl.); HILGENDORF (Bibl.), p. 650 ss; KOCH (Bibl.), p. 703 ss, tous avec d'autres renvois.

[156] Cf. en résumé TRECHSEL (Bibl.), art. 7, n. 6; REHBERG/DONATSCH (Bibl.), p. 42 tous avec renvois.

[157] Suivant les critiques réitérées de HANS SCHULTZ, le Tribunal fédéral a modifié sa jurisprudence sur la notion de résultat dans l'ATF 105 IV 326 ; cf. en résumé l'ATF 125 IV 180 ss. Néanmoins, dans l'ATF 128 IV 145, 153, il s'éloigne à nouveau de cette interprétation du résultat : « Le Tribunal fédéral a longtemps considéré … que la notion de résultat selon l'art. 7 CP s'interprétait de la même manière que pour la définition du délit matériel (…). Il s'est récemment distancé de cette solution et est revenu à une interprétation plus large de la notion de résultat. »

l'étranger, la Suisse n'a aucune compétence juridictionnelle qui soit fondée sur le principe de la territorialité [158].

D'une part, cette interprétation présente des avantages : elle fait obstacle à ce que la Suisse ait une compétence totale de juger les délits d'expression ressentis comme tels dans le monde entier et, partant, à ce que les autorités suisses de poursuite pénale soient par trop sollicitées par des procédures inutiles engagées contre des auteurs qui séjournent à l'étranger. *Par ailleurs*, la restriction du critère du rattachement au lieu du résultat au sens de l'art. 7 CP recèle en même temps l'inconvénient de cette interprétation : la *possibilité qu'elle donne de contourner le droit pénal suisse*.

Exemple : un groupe de skinheads suisses désire utiliser la Toile comme vecteur de propagande pour ses activités extrémistes. S'ils chargent en Suisse des textes négationnistes sur un serveur, ils sont soumis à la compétence juridictionnelle suisse. Mais si, à cette fin, les skinheads se rendent aux Pays-Bas ou en Suède et chargent à partir de l'un de ces pays les contenus sur le net, il n'est pas possible de les poursuivre en Suisse en raison de l'absence de compétence juridictionnelle [159]. Etant donné qu'en général, le législateur conçoit les éléments constitutifs indépendamment des conséquences possibles au niveau du droit de l'application des peines, les rattachements ne sont pas toujours évidents. L'art. 197, ch. 2 CP par exemple semble permettre un rattachement (Protection des adultes contre la confrontation avec la pornographie douce, délit de mise en danger concrète), mais pas l'art. 197, ch. 3 CP (pornographie dure, délit de mise en danger abstraite).

6.422 Le résultat en tant que lésion ou mise en danger d'un objet de l'atteinte

La *deuxième tentative d'interprétation* [160] part en revanche du principe que tous les faits constitutifs de l'infraction figurant dans les dispositions spéciales du Code pénal doivent reposer sur une lésion ou une mise en danger d'un objet de l'atteinte. Dans le cas des *délits de mise en danger abstraite*, le résultat consiste en la création d'un

---

[158] CASSANI (Bibl.), p. 246; NIGGLI, RASSENDISKRIMINIERUNG (Bibl.), n. 63 s.; WIDMER/BÄHLER (Bibl.), p. 310 s.; à propos de l'Allemagne : HILGENDORF (Bibl.), p. 650 ss; KOCH (Bibl.), p. 703 ss avec d'autres renvois.

[159] Le « mensonge d'Auschwitz » (art. 261bis al. 4 CP, pur délit formel) n'est pas pénalement répréhensible notamment aux Etats-Unis, au Danemark, aux Pays-Bas, en Suède et en Grande-Bretagne, cf. KOCH (Bibl.), p. 704 avec renvois. Le principe actif de la personnalité (art. 6 ch. 1 CP) ne permet pas non plus de rattachement car il manque la condition de la double punissabilité. Des considérations identiques peuvent être déterminantes dans le cas des fournisseurs d'hébergement et des fournisseurs d'accès agissant au niveau international quant au choix du lieu ; cf. HEINE (Bibl.), p. 106.

[160] FRANZ RIKLIN, Information Highway und Strafrecht, in : R. M. Hilty (Editeur), Information Highway, Berne/Munich 1996, 581 s.; SCHWARZENEGGER, GELTUNGSBEREICH (Bibl.), p. 123 ss; SCHWARZENEGGER, ABSTRAKTE GEFAHR (Bibl.), p. 249 ss; LAURENT MOREILLON, Nouveaux délits informatiques sur Internet, Medialex 2001, p. 25 s.; WEBER (Bibl.), p. 538 (restriction : la personne lésée est considérablement touchée); cf. égal. HEINE (Bibl.), p. 109 (« évident quant aux infractions relevant de la UWG », point en général laissé en suspens). Est également implicite l'Arrêt du Tribunal correctionnel du District de Lausanne, 7 juillet 1997, Medialex 1997, p. 235 (Pornographie dure); à propos de l'Allemagne : BGHSt 46, p. 212; DIRK-M. BARTON, Mulitmedia-Strafrecht, Neuwied/Kriftel 1999, p. 146 ss; BERND HEINRICH, Der Erfolgsort beim abstrakten Gefährdungsdelikt, GA 1999, p. 79 ss; LEHLE (Bibl.), p. 57 ss avec d'autres renvois.

danger très important pour des objets de l'atteinte encore non concrétisés (par exemple n'importe quel enfant en Suisse pourrait être confronté à la pornographie douce mise à disposition sur un serveur à l'étranger, art. 197, ch. 1 CP), et il est possible de déterminer le lieu où s'étend ce danger abstrait. En outre, il convient de relever que dans ce genre de délits, le lieu de l'acte d'exécution et le lieu de production du résultat ainsi défini ne concordent pas absolument dans tous les cas. Pour ce qui est des cyberdélits, il convient, par conséquent, d'admettre un rattachement au lieu du résultat au sens de l'art. 7, al. 1 CP si le danger important d'y être confronté est réalisé par la possibilité d'appeler les contenus illicites en Suisse.

Le point fort de cette interprétation est de placer au premier plan les préoccupations de la *protection des biens juridiques* et de se fonder sur les faits constitutifs de l'infraction. En outre, elle donne un point de rattachement pour les actes de participation qui, conformément à la pratique du Tribunal fédéral, doivent être jugés selon le droit qui s'applique à l'acte principal (cf. ci-dessous ch. 6.43). Par contre, l'étendue de la compétence et une éventuelle collision avec d'autres compétences juridictionnelles semble constituer un désavantage.

Si l'on veut prévenir la double pénalisation et éviter d'accabler les autorités de poursuite pénale de procédures longues et vaines, un certain nombre de *mesures de limitation* s'imposent : coopération internationale (délégation de la poursuite pénale à d'autres Etats ; cf. art. 88 EIMP, RS 351.1), demandes d'extradition, réduction du nombre des procédures par l'application du *principe de l'opportunité* aux actes exécutés à l'étranger et à propos desquels seul le résultat se produit en Suisse, restriction aux cas auxquels s'applique le critère international du point de rattachement « judicieux » en Suisse [161].

6.43 Le rattachement des actes de participation

Selon la jurisprudence du Tribunal fédéral, en cas de participations exécutées en Suisse (Instigation, art. 24 CP; Complicité, art. 25 CP) à un cyberdélit entièrement réalisé à l'étranger, selon la jurisprudence du Tribunal fédéral, le lieu de commission suisse de la participation ne s'applique pas comme point de rattachement au sens de l'art. 7 CP [162] en raison du caractère accessoire de celle-ci par rapport à l'acte principal. Du fait de cette *accessoirité*, une multitude de cas Internet échappe à la compétence juridictionnelle de la Suisse. Si l'on considère les règles relatives au champ d'application géographique comme condition matérielle de la punissabilité, la responsabilité pénale devient également caduque [163]. Il n'est donc pas possible de poursuivre pénalement pour complicité un fournisseur d'accès ou d'hébergement

[161] Une solution flexible figure par exemple à l'art. 4, al. 1, ch. 4 du code de procédure pénale bernois (CPP). De même à l'art. 8, al. 2, let. d de l'avant-projet de code de procédure pénale fédéral, Berne 2001 : dans la mesure où des intérêts non essentiels de la partie plaignante ne s'y opposent pas, le ministère public et les tribunaux renoncent à la poursuite pénale lorsque … « l'infraction est déjà poursuivie par une autorité étrangère ou lorsque la poursuite a été cédée à une telle autorité ». Cf. les commentaires explicatifs figurant à ce propos dans l'avant-projet d'un code de procédure pénale suisse, Berne 2001, p. 36.

[162] ATF 81 IV 37; 104 IV 86; 108 Ib 303; J.-L. COLOMBINI, La prise en considération du droit étranger (pénal et extra-pénal) dans le jugement pénal, thèse Lausanne 1983, p. 35; POPP (Bibl.), n. 14.

[163] POPP (Bibl.) avant l'art. 3, n. 4; à propos de la condition de recevabilité, voir SCHWARZENEGGER, GELTUNGSBEREICH (Bibl.), p. 127.

suisse [164]. Il en va de même de la poursuite pénale contre des poseurs de liens dans le cas d'un renvoi hyperlink sur un site à l'étranger.

Le Tribunal fédéral appuie sa pratique sur la théorie de la participation au fait illicite (Unrechtsteilnahme-Theorie) selon laquelle la punissabilité du participant dépend, en règle générale, de celle de l'auteur principal. Son appréciation est soumise au droit étranger et incombe uniquement au tribunal du lieu où l'acte a été exécuté. Cette position est toutefois partiellement mise en doute parce que le droit de l'application des peines n'a pas pour objet le caractère accessoire de la punissabilité, mais la question de la localisation d'une infraction [165]. Exception faite du cas spécial de la tentative d'instigation à commettre un crime (art. 24, al. 2 CP), l'instigation et la complicité ne sont punissables que si elles ont pour ainsi dire donné un résultat, c'est-à-dire si l'acte principal a au moins fait l'objet d'une tentative de réalisation.

En conséquence, à propos de la complicité, il convient de faire la distinction, par exemple, entre un acte d'exécution - une contribution quelconque favorisant l'acte principal - et le résultat - réalisation ou tentative de réaliser l'acte principal. Si l'auteur exécute l'acte de complicité en Suisse, cela devrait suffire à fonder la compétence juridictionnelle de la Suisse tout comme dans un cas d'escroquerie où seul l'astuce est réalisée en Suisse [166]. Afin d'éviter les résultats choquants, il est proposé, à titre de mesure limitative, de requérir dans ces cas comme condition supplémentaire la punissabilité de l'acte principal au lieu où il a été commis [167].

6.44 Cas d'espèce (cf. annexe)

Un cyberdélit peut-il en Suisse faire l'objet d'une action en justicel ? Il est encore *difficile de répondre de manière claire* à cette question - ainsi qu'il ressort d'ailleurs des considérations précédentes. Les trois cas exposés en *annexe* ont pour but d'illustrer en quelques mots la complexité de l'imbrication entre le droit de l'application des peines et le droit pénal matériel, ainsi que celle des règles spéciales du droit pénal des médias. Bon nombre de questions ne trouveront pas de réponses claires.

Le *premier cas* est celui de la préparation d'un fichier image de pornographie enfantine sur un site (art. 197, ch. 3 CP), le *deuxième* cas celui d'une provocation à l'incendie dans un forum de discussion (art. 259, al. 1 CP) et le *troisième* celui d'un site web de textes rabaissant systématiquement les membres d'une ethnie

---

[164] A moins que l'action principale ne soit soumise à la compétence juridictionnelle de la Suisse en vertu des art. 3 (résultat), 4, 5, 6 ou 6bis CP. Dans ce cas, celle-ci est également fondée pour la participation.

[165] SCHWARZENEGGER, E-COMMERCE (Bibl.), p. 346; cf. HANS SCHULTZ, Gesetzgebung und Rechtsprechung der Schweiz im internationalen Strafrecht 1970 bis 1972, ASDI vol. XXIX, p. 416 s.; TRECHSEL (Bibl.), art. 7, n. 8; POPP (Bibl.), art. 7, n. 14 avec renvois. La pratique cantonale diverge aussi en partie de celle du Tribunal fédéral : voir HANS SCHULTZ, Gesetzgebung und Rechtsprechung der Schweiz im internationalen Strafrecht 1942 bis 1963, ASDI vol. XX, p.192 s.

[166] Il s'agit de cas d'escroquerie dont le résultat, c'est-à-dire l'erreur, la disposition de biens et le préjudice pécuniaire sont produits totalement à l'étranger ; cf. à ce propos CHRISTIAN SCHWARZENEGGER: Handlungs- und Erfolgsort beim grenzüberschreitenden Betrug, Festschrift Niklaus Schmid, Zurich 2001, p. 158 s. avec renvois.

[167] Principe de la norme identique, TRECHSEL (Bibl.), art. 7, n. 8 avec renvois.

particulière (art. 261bis, al. 2 CP). La Toile et les forums de discussion (*news groups*) sont ici synonymes de services Internet qui s'adressent au public.

La présentation détaillée de ces trois cas dans différentes variantes figure en annexe.

6.5 Juridiction fédérale ou juridiction cantonale ?

Les difficultés entourant la détermination de la compétence juridictionnelle (cf. ci-dessus ch. 6.4) ont pour conséquence directe la question de la poursuite pénale. En principe, dans le cas d'un cyberdélit, on ignore à l'ouverture de l'enquête où l'acte a été exécuté. Il s'ensuit que pour la plupart, les procédures pénales en cas de délits commis via Internet peuvent être engagées par des autorités non compétentes et qu'elles ne peuvent être transférées aux autorités compétentes qu'au cours de l'enquête [168].

Un rattachement au résultat serait la seule alternative possible. Mais si, à l'instar de la doctrine et de la jurisprudence dominantes [169], on entend par résultat l'élément constitutif de l'infraction, les délits qui n'aboutissent pas à un résultat dans ce sens (donc par ex. la plupart des délits dits d'expression, cf. tableau ch. 6.12, 2^{e} colonne) ne peuvent être rattachés géographiquement qu'au lieu de commission de l'infraction.

Une définition large du « résultat » au sens de l'art. 7 CP permet certes de fonder une compétence suisse pour la poursuite pénale selon l'art. 7 CP parce que le résultat devient par là fondamentalement « *ubiquitaire* », c'est-à-dire qu'il se produit partout où l'information incriminée est perçue. Mais ce qui est peut-être souhaitable au plan international mène, transposé à l'échelle nationale, à une prolifération de compétences : chaque autorité de poursuite pénale qui s'estime compétente ou qui devient compétente à la suite d'une plainte est également compétente [170].

Conformément à l'art. 346, al. 1 CP, l'autorité compétente pour la poursuite est celle du lieu où l'auteur a agi (lieu de commission) ou - dans la mesure où seul le résultat a été produit en Suisse - l'autorité du lieu du résultat. La seconde situation devrait constituer la variante normale pour les délits commis sur Internet, du moins provisoirement. Ce qui pose, *en premier lieu,* la question de savoir comment procéder en cas de délits qui ne présentent aucun résultat au sens d'élément constitutif de l'infraction. *En second lieu*, il en résulte que même si l'on opte pour une large définition du résultat au sens de l'art. 7 CP, la compétence de la poursuite revient certes à la Suisse, mais au plan intérieur, la poursuite dépend de contingences. En vertu de l'art. 346, al. 2 CP, si le résultat se produit en plusieurs endroits - donc en principe toujours dans le cadre d'une large conception du résultat pour les délits d'expression - l'autorité compétente est celle du lieu où l'enquête a été entamée en premier lieu. Cela signifie qu'en principe - du moins en cas de délit contre l'honneur, de représentations de la violence, de pornographie, de discrimination raciale, mais aussi de fourniture d'indications en vue de la fabrication

---

[168] NIGGLI, NATIONALES STRAFRECHT (Bibl.), p. 169 s.
[169] Autre avis récent in ATF 128 IV 145, 153.
[170] NIGGLI, INTERNET-KRIMINALITÄT, (Bibl.), p. 6 s.

de virus informatiques(art. 144bis, ch. 2 CP) - chaque autorité suisse de poursuite pénale est compétente dès qu'une première plainte a été déposée [171].

L'attribution d'une compétence générale sur tous les cyberdélits à toutes les autorités suisses de poursuite pénale a pour conséquence d'innombrables *doublons.* Dans d'autres cas, une *coordination* est absolument nécessaire, comme l'a montré récemment le fameux « cas Landslide » [172].

Seule l'attribution de *la compétence à la Confédération* permettrait de remédier à cette situation. C'est exactement l'objectif que poursuivait l'initiative parlementaire Aeppli Wartmann déposée le 26 septembre 2002 (Pa. Iv. 02.452, cf. ci-dessus ch. 1.22). Cette initiative demande la création d'une compétence fédérale au sens de l'art. 340bis CP (Crime organisé, Criminalité économique), c'est-à-dire une compétence de la Confédération dans tous les cas ou l'acte a été commis pour une part essentielle à l'étranger ou dans plusieurs cantons, à savoir le cas type des cyberdélits, du moins pour ce qui est des délits d'expression.

[171] NIGGLI, INTERNET-KRIMINALITÄT (Bibl.), p. 6 s.

[172] Des utilisateurs pouvaient consulter et télécharger des sites de pornographie enfantine sur un site commercial situé aux Etats-Unis et payer par carte de crédit. Après l'arrestation des exploitants du site, le FBI poursuivit l'exploitation du portail et transmit à l'Office fédéral de la police via INTERPOL les données concernant les cartes de crédit des clients suisses de Landslide. A l'automne 2002, une opération coordonnée des autorités de poursuite pénale cantonale (l'opération Genesis) fut lancée bien que des informations aient déjà filtré dans certains cantons alors que d'autres cantons n'avaient pas encore terminé les perquisitions et les saisies d'ordinateurs auprès des suspects se trouvant dans leur secteur de compétence.

L'introduction d'instruments de droit administratif admis et requis ne nécessite ni une révision du droit des télécommunications, ni une nouvelle loi, mais une révision du code pénal telle qu'elle proposée. Cette solution permet par ailleurs d'éviter les mesures d'accompagnement de droit administratif.

7. Une possibilité : les mesures de droit administratif

7.1. Situation initiale

7.11 Besoins

La commission d'expert s'est penchée sur les besoins en la matière : la lutte contre les atteintes aux biens juridiques protégés dans les réseaux de communication nécessite-t-elle des mesures et des réglementations de droit pénal *et de droit administratif* ? Ces dernières permettraient, le cas échéant, de prévenir les atteintes aux biens juridiques protégés et, par ailleurs, d'agir là où le droit pénal (suisse) ne peut être appliqué.

Cette contribution du droit administratif doit, bien entendu, être l'expression des garanties qui découlent des droits fondamentaux de la libre communication [173]. En outre, ces mesures de soutien ne devront revêtir qu'une fonction *d'accompagnement*, *de complément* au droit pénal.

7.12 Compétence de la Confédération

Les télécommunications (notamment les réseaux de télécommunication) et les médias électroniques sont régis par l'art. 92 (Services postaux et télécommunications) et l'art. 93 Cst. (Radio et télévision) : conformément à ces deux dispositions constitutionnelles, il appartient à la Confédération de réglementer *toutes* les questions se posant en la matière. Ces compétences fédérales sont par ailleurs de nature *exclusive* ; elles interdisent les réglementations cantonales même si une norme de droit fédéral est lacunaire [174].

---

[173] Cf. ci-dessus chapitre 5.

[174] Cf. par ex. ROLF H. WEBER, § 60 Energie und Kommunikation, in : Thürer/Aubert/Müller (Editeurs), Verfassungsrecht der Schweiz/Droit constitutionnel suisse, Zurich 2001, p. 943 ss, ch. marg. 27; voir en outre ANDREAS KLEY, Bundeskompetenzen mit ursprünglich derogatorischer Wirkung aus historischer Perspektive, in : recht 1999, p. 189 ss, p. 200.

7.13 Le droit actuel

7.131 Droit des télécommunications

En sa qualité de droit de l'infrastructure, le droit des télécommunications règle en premier lieu le transport d'informations transmises au moyen de techniques de télécommunication (cf. art. 2 en rel. avec l'art. 3, let. b et c LTC). Internet est à cet égard essentiellement pris en compte comme plate-forme de communication individuelle (courrier électronique, voix ou IP, transmission de données) ou de diffusion, au moyen de techniques de télécommunication, d'informations qui ne sont pas considérées comme émissions de radio ou de télévision.

Seul un petit nombre de dispositions se réfèrent au *contenu* des informations transmises [175]. Elles ne peuvent néanmoins pas servir de base aux mesures de droit administratif dont il est question ici.

7.132 Droit de la radiodiffusion

La LRTV est ciblée sur les émissions de radio et de télévision traditionnelles et n'est pas appropriée aux mesures requises dans le présent contexte. La nouvelle loi - en préparation - sur la radio et la télévision a, elle aussi, uniquement pour but de réglementer l'organisation, la diffusion et la réception de programmes à proprement parler [176]. Un programme est une série d'émissions offertes en permanence, dont le déroulement est fixé dans le temps, qui est transmise par des techniques de communication et destinée au public en général.

Internet par exemple ne joue qu'un rôle d'infrastructure de diffusion. Les programmes de radio et de télévision diffusés par le biais d'Internet sont soumis à la LRTV. Par contre, à l'avenir aussi, le droit de la radiodiffusion ne réglera pas d'autres services Internet.

7.133 Conclusion

Le droit en vigueur n'offre donc *pas de prescriptions* sur lesquelles on pourrait fonder les mesures de droit administratif en vue de lutter contre les atteintes portées aux biens juridiques protégés dans les réseaux de communication. En général, du point de vue du droit administratif, l'activité des fournisseurs est régie par la LTC uniquement pour ce qui est de la transmission d'informations.

---

[175] Cf. par ex. art. 43 ss LTC (Obligation d'observer le secret), art. 48 LTC (Restriction des communications pour des raisons importantes), art. 49 LTC (Falsification ou suppression d'informations), art. 31 OST (Obligation faite aux fournisseurs de prestations relevant du service universel d'offrir la possibilité de bloquer gratuitement les communications sortantes vers des services à caractère érotique ou pornographique).

[176] DETEC, Rapport explicatif relatif au projet de nouvelle loi sur la radio et la télévision (LRTV), Procédure de consultation de décembre 2000, p. 18 s. – Le message relatif à la révision totale de la loi sur la radio et la télévision a été adopté par le Conseil fédéral le 18 décembre 2002; cf. FF 2003, 1425 ss.

7.2. Les instruments de droit administratif possibles

7.21 Réglementations et décisions de police

Il s'agit en premier lieu de créer une base légale pour les décisions de police protégeant des *biens juridiques spécifiques*. L'admissibilité d'un règlement de cet ordre dépend du genre de *mesures* qui y sont prévues.

7.211 Autorisation obligatoire

Imposer une autorisation obligatoire pour *ouvrir un site web* est incompatible avec l'interdiction de la *censure* (art. 17, al. 2 Cst.) [177].

De même, soumettre à autorisation *l'offre de capacité de mémoire* pour des informations de tiers destinées au public en général équivaut à une censure préalable illicite ; d'autant plus si l'octroi de l'autorisation est assorti de l'installation de certains dispositifs de sécurité (p. ex. les filtres).

7.212 Obligation de contrôler les contenus

On pourrait par ailleurs envisager de créer une norme spéciale obligeant les fournisseurs à procéder à des *contrôles des contenus*, norme dont le respect serait assuré par des *mesures de surveillance*. Cette mesure pourrait, selon les cas, être liée à l'installation obligatoire d'un *système de contrôle automatisé* qui filtrerait certaines informations ou les exclurait de l'accès public.

Cependant, ce genre de réglementation reviendrait à transférer aux fournisseurs la souveraineté de l'Etat en matière d'application du droit, leur permettant ainsi de déterminer eux-mêmes quels contenus ils doivent filtrer comme étant illégaux - possibilité qui est dénuée de toute base constitutionnelle[178]. Les fournisseurs pourraient par ailleurs en abuser pour éliminer délibérément leurs concurrents et pratiquer la concurrence déloyale [179].

En outre, dans la plupart des cas, une obligation légale générale de contrôle des contenus se révèlerait probablement inappropriée et de ce fait disproportionnée. En effet, il est relativement facile de contourner filtres et programmes de protection par de simples opérations techniques. En outre, les pays étrangers (voisins) ne

---

[177] Cf. dans le même sens la « Déclaration sur la liberté de la communication sur l'Internet » du comité des ministres du Conseil de l'Europe du 28 mai 2003 : http://www.coe.int/T/F/Droits_de_l%27Homme/media/5_Ressources_documentaires/1_Textes_de_base/2_%20Textes_du_Comite_des_Ministres/PDF_D%E9claration%20libert%E9%20de%20communication%20sur%20Internet%20%20(f).pdf

[178] Cf. avec le même résultat la « Déclaration sur la liberté de la communication sur l'Internet » (loc. cit.).

[179] Cf. SEMKEN, (Bibl.), p. 270 s., qui donne un exemple clair de l'installation d'un « filtre de protection de l'enfance » par un fournisseur qui fonctionne en même temps comme fournisseur de contenu dans le but d'évincer certains produits concurrents.

disposant pas de prescriptions dans ce sens, ce genre de réglementation est appelé à n'avoir pratiquement aucun effet du moins auprès des fournisseurs d'accès [180].

7.213 Obligation d'annoncer et de déclarer

Si l'on associe une obligation d'annoncer et de déclarer - imposée au prestataire - et le contrôle obligatoire (et préalable) du contenu, l'obligation en question n'est pas admissible pour les raisons citées plus haut. Par contre, il n'apparaît pas d'emblée irrecevable d'obliger les prestataires qui ont connaissance d'une atteinte probable à des biens juridiques protégés, sur la base d'indications qui leur ont été directement adressées, d'annoncer ou de déclarer le fait aux autorités [181]. En effet, dans ce cas, il n'y a ni cession de la souveraineté de l'Etat en matière d'application du droit, ni obligation pour le prestataire de procéder à un contrôle du contenu. Néanmoins, le cercle des prestataires tenus d'annoncer les cas suspects doit être défini selon des critères objectifs, dans le respect du principe de l'égalité du droit.

La commission d'experts estime judicieux d'intégrer cette obligation limitée d'annoncer dans la proposition de nouvel article 322bis, ch. 1, al. 2 CP et de garantir le respect de cette obligation [182].

7.214 Monitoring

Les avis divergent [183] quant à savoir si le « *monitoring* » [184] doit aussi être considéré comme censure préalable ou comme censure a posteriori justifiable (art. 36 Cst.). Si une mesure de ce genre est mise en place, il faudrait veiller à ce que le contrôle ne soit pas le fait d'automatismes techniques ; en effet, seul l'être humain peut constater la présence d'une atteinte à un bien juridique protégé. En outre, le blocage ou la suppression d'un site résultant d'une censure a posteriori devrait être conçu comme une décision (susceptible de recours).

---

[180] Conformément à l'art. 15, ch. 1 de la directive européenne sur le commerce électronique (cf. ci-dessus chapitre 4), selon lequel il est interdit aux Etats membres d'imposer aux prestataires, fournisseurs, d'accès, de « *caching* » et d'hébergement, 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.

[181] Cf. égal. l'art. 15, ch. 2 de la directive européenne sur le commerce électronique selon lequel les Etats membres peuvent obliger les prestataires de services de la société de l'information à informer promptement les autorités compétentes d'activités illicites alléguées qu'exerceraient les utilisateurs ou d'informations illicites alléguées que ces derniers fourniraient.

[182] Cf. à ce propos ci-dessous chapitre 9 - L'obligation d'annoncer est judicieusement limitée aux fournisseurs qui mettent à disposition des informations d'autrui de manière automatisée sur un réseau de communications électroniques (les fournisseurs d'hébergement).

[183] Cf. sur l'ensemble de la question avec force détails MARKUS SCHEFER, Die Kerngehalte von Grundrechten, thèse d'habilitation, Berne 2001, p. 462 ss. – Depuis janvier 2003, le « Service de coordination de la lutte contre la criminalité sur Internet » (SCOCI) recherche les infractions commises sur Internet. De l'avis de la commission d'experts, il s'agit d'une sorte de « patrouille sur Internet » que l'on peut certes qualifier absolument de « monitoring », qui se justifie néanmoins tout à fait et, par-là, est compatible avec la constitution.

[184] On entend ici par « monitoring » le contrôle systématique, effectué par des services étatiques, des informations diffusés sur les réseaux de communications dans le but de détecter les violations potentielles du droit.

7.215 Décision de blocage et de suppression

La création d'une réglementation légale qui, sur la base du « principe du perturbateur », qualifie tant le fournisseur de contenu que le fournisseur d'hébergement de destinataires potentiels d'une décision de suppression est *conforme au droit*. Si le fournisseur n'est pas d'accord avec l'injonction concrète des autorités, il peut demander que le cas soit examiné par un tribunal. De l'avis de la commission d'experts, il est cependant judicieux d'intégrer la base légale de ce genre de décision dans le nouvel art. 322bis , ch. 1, al. 5 CP tel qu'il est proposé [185].

Par contre, pour ce qui est des fournisseurs d'accès, une obligation générale abstraite de restreindre l'accès à certaines données apparaît inefficace, donc *disproportionnée*. En effet, il est relativement facile de contourner techniquement ce genre de restriction de l'accès [186].

7.22 Elargissement du régime de la concession et des conditions d'octroi des concessions ?

7.221 Bases

Selon le droit actuel des télécommunications, le régime de la concession est rattaché à l'exploitation indépendante d'installations de télécommunications. A cet égard, le contenu ne constitue pas un critère. Etant donné que la plupart des prestataires suisses n'exploitent pas de manière indépendante des installations de télécommunication utilisées pour la transmission, ils ne sont en principe pas soumis au régime de la concession, mais tout au plus à l'obligation d'annoncer (art. 4, al. 2 LTC).

Dans l'optique de la lutte contre la cybercriminalité, on pourrait théoriquement élargir la portée personnelle du régime de la concession et, parallèlement, étendre au contenu les conditions d'octroi de la concession aux fournisseurs de services de télécommunication. Les *fournisseurs d'accès* seraient ainsi tenus de contrôler le contenu des flux de données qui passent par leurs installations d'infrastructure. Toutefois, une telle réglementation non seulement va à l'encontre de la tendance actuelle, mais encore n'est *pas admissible:*

7.222 Inadéquation au regard de la tendance actuelle

L'élargissement du régime des concessions va clairement à l'encontre de la tendance actuelle. Dans le domaine de la LRTV, l'obligation d'annoncer doit s'imposer. Une obligation de concession ne doit demeurer que lorsqu'il faut attribuer des biens disponibles de manière limitée (par ex. les fréquences) ou des fonds publics (quote-part provenant des redevances de réception).

---

[185] Cf. à ce propos le chapitre 9 ci-dessous.
[186] Cf. néanmoins la disposition, qui va plus loin encore, de l'art. art. 12, ch. 3 de la directive européenne sur le commerce électronique ; cf. ci-dessus chapitre 4.

La *révision partielle de la loi sur les télécommunications* mise en consultation en juin 2002 prévoit, elle aussi, d'abandonner l'actuel système global de concession pour les services de télécommunication, tout en améliorant la surveillance de l'Etat [187].

7.223 Caractère inadmissible

Si elle se traduit dans les faits par une *censure (préalable)* (art. 17, al. 2 Cst.), la délégation du contrôle étatique des contenus à des concessionnaires est inadmissible car elle touche à l'essence même de la liberté de pensée et de la liberté des médias.

Cela dit, la délégation du contrôle à des concessionnaires qui reviendrait à une *censure a posteriori*, est aussi inadmissible. En effet, une réglementation de ce genre retire la souveraineté en matière d'application du droit de la sphère de l'Etat pour la confronter à l'arbitraire et à l'abus.

L'élargissement aux contenus des conditions requises par les concessions obligerait les fournisseurs d'accès à installer et à exploiter un système de sécurité et de contrôle, ce qui semble néanmoins disproportionné et de ce fait inadmissible (cf. ci-dessus ch. 7.212).

7.23 Gentlemen's agreement

Les *arrangements informels* (« gentlemen's agreements ») offrent une solution de rechange au droit classique de la police pour la protection des bien juridiques menacés. Ces arrangements ont pour objectif d'influer sur le comportement sans établir des relations ayant force obligatoire [188]. Ils sont surtout répandus dans le domaine du droit de l'environnement et du droit administratif économique.

Le principe de la légalité ne s'oppose pas à ce genre d'accord tacite sauf lorsque par sa portée et son but, une norme l'interdit explicitement ou implicitement - par exemple par renvoi aux formes d'exercice de la décision ou du contrat [189].

Néanmoins, ce genre d'arrangements informels semble peu adaptés au présent contexte. Certes, ils permettent de déterminer d'un commun accord les mesures de sécurité et de contrôle techniquement possibles et raisonnablement exigibles de la part des prestataires. Mais en même temps, il faudrait garantir que les autorités étatiques continuent à déterminer les contenus illégaux et de ce fait conservent la souveraineté en matière d'application du droit. Par ailleurs, les arrangements informels révèlent leurs limites lorsqu'ils portent atteinte aux droits fondamentaux de tiers - telles la liberté de l'information du public ou la liberté économique d'autres prestataires. La doctrine requiert dans ces cas que les tiers concernés soient entendus au préalable; à défaut, il appartient à l'autorité compétente de prendre une

---

[187] Cf. sur l'ensemble de la question <http://www.bakom.ch/de/telekommunikation/grundlagen/konsult/fmg/ index.html>.
[188] HÖSLI (Bibl.), p. 39 s.; PFENNINGER (Bibl.), p. 228; HÄFELIN/MÜLLER (Bibl.), n. 734 ss, 737; TSCHANNEN/ZIMMERLI /KIENER (Bibl.), p. 265.
[189] Cf. HÖSLI (Bibl.), p. 168 ss; PFENNINGER (Bibl.), p. 81 ss, 102 ss.

décision sur le fond [190]. Au demeurant, les limites des arrangements informels, dont la portée n'a été que peu clarifiée jusqu'ici, semblent être encore plus sensibles dans le présent contexte que dans d'autres domaines du droit [191].

7.3 Conclusion : pas de mesures d'accompagnement de droit administratif

Les gardes-fous posés par la constitution (interdiction de la censure préalable, principe de la proportionnalité) restreignent grandement l'ampleur des réglementations administratives admissibles. Selon la commission d'experts, l'introduction des instruments relevant (en soi) du droit administratif, qui sont admissibles au regard de la constitution et qui, en outre, sont indiqués, ne nécessite pas une révision du droit des télécommunications en vigueur, et encore moins la création d'une nouvelle loi. Ces mesures sont en revanche aisément intégrables dans la révision du code pénal ici proposée et, en outre, peuvent si nécessaire être associés à la procédure législative en cours.

- La proposition de nouvel *art. 322bis, ch. 1, al. 2 CP* rend superflue une *obligation d'annoncer* de droit administratif. En effet, cette disposition contient une obligation d'annoncer certes restreinte, mais suffisante pour les fournisseurs d'hébergement (cf. ci-dessous chapitre 9).
- Au lieu d'établir des dispositions de droit administratif particulières pour les *décisions de blocage et de suppression* à l'encontre des prestataires d'hébergement et de contenu, la disposition proposée par la commission d'experts pour l'art. 322bis, ch. 1, al. 5 CP permet de parvenir à l'élimination des contenus illégaux, que la Suisse ait ou non une cométence jurdictionnellle (cf. ci-après chapitre 9). Les mêmes motifs que ceux qui ont déjà été exposés à propos des mesures administratives de blocage s'opposent aux décisions de suppression et de blocage dirigées contre les fournisseurs d'accès, qu'ils soient fondés sur une interprétation extensive de l'art. 58 CP ou sur des normes de procédure pénale (voir ci-dessus 7.215).
- A la place d'un « *monitoring* », non sans inconvénients du point de vue constitutionnel, on pourrait créer une base légale pour les *investigations secrètes*. Ce genre de procédure serait probablement porteuse d'une plus grande efficacité dans la lutte contre les contenus illégaux mis en ligne sur les réseaux de communication. La commission d'experts a néanmoins décidé de ne pas proposer une telle base légale dans le présent contexte et de se contenter de relever que la loi fédérale sur l'investigation secrète (LFIS) est actuellement examinée par les Chambres fédérales.

[190] TSCHANNEN/ ZIMMERLI/KIENER (Bibl.), p. 267.
[191] HÄFELIN/MÜLLER (Bibl.), ch. marg. 736.

La responsabilité civile en rapport avec les violations du droit sur Internet est régie par le droit des obligations et par des règles juridiques spéciales relatives à la responsabilité. Il n'existe actuellement aucune disposition spécifique applicable aux prestataires Internet. La future législation en la matière doit avoir comme assise principale la directive européenne sur le commerce électronique.

8. Responsabilité civile

8.1 Remarques préliminaires

Outre le droit pénal, le droit civil joue un rôle considérable dans le régime des responsabilités qui détermine l'activité et les décisions d'investissement des prestataires de services Internet. L'indignation soulevée par la diffusion de contenus punissables (par ex. pornographie, discrimination raciale, représentation de la violence) relègue néanmoins au second plan les aspects de droit civil de la responsabilité comme la violation du droit de la propriété intellectuelle, du droit de la concurrence et du droit de la personnalité.

Pourtant, la jurisprudence étrangère montre que les plaintes de droit civil contre les fournisseurs d'accès et d'hébergement s'accumulent et que la responsabilité civile gagne en importance. Lorsque la responsabilité pénale des prestataires Internet est examinée, il est impossible, si l'on veut être cohérent, de laisser de côté les aspects civils de la responsabilité. Il convient à ce propos de tenir compte à parts égales des points communs et des divergences entre responsabilité pénale et responsabilité civile.

Bien que ses travaux aient été axés en premier lieu sur la responsabilité pénale, la commission d'experts s'est également interrogée sur une éventuelle modification des dispositions de droit civil régissant la responsabilité. S'appuyant sur le rapport explicatif accompagnant le projet de loi fédérale sur le commerce électronique [192], qui souligne la nécessité de réglementer la responsabilité des prestataires [193], la commission a examiné *en premier lieu* si une modification du droit civil répondait à une nécessité fondamentale. *En second lieu*, elle a analysé la pertinence d'une

[192] Rapport explicatif du 17 janvier 2001 relatif au projet de loi fédérale sur le commerce électronique (Révision partielle du code des obligations et de la loi fédérale sur la concurrence déloyale), <http://www.ofj.admin.ch/themen/e-commerce/vn-ber-b-d.pdf>.

[193] Op. cit., p. 9: « De même, les éventuelles adaptations du droit des biens immatériels et de la responsabilité pénale et civile du fournisseur d'accès dépendent pour l'essentiel des développements sur le plan international. Un besoin de légiférer n'existe pas dans l'immédiat. Des solutions adéquates peuvent être trouvées sur la base des règles actuelles. »

adaptation simultanée du droit pénal et du droit civil par rapport à une réforme étalée dans le temps des deux domaines du droit.

En dépit du caractère transfrontalier du flux d'informations sur Internet, la commission d'experts a renoncé à aborder le problème sous l'angle du *droit international privé*. Un examen de ces questions serait allé au-delà de son mandat, conformément auquel elle devait se prononcer notamment sur la teneur à donner à la responsabilité pénale des prestataires Internet.

Les éléments constitutifs décrits dans *les actes spéciaux de droit civil*, et plus précisément dans la loi sur le droit d'auteur (LDA, RS 231.1), dans la loi fédérale sur la protection des marques (LPM, RS 232.11) ainsi que dans la loi fédérale contre la concurrence déloyale (LCD, RS 241) sont traités au chapitre consacré à la responsabilité pénale (voir ci-dessus ch. 6.12).

8.2 Responsabilité non contractuelle

8.21 Bases de la responsabilité

Le droit suisse ne connaît pas de normes spécifiques de responsabilité qui régissent la responsabilité délictuelle en cas de violation du droit dans le domaine de l'utilisation d'Internet. Pour juger de cette question, il convient de se rapporter aux *dispositions générales du code des obligations* (CO, RS 220) sur la responsabilité découlant d'actes illicites (notamment en cas d'atteintes à la personnalité) ou aux *règles juridiques spéciales relatives à la responsabilité* (dans ce cas surtout art. 62 LDA, art. 55 LPM, art. 9 LCD). Cependant, les prétentions pécuniaires qui peuvent être élevées sur la base de ces lois spéciales sont également régies par les dispositions du code des obligations [194].

8.22 Responsabilité des fournisseurs d'accès et des fournisseurs d'hébergement

Le débat autour de la responsabilité civile des fournisseurs d'accès et des fournisseurs d'hébergement débute pratiquement comme celui qui a trait à la responsabilité pénale : lorsque l'infraction a été commise via Internet, l'identification et la recherche de la personne directement responsable d'une violation du droit semblent dans les faits parfois impossibles ou bien requièrent des moyens disproportionnés.

---

[194] Les *actions en cessation ou suppression du trouble* sont données contre tout comportement objectivement illégal. Une faute n'est pas nécessaire, pas plus que la preuve d'un dommage. Dans les conditions prévues par l'art. 41 CO, *l'action en dommages-intérêts* requiert la preuve d'un dommage, de l'illicéité du comportement, du rapport de causalité entre le comportement préjudiciable et la production du dommage ainsi que de la faute de la personne ayant agi de manière illicite. *L'action en réparation du tort moral* présuppose par contre, outre l'illicéité et le lien de causalité une violation de la personnalité d'une certaine gravité. Selon la jurisprudence traditionnelle, *l'action en rétrocession de bénéfices* en vertu de l'art. 423 CO existe indépendamment d'une faute.

Même si l'on identifie le responsable, une poursuite peut sembler d'avance vouée à l'échec. C'est notamment le cas lorsque cette personne se trouve à l'étranger ou ne dispose pas de moyens financiers suffisants qui pourraient servir de garantie en cas d'action en dommages-intérêts. Du point de vue du titulaire du droit, la question se pose de savoir s'il peut faire valoir des prétentions vis-à-vis de tiers pour la violation du bien juridiquement protégé. A cet égard, les fournisseurs d'accès et d'hébergement, qui participent au processus de communication, entrent aussi en considération.

L'art. 50 CO, auquel renvoient l'art. 28a CC ainsi que les lois spéciales, peut être invoqué à l'appui d'une action en réparation à l'encontre de ces personnes. Conformément à cet article, toute personne possède la légitimation passive pour les actions en dommages-intérêts si elle a pris part à une atteinte ou à une mise en danger d'un bien juridique protégé (en tant qu'instigatrice ou complice). Il n'est pas nécessaire qu'il y ait eu préalablement entente entre les fautifs. Il suffit que les participants soient obligés de reconnaître que leur comportement ou leur négligence est fautive et donc apte à provoquer l'atteinte portée au bien juridique protégé.

8.221 Prétentions à raison de la faute

Dans nombre de cas, la suite qui sera donnée aux demandes de dommages-intérêts à raison de la faute, déposées à l'encontre de fournisseurs d'hébergement et de fournisseurs d'accès, dépendra de l'appréciation qui sera faite des griefs de négligence qui, en cas d'omission, entrent en concurrence avec les griefs de violation d'une obligation d'agir. Les devoirs de diligence des fournisseurs d'accès et des fournisseurs d'hébergement à ce propos *ne sont pas encore clarifié*s [195] pour ce qui concerne la Suisse. A propos des fournisseurs d'accès, la question est de savoir si et, le cas échéant, dans quelle mesure on peut raisonnablement exiger d'eux qu'ils connaissent les contenus dont ils permettent l'accès. Et quant aux hébergeurs, il convient de déterminer si et, le cas échéant, dans quelle mesure les obligations de contrôle et de surveillance les concernent et, partant, jusqu'à quel point ils sont tenus de répondre de leurs violations.

Dans leur majorité, les ouvrages spécialisés soulignent qu'il n'y a devoir de vigilance que dans les limites *de ce qui est raisonnablement exigible et possible*. En cas de simple préparation de l'infrastructure technique pour le transport des données ou pour l'accès au réseau, on ne demande en général pas au prestataire de services de connaître et de contrôler les contenus transmis (ce qui revient à dénier toute responsabilité à raison de la faute des exploitants de réseaux et des fournisseurs d'accès pour les contenus étrangers illicites). Par contre, les avis divergent sur ce que l'on peut raisonnablement exiger du fournisseur de contenus quant à la connaissance et à la vérification des contenus étrangers illicites. Soit on admet un devoir restreint de connaissance des contenus étrangers, soit on admet un devoir restreint de vérification du contenu.

---

[195] Voir à propos de l'état de l'opinion en Suisse WEBER (Bibl.), p. 507 ss (fournisseurs d'accès) et 515 ss (fournisseurs d'hébergement), avec d'autres renvois; PHILIPPE GILLIÉRON, La responsabilité des fournisseurs d'accès et d'hébergement, RDS NF Vol. 121/I, p. 387 ss, en part. p. 430 ss. Voir à propos de l'état de l'opinion en Europe ANDREA SCHMOLL : Die deliktische Haftung der Internet-Service-Provider : Eine rechtsvergleichende Untersuchung zu Deutschland, Frankreich, England und den USA, Francfort/Main 2001.

En conséquence, la doctrine tend à *limiter la responsabilité des fournisseurs d'hébergement* et tient compte du fait que certains hébergeurs assument d'autres fonctions comme le suivi de sites web ou l'animation de forums de discussion.

8.222 Prétentions sans égard à une éventuelle faute

La prétention en cessation ou en suppression qui présuppose uniquement une atteinte illicite à des droits étrangers, ne requiert donc pas qu'il y ait eu faute. En conséquence, pour pouvoir élever une prétention en suppression, il suffit qu'il y ait eu participation causale adéquate à la violation du droit et possibilité (raisonnablement exigible) de la prévenir. Les demandes de blocage ou d'effacement pourraient de ce fait être imposées à l'encontre des fournisseurs d'hébergement et des fournisseurs d'accès, même si ce n'est que dans la mesure où le blocage ou l'effacement sont techniquement possibles et raisonnablement exigibles. Dans l'appréciation de ce dernier critère, il conviendra, en accord avec la doctrine et la jurisprudence en Europe, de *mettre en relation le déploiement de mesures techniques avec la possibilité de les contourner*.

La *question* se pose néanmoins de savoir si chaque individu qui contribue par une cause partielle à une chaîne causale aboutissant à une violation du droit possède la légitimation passive et est tenu de faire cesser ou de prévenir la violation du droit juridique protégé. L'exigence d'une limitation de la responsabilité pour les fournisseurs d'accès et d'hébergement existe donc également en relation avec les actions en cessation et en suppression de l'acte incriminé. Il est partiellement tenté de l'atteindre par la notion de causalité adéquate. En Allemagne, le législateur a eu aussi recours dans ce contexte à la notion de « perturbateur » issue du droit administratif (cf. ci-dessus ch. 5.12). En Suisse, cette question n'a pas, jusqu'à ce jour, fait l'objet d'une discussion approfondie.

8.23 Nécessité de légiférer

Il ressort des considérations développées ci-dessus que le droit suisse en matière de responsabilité des fournisseurs d'accès et des fournisseurs d'hébergement *manque de clarté*, ce qui pourrait se répercuter négativement sur les décisions d'investissement des acteurs économiques. Même si la jurisprudence en Suisse livre probablement des solutions soutenables quant à l'interprétation des dispositions générales relatives à la responsabilité, il faudrait des années avant que les lignes de force d'une réglementation ne se dessinent. La nécessité de renforcer rapidement la sécurité du droit demande donc que ce soit le législateur qui apporte une réponse aux questions de droit en suspens. Cette clarification pourrait avoir lieu dans le cadre soit de la *loi fédérale sur le commerce électronique*, soit des travaux relatifs à la *loi fédérale sur la révision et l'unification du droit de la responsabilité civile (loi sur la responsabilité civile)* [196].

[196] Ces deux projets de révision n'en sont pas au même stade de la procédure : le 9 décembre 2002, le Conseil fédéral a mandaté le DFJP d'élaborer un message relatif à la *loi sur le commerce électronique*. Au cours de l'année 2003, il a pris connaissance du résultat de la procédure de consultation relative à l'avant-projet de loi fédérale sur *la révision et l'unification du droit de la responsabilité civile*. Il conviendra de tenir compte de cette différence au niveau de l'état des

Insensible aux frontières, Internet requiert une *uniformisation à l'échelle internationale des dispositions* régissant la responsabilité des prestataires. Aucun effort n'est entrepris à ce niveau pour harmoniser de manière cohérente cette responsabilité en droit civil et en droit pénal et il faudra probablement attendre encore longtemps avant de voir naître une solution rassemblant les nations. La voie *suisse* s'impose donc d'ici là. Néanmoins, même si elle s'attèle à une réglementation nationale, la Suisse ne peut se soustraire à la dimension mondiale de la question. Il conviendra donc de tenir compte des tentatives de solution et des expériences rassemblées à l'étranger (cf. ci-dessus chapitre 4).

Dans ce contexte, les art. 12 à 15 de la *directive européenne sur le commerce électronique* [197] peuvent servir de point de départ à une réglementation nationale. Les premières expériences tirées de son application montrent cependant qu'il faut édicter des règles complémentaires spécifiques pour les prétentions en cessation ou en suppression de l'acte incriminé, permettant de clarifier, sur la base du droit civil, la question des obligations de blocage et d'effacement. Enfin, la responsabilité concernant les liens devra aussi faire l'objet d'une réglementation.

8.24 Coordination avec le droit pénal

La responsabilité pénale et la responsabilité civile *présentent*, dans le contexte de la cybercriminalité, différents *points de convergence*. La solution de droit pénal proposée par la commission d'experts (cf. ci-dessous chapitre 9) permet de poser des appréciations à propos de la responsabilité des fournisseurs d'accès et des fournisseurs d'hébergement qui sont également déterminantes quant aux prétentions en dommages-intérêts à raison de la faute qui relèvent du droit civil. Cela concerne en premier lieu l'appréciation d'éventuels devoirs de contrôle ou de surveillance. Pour leur part, les éléments constitutifs de l'infraction peuvent constituer des normes de protection qui fondent l'illicéité en cas de simple dommage patrimonial [198]. En outre, les éléments de droit civil constitutifs de la violation du droit consacrés par des normes sont également assortis de sanctions pénales. A cet endroit, se pose la question concrète de l'application du droit pénal des médias, ou de la réglementation ici proposée, aux actes commis par le biais des réseaux de communication électronique.

Il ne faudrait toutefois pas négliger les *différences structurelles* qui séparent les deux domaines du droit : en droit pénal, la négligence ne joue guère de rôle e^n regard des délits dont il est ici question. En particulier, la complicité au sens du droit pénal,

---

procédures respectives lors du choix du projet auquel il conviendra d'intégrer une réglementation de la responsabilité des fournisseurs accès et et des fournisseurs d'hébergement.

[197] Directive 2000/31/CE du Parlement européen et du Conseil 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 (« directive européenne sur le commerce électronique », cf. ci-dessus chapitre 4).

[198] Selon la jurisprudence du Tribunal fédéral (voir par ex. ATF 119 II 127 cons. 3) et selon la doctrine dominante, la norme relative à la responsabilité de l'art. 41 CO est fondée sur la théorie objective de l'illicéité. Selon cette théorie, un dommage est illicite s'il est contraire à un devoir légal général soit parce qu'il porte atteinte à un droit absolu du lésé (*Erfolgsunrecht*), soit parce qu'il provoque un pur préjudice patrimonial en enfreignant une norme de protection du bien juridique atteint (*Verhaltens-unrecht*).

qui est régulièrement mise en avant comme base juridique permettant éventuellement d'inférer une responsabilité des prestataires Internet, présuppose qu'il y ait eu intention. Or la complicité de droit civil au sens où l'entend l'art. 50 CO peut aussi s'opérer par négligence. Il convient en outre de souligner que la notion civile de faute est une notion objectivée. Par conséquent, la question de savoir ce que l'on peut raisonnablement exiger d'éventuelles contre-mesures des prestataires est examinée en droit civil selon des critères généraux et non en fonction des circonstances spécifiques caractérisant chaque prestataire. Et surtout, la question de la responsabilité civile se posant en relation avec les prétentions de droit civil en cessation et suppression de l'acte incriminé, qui sont soulevées sans égard à une éventuelle faute, déborde le cadre de la question pénale qui présuppose la culpabilité.

Au vu des différences mises en relief ci-dessus, une *réglementation transversale* englobant droit pénal et droit civil s'impose tout aussi peu que deux réglementations parallèles pour chacun des deux domaines de droit. L'analyse dogmatique approfondie qui devra présider à l'élaboration d'une proposition concrète de solution dans le domaine de la responsabilité civile - solution qui devrait s'appuyer sur l'art. 50 CO - plaide davantage en faveur de deux réglementations distinctes.

8.3 Responsabilité contractuelle des fournisseurs d'accès et des fournisseurs d'hébergement

L'appréciation de la responsabilité contractuelle des prestataires Internet [199] ne présente qu'un rapport limité avec l'exposé de la question sur le plan pénal : ce rapport existe surtout lorsque, face à une éventuelle responsabilité pénale, un prestataire Internet ne peut plus ou ne peut correctement fournir les prestations contractuelles, cela de son propre chef ou suite à une décision de blocage ou à une autre mesure prononcée par les autorités de poursuite pénale. Néanmoins, les conventions contractuelles et le droit en vigueur (art. 97 CO) permettent d'apporter des solutions adéquates dans ce genre de cas [200]. En particulier lorsque la perturbation de la prestation repose sur un acte de puissance publique (par ex. une décision de blocage), elle ne peut pas être imputée au prestataire obligé. Il conviendrait de se prononcer dans un autre sens notamment si on pouvait reprocher au prestataire, en sa qualité d'obligé, d'avoir omis des mesures techniques usuelles et raisonnablement exigibles qui auraient permis un blocage des contenus incriminés sans entraver pour autant la fourniture des prestations à laquelle il est tenu contractuellement. .

Même si la thématique de la responsabilité contractuelle et celle de la question de droit pénal présentent des points de concordance, la commission d'experts n'estime pas nécessaire que le législateur intervienne dans le droit des obligations.

---

[199] Voir à propos de la responsabilité contractuelle en général WEBER (Bibl.), p. 511 ss (fournisseurs d'accès) et 521 ss (fournisseurs d'hébergement), avec d'autres renvois.

[200] MARKUS H. BERNI: Die zivil- und strafrechtliche Verantwortung des ISP, in: Hans Rudolf Trüeb (Editeur), Aktuelle Rechtsfragen des E-Commerce, Zurich 2001, p. 117 ss, 134, rejette d'une manière générale l'idée d'une responsabilité en se prévalant de l'art. 20 CO.

8.4 Conclusions de la commission d’experts

De l’avis de la commission d’experts, la question de la responsabilité extra-contractuelle des prestataires de services Internet, notamment des fournisseurs d’accès et des fournisseurs d’hébergement, doit être clarifiée par le législateur. A cet égard, la légitimation passive de ces prestataires en cas d’actions en cessation et en suppression devra faire l’objet d’une analyse approfondie.

Par ailleurs, la commission estime que ces questions pourraient trouver une solution positive soit dans la *loi fédérale sur le commerce électronique*, soit dans le cadre des travaux sur *la loi fédérale sur la révision et l’unification de la responsabilité civile* (loi sur la responsabilité civile) avec comme assise la directive européenne sur le commerce électronique ; la réglementation adoptée en Suisse devra, bien sûr, répondre aussi aux questions fondamentales que la directive de l'UE laisse au législateur de chaque Etat membre le soin de régler.

9. Propositions de la commission d'experts

Proposition de législation (modification du code pénal)

(nouveau titre) 6. Infractions commises sur des réseaux de communications électroniques et dans des médias

Art. 27 CP (nouveau) Infractions commises sur des réseaux de communications électroniques

1. Lorsqu'une infraction aura été commise par voie de transmission, de préparation ou de mise à disposition d'informations sur un réseau de communications électroniques, les règles générales sont applicables sous réserve des dispositions suivantes.

2. Lorsque l'auteur de l'infraction est auteur ou rédacteur au sens de l'art. 27bis, sa punissabilité est régie par cette disposition.

3. La personne qui aura mis à disposition, selon un procédé automatisé, des informations d'autrui sur un réseau de communications électroniques sera punissable aux conditions prévues à l'art. 322bis, ch. 1. La mise à disposition d'un répertoire intégrant des informations d'autrui selon un procédé automatisé est considérée comme mise à disposition d'informations d'autrui.

4. Celui qui se borne à fournir l'accès à un réseau de communications électroniques n'est pas punissable. Le stockage automatique et temporaire d'informations d'autrui suite à la consultation d'un site est considéré comme une fourniture d'accès.

Art. 27bis (nouveau) CP ***Infractions commises dans des médias***

[1] Lorsqu'une infraction aura été commise et consommée sous forme de publication dans un média, l'auteur sera seul punissable, sous réserve des dispositions suivantes.

[2] Si l'auteur ne peut être découvert ou qu'il ne peut être traduit en Suisse devant un tribunal, le rédacteur responsable est punissable en vertu de l'art. 322bis, ch. 2. A défaut de rédacteur, la personne responsable de la publication en cause est punissable en vertu de ce même art., ch. 2.

[3] Si la publication a eu lieu à l'insu de l'auteur ou contre sa volonté, le rédacteur ou, à défaut, la personne responsable de la publication, est punissable comme auteur de l'infraction.

[4] L'auteur d'un compte rendu véridique de débats publics ou de déclarations officielles d'une autorité n'encourra aucune peine.

L'art. 27bis CP inchangé devient l'art. 27ter (nouveau) CP *Protection des sources*

Art. 322bis (nouveau) CP Défaut d'opposition à une infraction commise sur un réseau de communications électroniques et dans un média

(nouveau) 1. Celui qui aura mis à disposition, selon un procédé automatisé, sur un réseau de communications électroniques, des informations d'autrui dont il est sûr qu'elles constituent une infraction et qui aura omis d'en prévenir l'utilisation, bien qu'on puisse techniquement et raisonnablement l'exiger de lui, sera puni de l'emprisonnement ou de l'amende.

Celui qui aura mis à disposition, selon un procédé automatisé, sur un réseau de communications électroniques, des informations d'autrui constituant une infraction et qui aura omis de transmettre aux autorités de poursuite pénale les avertissments qui lui ont été adressés par des tiers et lui sont effectivement parvenus, sera puni de l'emprisonnement ou de l'amende.

Si l'infraction au sens des al. 1 et 2 est poursuivie sur plainte, l'acte ne sera poursuivi que si cette plainte a été effectivement déposée.

La question de savoir si une infraction au sens des al. 1 et 2 peut être commise au moyen d'une information doit être appréciée en vertu du droit suisse.

Les informations au sens des al. 1 et 2 seront supprimées, que la Suisse ait ou non une compétence juridictionnelle.

(texte modifié de l'art. 322bis) 2. La personne responsable au sens de l'art. 27bis, al. 2 et 3, d'une publication constituant une infraction sera punie de l'emprisonnement ou de l'amende si intentionnellement, elle ne s'est pas opposée à la publication. Si elle a agi par négligence, la peine sera les arrêts ou l'amende.

Art. 340ter (nouveau) CP En matière d'infractions commises sur les réseaux de communications électroniques

1 Sont également soumises à la juridiction fédérale les infractions commises sur des réseaux de communications électroniques :

a. si plusieurs cantons sont concernés par l'infraction sans qu'il y ait de prédominance évidente dans l'un d'entre eux ; ou
b. si une procédure d'investigation est nécessaire dans plusieurs cantons.

2 Le Ministère public de la Confédération peut en outre ouvrir une procédure d'investigation si une autorité cantonale de poursuite pénale compétente sollicite de celui-ci la reprise de la procédure.

3 L'ouverture de la procédure d'investigation prévue à l'al. 2 fonde la compétence fédérale.

Adaptations nécessaires au regard des propositions ci-dessus

Art. 347 CP

[1] Pour les infractions prévues à l'art. 27bis commises en Suisse, la compétence appartient à l'autorité du lieu où …

Art. 18bis Procédure pénale fédérale (PPF, RS 312.0)

[1] Après la clôture de l'instruction, le procureur général peut déléguer aux autorités cantonales le jugement d'une affaire de droit pénal fédéral au sens de l'art. 340, ch. 2, de l'art. 340bis et de l'art. 340ter du code pénal. Dans ce cas, il soutient l'accusation devant le tribunal cantonal.
[2] (inchangé)
[3] (inchangé)

Art. 26 Loi fédérale sur le Tribunal pénal fédéral (LTPF, non encore en vigueur)

La cour des affaires pénales statue :
a. sur les affaires qui relèvent de la juridiction fédérale en vertu des art. 340, 340bis et 340ter du code pénal, pour autant que le procureur général de la Confédération n'en ait pas délégué l'instruction et le jugement aux autorités cantonales ;
b. …

9.1 Projet de réglementation de la commission d'experts et commentaire relatif à la proposition de législation

9.11 La réglementation de la responsabilité : considérations générales

Face à l'interperméabilité croissante des différents réseaux de communications électroniques et à la mutation rapide des technologies de l'information, il s'impose avant tout de ne pas délimiter le domaine de réglementation de la cybercriminalité en en fonction des seules notions de « Internet » et « transport de données TCP/PI » 201.

Par ailleurs, une réglementation stable et durable des faits touchant à Internet doit couvrir divers domaines qui se recoupent dans le champ de la communication, de l'information et des services de médias, par conséquent se référer aux supports et contenus de la communication. A cet égard, nous avons tenté ci-après (ch. 9.12)[202] de **dégager** *plusieurs approches.*

9.12 Approche horizontale ou réglementation spécifique par domaine ?

9.121 Une réglementation horizontale pour tous les domaines du droit

Le législateur pourrait réglementer la responsabilité et la punissabilité pour tous les participants dans un texte légal distinct. Cette réglementation serait pareillement contraignante pour le droit pénal, le droit de la responsabilité civile, le droit d'auteur, le droit de la concurrence, etc. C'est la voie qu'a choisie par exemple l'Allemagne avec la *Teledienstegesetz* (TDG, loi sur les téléservices) du 22 juillet 1997 203. De même, la *directive européenne sur le commerce électronique* 204 préconise fondamentalement une « réglementation » uniforme « de la responsabilité ». Néanmoins, une réglementation horizontale pourrait aussi être intégrée dans une loi existante. Ainsi, en Suisse, on a, par exemple, proposé d'extraire des textes relevant des différents domaines du droit les normes concernant la responsabilité et la punissabilité pour les intégrer dans la *loi sur les télécommunications* (LTC, RS 784.10).

Mais l'atout d'une réglementation horizontale - qui doit être de clarifier, dans une loi autonome, toutes les questions de responsabilité et de punissabilité en droit public et en droit civil - est contrebalancé par des inconvénients de poids. Ce genre de « loi dans la loi » crée d'énormes problèmes d'intégration dans le système des conditions de la responsabilité et de la punissabilité statuées par les lois existantes (CP, CO).

---

201 Pour plus de détails, cf. ci-dessus, chiffre 2.44.

202 Voir à ce propos NIGGLI/SCHWARZENEGGER (Bibl.), p. 63 et 66 ss.

203 Modifiée par la loi intitulée *Gesetz über die rechtlichen Rahmenbedingungen für den elektronischen Geschäftsverkehr* (EGG, loi relative aux conditions-cadres légales du commerce électronique) en vigueur depuis le 22.12.2001, cf. BGBl. I 2001 p. 3721. La réglementation de la responsabilité figure aux §§ 8 à 11 TDG (nouvelle version) ; cf. ci-dessus chapitre 4, ch. 4.31.

204 Cf. art. 12 ss de la directive européenne sur le commerce électronique ; voir ci-dessus chapitre 4.

Ainsi, en *Allemagne*, les avis divergent, eu égard au code pénal, sur la manière de classer les §§ 8 ss TDG dans la hiérarchie de la punissabilité 205. Avec les notions horizontales de « connaissance » et de « responsabilité », on s'éloigne tant en droit civil qu'en droit pénal de l'arsenal des notions familières, ce qui suscite encore d'autres difficultés d'interprétation. Sur d'autres questions, comme celle de la punissabilité du renvoi-liens à des contenus illicites, la réglementation horizontale de la loi allemande sur les téléservices (notamment § 5 TDG ancienne version) a créé une confusion supplémentaire 206. Même si l'on s'en tient aux principes figurant dans la directive européenne sur le commerce électronique, une réglementation horizontale ne s'impose pas nécessairement.

En *France*, une modification importante des conditions de la punissabilité pour les prestataires est intervenue en 2000. Le principe de la responsabilité restreinte a été introduit dans la loi relative à la liberté de communication à l'art. 43-8, al. 1. Selon ce principe, le fournisseur d'hébergement n'est pénalement responsable que si, ayant été saisi par une autorité judiciaire, il n'a pas agi promptement pour empêcher l'accès au site incriminé. Il apparaît aussi clairement que par cette réglementation, toute punissabilité des fournisseurs d'accès disparaît. Le projet de loi prévoyait un complément plus strict de l'art. 43.8. Ainsi, il établissait à l'art. 43.8, al. 2 qu'il pouvait également y avoir punissabilité si le fournisseur d'hébergement avait été informé par un utilisateur et n'avait pas réagi à cette communication. Cette phrase a été néanmoins déclarée non conforme à la Constitution par décision du Conseil constitutionnel. Or elle ne se référait qu'aux conditions de la punissabilité car, selon le droit pénal français, la complicité présuppose une intention directe. Le dol éventuel qui aurait été pris en compte par la formulation de l'art. 43-8, al. 2 du projet de loi n'existe pas dans le cadre des délits intentionnels 207. Une première proposition de loi du 14 juin 2001 visant la mise en application de la directive européenne sur le commerce électronique ne prévoyait donc plus qu'une limitation de la responsabilité spécifique pour le droit civil 208.

---

205 On ne connaît jusqu'ici aucune modification des Dispositions générales du Code pénal allemand par des textes légaux extérieurs au droit pénal, raison pour laquelle la prétendue clarté de la réglementation horizontale a fait naître de nouveaux problèmes et des avis contraires dans la doctrine pénale (« Vorfilterlösung » [fonction de filtre préalable du § 5 TDG], modification de l'élément constitutif, justification, exclusion de la faute, motif de libération de la peine, fonction de filtre ultérieur). Cf. à ce propos NIGGLI/SCHWARZENEGGER (Bibl.), p. 66.

206 En résumé CHRISTIAN SCHWARZENEGGER: Die strafrechtliche Beurteilung von Hyperlinks, in: Festschrift Rehbinder, München 2002, p. 723 ss avec d'autres renvois; même avec la clarification apportée par la nouvelle version de la TDG, la confusion demeure ; voir entre autres HENNING ROSENAU / LARS WITTECK, Der Castor-Transport und die Hakenkralle im Internet, JURA 2002, 781 ss.

207 Loi du 1er août 2000 relative à la communication (loi n° 2000-719 du 1er août 2000, modifiant la loi n° 86-1067 du 30 septembre 1986 relative à la liberté de communication, JO du 2 août 2000, 11903). Pour le libellé de l'art. 43-8 de cette loi, se reporter plus haut, ch. 4.33. Voir égal. Conseil constitutionnel, Décision n° 2000-433 DC du 27 juillet 2000, JO du 2 août 2000, 11922 ss, notamment 11926. Pour plus de détails, MOREILLON/DE COURTEN, (Bibl.), p.12 avec renvoi.

208 Voir le projet de loi sur la société de l'information, enregistré à la Présidence de l'Assemblée nationale le 14 juin 2001. A la suite du changement de gouvernement, ce projet de loi a été retiré. Depuis, le Ministère de l'Industrie a déposé un nouveau projet de loi le 15 janvier 2003 (Projet de loi pour la confiance dans l´économie numérique) qui prévoit deux normes indépendantes pour la responsabilité civile et la punissabilité des fournisseurs d'hébergement (nouveaux art. 43-8 et art. 43-9) dans la loi relative à la liberté de communication (loi n° 86-1067 du 30 septembre 1986). L'exonération de la responsabilité et l'impunité du fournisseur d'accès pour la transmission automatique sont désormais codifiées dans le Code des postes et télécommunications (nouvel art. L. 32-3-3). Au *Japon*, une réglementation spécifique a été introduite ; cf. Law concerning limitation of

De l'avis de la commission d'experts, *il n'apparaît pas souhaitable* d'opter pour une réglementation horizontale dans le cadre d'une « loi de responsabilité Internet ».

Au surplus, une réglementation horizontale dans la loi sur les télécommunications ne suffirait pas car la notion de services de télécommunication ne couvre que les activités de fourniture d'accès en vue de l'utilisation d'informations (cf. art. 3 LTC), mais non la préparation ou la mise à disposition de la transmission au moyen de techniques de télécommunication. Les questions de dogmatique pénale en relation avec l'hébergement n'en seraient pas résolues et l'insécurité du droit persisterait. Par ailleurs, l'art. 2 LTC prévoit une exception pour la diffusion et de la rediffusion de programmes au sens de la loi fédérale sur la radio et la télévision (LRTV, RS 784.40), qui couvrirait probablement aussi la radio et la télévision Internet. Enfin, la LTC ne vise que les services de télécommunication, mais non les services d'informations et de médias 209. La commission d'experts tient donc également pour inadéquat ce cadre de réglementation.

9.122 Réglementation spécifique dans les différents domaines du droit

La commission d'experts préconise par conséquent une solution propre à chaque domaine, dont la priorité serait l'adaptation du code pénal. Cette option permet, d'une part, une adaptation immanente au système des conditions de la punissabilité - adaptation qui ne touche ni à la structure des éléments constitutifs, ni aux notions spécifiques traditionnelles.

Le droit pénal et le droit civil règlent des domaines pour la plupart très différents. En effet, les éléments constitutifs de nombre d'infractions relevant de la cybercriminalité sont conçus pour protéger les intérêts collectifs, et non des intérêts individuels de lésés. Au surplus, les dispositions en question sanctionnent les auteurs dès le stade de la mise en danger d'un bien juridique. D'autre part, cette option n'entrave en rien une adaptation des conditions de la responsabilité civile respectueuse des intérêts spécifiques des parties et harmonieuse sur le plan de la dogmatique. Ce procédé par étapes sera mieux à même d'aboutir à une situation juridique claire et durable.

9.13 Les trois piliers de la nouvelle réglementation

- S'agissant des réseaux de communications électroniques, il convient de clarifier les limites de la punissabilité des prestataires d'infrastructures à propos des procédés automatisés. Si la participation des fournisseurs d'accès se limite à une simple fourniture d'accès, celle-ci doit demeurer impunie. En ce qui concerne les fournisseurs d'hébergement, la différence devra être faite entre le cas le plus courant du transfert automatisé des données, dont ils ne connaissent rien, et les circonstances dans lesquelles ils détectent ultérieurement la punissabilité (éventuelle) des contenus. Dans le premier cas, ils ne sont pas punissables, dans le second par contre, ils le sont s'ils n'entreprennent rien. Un large consensus règne à cet égard à l'échelle internationale.

---

damages to specific telecommunications service provider and disclosure of sender information, passed on November 22, 2001.

209 NIGGLI/SCHWARZENEGGER (Bibl.), p. 68.

- Le problème des « comportements neutres » est ainsi désamorcé de manière sectorielle (cf. à ce propos ci-dessus ch. 6.3). Des conditions-cadres pénales uniformes et claires sont imposées aux prestataires d'infrastructures des réseaux de communications électroniques.

- Enfin, la nouvelle réglementation doit formuler des critères de délimitation précis entre le droit pénal des médias et le droit pénal des réseaux informatiques. D'une part, le privilège dont bénéficient les médias en matière de communication sur les réseaux doit être maintenu, mais de l'autre des solutions claires doivent être proposées pour tous les autres états de fait qui sortent du cadre de ce droit pénal spécial.

9.2 Commentaire relatif à l'art. 27 (nouveau) CP [210]

9.21 Titre marginal 6 : « Infractions commises sur des réseaux de communications électroniques et dans des médias »

La commission d'experts a établi les lignes de force de la réglementation sur les prémisses suivantes :

- La réglementation spéciale de la responsabilité pénale ne doit *pas se rapporter uniquement au réseau Internet* (cf. ci-dessus chapitre 2, ch. 2.24, 2.4 à 2.6).
- Elle est *neutre du point de vue technologique* dans la mesure où elle ne prend en compte ni le mode de transmission des informations (transmission sur des lignes ou transmission sans fil) ni l'infrastructure de transmission (conduite téléphonique, conduite électrique, etc.).
- La réglementation spéciale de la punissabilité *n'est pas rattachée à la publication* [211]. Elle couvre donc en principe aussi les contenus punissables transmis par courrier électronique.
- La réglementation spéciale de la punissabilité ne vise pas seulement les délits d'expression, mais *tous* les délits commis par le biais de la transmission, de la préparation ou de la mise à disposition d'informations sur les réseaux de télécommunication.
- La réglementation *est applicable* que les informations soient accessibles unilatéralement (par ex. dans le cadre des émissions traditionnelles de radio et de télévision) ou de manière interactive, c'est-à-dire dans le cadre de l'échange bilatéral de données (par ex. dans les conversations téléphoniques ou dans l'envoi et la réception de courrier électronique). Elle englobe aussi la

---

210 Le *commentaire* de la proposition de nouvelle réglementation porte sur les chiffres 9.2 (art. 27 CP), 9.3 (nouvel art. 322bis CP) et 9.4 (nouvel art. 340bis CP) - L' « art. 27 CP » désigne l'art. 27 du code pénal dans sa version actuelle (donc le droit pénal des médias) ; lorsque notre projet de révision s'y réfère, cette référence est indiquée par la mention « art. 27 (nouveau) CP». Il sera procédé de manière analogue pour les autres propositions de nouvelles prescriptions.

211 C'est le cas de l'actuel art. 27, al. 1 CP qui exclut la communication individuelle. Selon la jurisprudence du Tribunal fédéral, le critère de la publication suppose que le contenu en question soit destiné à la publication et non pas seulement à des personnes individuellement déterminées (ATF125 IV 177, 183 s.).

communication à sens unique. Tombent donc également sous le coup de la réglementation prévue la diffusion des programmes de radio et de télévision par les réseaux câblés traditionnels ou, dans un proche avenir, dans le cadre de la télévision numérique (Digital Video Broadcasting, DVB) ou de la radio numérique (Digital Audio Broadcasting, DAB) [212].

Trois dénominations entrent en ligne de compte pour circonscrire *de manière générique* tous les domaines mentionnés :

9.211 Infractions commises «sur un réseau de télécommunication »

Le droit suisse actuel ne connaissant pas cette notion, le *but* est ici d'appréhender les phénomènes suivants non couverts par la LTC :

- La préparation et la mise à disposition d'informations (et pas seulement leur transmission [213]).
- Les programmes au sens de la LRTV [214].
- Les services d'information et de médias (et pas seulement les services de communication).

Cette terminologie a *d'une part* l'inconvénient de ne pas se référer à des définitions existantes, ce qui devrait nécessiter un certain déploiement d'argumentation tant en procédure législative que dans l'application du droit. *D'autre part*, la notion de télécommunication est rattachée initialement à la communication individuelle comme la téléphonie ou la télégraphie et s'est aussi partiellement éloignée de la notion de programmes de radio et de télévision transmis unilatéralement (en général, on entend par radio et télécommunication deux domaines distincts l'un de l'autre). Pour le moins, il n'est pas manifeste que la notion de « réseaux de télécommunication » englobe également la communication unilatérale.

9.212 Infractions commises « par voie de transmission ou de mise à disposition d'informations au moyen de techniques de télécommunication »

Cette formulation, très proche de la terminologie de la loi sur les télécommunications, ne prend pas seulement en compte la transmission, mais aussi la mise à disposition d'informations. Elle a néanmoins deux inconvénients. D'une part, elle est lourde du point de vue stylistique; d'autre part, elle pourrait être une source de confusion car la notion de techniques de télécommunication est souvent mise sur le même plan que téléphonie. Cette formulation n'indique pas clairement que les programmes de radio et de télévision, que l'art. 2 LTC exclut du domaine de réglementation, sont

---

[212] Il convient de souligner que; dans le domaine de la communication unilatérale, la fonction de fournisseur d'hébergement n'existe pas actuellement. La nécessité de clarifier les conditions de la punissabilité s'impose toutefois ici aussi : les fournisseurs de contenus doivent en principe être soumis aux règles générales, et les purs transmetteurs d'information par contre être exclus de la punissabilité.

[213] L'art. 2 LTC règle la transmission au moyen de techniques de télécommunication.

[214] N'est pas pris en compte conformément à l'art. 2 LTC.

également compris. La prise en compte des programmes de radio et de télévision devrait donc être réglementée de manière explicite au surplus [215].

9.213 Infractions commises sur des « réseaux de communications électroniques »

Cette notion est très large et a l'avantage de se rattacher à la terminologie du droit européen. On trouve une *définition* de la notion de réseau de communications électroniques à l'art. 2, let. a de la directive de l'UE relative à un cadre réglementaire commun pour les réseaux et services de communications électroniques de mars 2002 [216]:

> "Réseau de communications électroniques" : les systèmes de transmission et, le cas échéant, les équipements de commutation ou de routage et les autres ressources qui permettent l'acheminement de signaux par câble, par voie hertzienne, par moyen optique ou par d'autres moyens électromagnétiques, comprenant les réseaux satellitaires, les réseaux terrestres fixes (avec commutation de circuits ou de paquets, y compris l'Internet) et mobiles, les systèmes utilisant le réseau électrique, pour autant qu'ils servent à la transmission de signaux, les réseaux utilisés pour la radiodiffusion sonore et télévisuelle et les réseaux câblés de télévision, quel que soit le type d'information transmise.“

C'est cette notion de « réseau de communications électroniques » qui recouvre avec le plus de précision toutes les fonctions de réseau qu'il convient d'inclure. Le titre marginal 6 doit donc être refondu en «Infractions commises sur des réseaux de communications électroniques et dans des médias ».

L'imprécision inhérente à la tournure *« sur des* réseaux de communications électroniques » doit être tolérée. En effet, le titre doit constituer une notion générique à la fois pour les infractions, commises au travers des réseaux de communications électroniques, et pour les délits de média qui doivent être consommés sous forme de publication. En revanche, une précision est apportée par l'art. 27 (nouveau), ch. 1 qui parle d'« infraction … commise par voie de transmission, de préparation ou de mise à disposition d'informations sur un réseau de communications électroniques » [217].

---

[215] Cela vaut au moins jusqu'à la révision totale de la LRTV qui, quant à la diffusion, impliquera également une modification de l'art. 2 LTC. A l'avenir, la diffusion des programmes de radio et de télévision sera régie par le droit des télécommunications ; cf. le message du Conseil fédéral du 18 décembre 2002 relatif à la révision totale de la radio et de la télévision, FF 2003 1659 s.

[216] Directive 2002/21/CE du Parlement européen et du Conseil du 7 mars 2002 relative à un cadre réglementaire commun pour les réseaux et services de communications électroniques (directive "cadre") Journal officiel n° L 108 du 24/04/2002 p. 33 à 50; disponible sur Internet à l'adresse : www.europa.eu.int/smartapi/cgi/sga_doc?smartapi!celexapi!prod!CELEXnumdoc&lg=DE&numdoc=32002L0021&model=guichett (état au 9.4.2003).

[217] Les infractions ne sont commises qu'en partie seulement « sur » la Toile. Il est également possible que la Toile soit seulement un moyen de parvenir à ses fins et ne joue qu'un rôle tout à fait secondaire (par ex. dans le cas de l'escroquerie).

9.22 Art. 27 (nouveau), ch. 1 CP (fournisseurs de contenus)

9.221 « Infractions commises par voie de … »

La formulation « infraction commise *par voie de* » a une portée plus large que « infraction commise *sur* ou *dans* » et a pour but d'englober tous les actes en rapport avec la transmission, la préparation ou la mise à disposition d'informations sur les réseaux de communications électroniques. Cette disposition entend aller au-delà du domaine qui est d'ordinaire mentionné comme l'exemple même de la cybercriminalité, à savoir les délits dits "d'expression" (représentations de la violence, pornographie dure, discrimination raciale, atteinte à l'honneur, etc.).

Certes, ce domaine doit être compris dans la réglementation, mais le champ d'application de cette dernière *ne doit pas s'y limiter*. Les délits informatiques par exemple, notamment la diffusion de virus informatiques, doivent aussi être soumis à la nouvelle réglementation (art. 144bis, ch. 2 CP). Celle-ci vise également tous les délits dits traditionnels (par ex. les délits patrimoniaux tels que l'escroquerie, art. 146 CP, ou l'utilisation frauduleuse d'un ordinateur, art. 147 CP; elle porte aussi sur les délits du droit pénal accessoire, dont ceux qui ont trait à la concurrence déloyale ou àla protection des marques ; cf. la liste figurant ci-dessus au ch. 2.2).

9.222 Transmission, préparation, mise à disposition

La disposition de l'art. 27 (nouveau) CP porte sur *trois aspects fondamentaux* de l'utilisation des réseaux, à savoir :

- la transmission, c'est-à-dire l'émission ou la réception d'informations, sur des lignes ou par des ondes hertziennes, au moyen de signaux électriques, magnétiques, optiques ou autres signaux électromagnétiques ;
- la préparation, c'est-à-dire le chargement d'informations sur un support de données public, accessible par le biais de réseaux de communications électroniques ;
- la mise à disposition, c'est-à-dire l'entretien d'un support de données public, accessible par le biais de réseaux de communications électroniques, sur lequel des informations sont stockées.

La dernière étape dans le processus de communication, *l'interrogation (ou consultation)*, est en général le fait de *l'utilisateur*. A ce stade, une telle action n'est pas punissable, mais peut le devenir si l'utilisateur stocke des informations sur un support local personnel (cf. art. 197, ch. 3bis CP).

9.223 Informations

La notion d' « informations » est très large puisqu'elle inclut aussi les programmes informatiques [218]. Le projet de loi ne se limite donc pas aux « délits d'expression» sur Internet [219], mais va plus loin : il entend aussi mettre en place une réglementation de la responsabilité de la cybercriminalité [220] et des délits pénaux en matière de droit d'auteur [221].

La commission d'experts a également examiné la notion de *contenus illicites*, mais ne l'a pas retenue. Cette notion ne couvre pas l'ensemble du domaine des informations requises; par exemple, dans le cas d'offres frauduleuses ou violant le droit d'auteur sur la Toile, ces contenus ne sont pas illégaux en eux-mêmes, mais c'est leur utilisation qui est illégale. Par ailleurs, la notion de contenu illicite est contestée dans sa portée. De ce fait, le projet utilise de manière systématique le terme d' « informations ». C'est d'ailleurs le terme figurant dans la LTC ainsi que dans la directive européenne sur le commerce électronique. La notion d'informations englobe aussi les contenus illégaux.

9.224 Applicabilité des règles générales

Le projet établit à l'art. 27 (nouveau), ch. 1 que les règles générales sont en principe aussi applicables aux infractions commises sur un réseau de communications électroniques. Cette précision peut sembler superflue, mais découle de la structure de la punissabilité telle que le projet la propose. Celle-ci est telle que des exceptions (réseaux de communications électroniques ; droit pénal des médias) aux règles générales sont établies. La réglementation proposée est structurée *sur trois niveaux de hiérarchie* :

- les règles générales sont fondamentalement applicables ;
- une réserve par rapport à ces règles générales est faite si les infractions sont commises sur un réseau de communications électroniques ;
- par rapport aux règles établies à l'art. 27 (nouveau) CP, l'art. 27 (nouveau), ch. 2 CP établit encore une autre réserve en faveur du droit pénal des médias actuel, néanmoins uniquement pour les auteurs et les rédacteurs.

Cette structure à trois niveaux a été choisie *d'une part* parce que les faits à réglementer (cybercriminalité) rappellent fortement, de par leur structure, les délits de média (participation nécessaire d'un grand nombre d'acteurs), mais *d'autre part* parce que les états de faits déjà pris en considération par le droit pénal des médias peuvent aussi être produits sur des réseaux de communications électroniques (par

---

[218] Cf. la définition légale de l'art. 3, let. a LTC: « informations: les signes, signaux, caractères d'écriture, images, sons et représentations de tout autre type destinés aux êtres humains, aux autres êtres vivants ou aux machines; »

[219] Par ex. représentations de la violence, art. 135, pornographie, art. 197, discrimination raciale, art. 261bis CP.

[220] Par ex. mise à disposition de virus informatiques, art. 144bis CP; offres frauduleuses sur la Toile, art. 146 CP.

[221] Par ex. la piraterie musicale, art. 67 et 69 LDA.

ex. publication en ligne d'un quotidien) ; les deux domaines se recoupent donc. Une hiérarchie de règlement à trois niveaux permet d'englober tous les états de fait pratiquement sans renvoi d'une norme à l'autre.

9.23 Art. 27 (nouveau), ch. 2 CP (délimitation par rapport au droit pénal des médias)

9.231 Renvoi au droit pénal des médias uniquement pour les auteurs et rédacteurs

L'art. 27 (nouveau), ch. 2 CP établit une réserve en faveur du droit pénal des médias, plus précisément de l'art. 27bis CP (nouveau). Etant donné que des états de fait, régis par le droit pénal des médias classique, peuvent selon leur utilisation (par ex. publication en ligne d'un quotidien) relever aussi des infractions commises sur les réseaux de communications électroniques, il convient de réserver l'application du droit pénal des médias, récemment modifié. Le but de cette réserve, donc de l'art. (nouveau) 27, ch. 2 CP, est de garantir que le droit pénal des médias ne soit pas éludé.

Néanmoins, la réserve ne mentionne que les *auteurs* et *rédacteurs*. Elle exclut donc la « personne responsable de la publication en cause » dont la réglementation actuelle tient compte à l'art. 27, al. 2 CP. Pour la raison suivante : dans le cas des infractions commises au travers de procédés automatisés sur les réseaux de communications électroniques, ce groupe de personnes justement - donc les responsables de la publication à l'exception des auteurs et rédacteurs - doivent tomber sous le coup de la nouvelle réglementation. Par contre, les autres membres de la rédaction et le personnel auxiliaire technique (par ex. les cameramen, les porteurs de câbles, etc.) demeurent soumis au droit pénal des médias en vertu de l'art. 27bis (nouveau) CP parce qu'ils sont totalement étrangers à toute transmission, mise à disposition et préparation automatisée des informations. Le texte de l'art. 27 (nouveau), ch. 2 CP ne suggère pas non plus d'interprétation divergente ; il n'est notamment pas question de « leur » punissabilité.

Si la réserve de l'art. 27 (nouveau), ch. 2 CP visait également ce groupe de personnes, les réglementations de l'art. 27 (nouveau), ch. 3 et 4 CP ne pourraient prétendre à une validité générale. Dans ce cas, il conviendrait de déterminer, à l'intersection entre droit pénal des médias et réseaux de communications électroniques, s'il s'agit d'un délit de média - ce qui mènerait à une application du droit pénal des médias - ou d'un délit « usuel », ce qui mènerait à l'application de la réglementation de l'art. 27 (nouveau), ch. 3 et 4 CP.

La restriction aux auteurs et rédacteurs de la réserve en faveur du droit pénal des médias garantit par contre à ces derniers que l'introduction des nouvelles dispositions n'impliquera pour eux aucune modification ; par contre, des réglementations spécifiques sont établies pour les fournisseurs d'accès et fournisseurs d'hébergement. Ces deux groupes ne sont donc plus menacés d'une éventuelle punissabilité selon l'actuel art. 322bis CP (dans le nouvel ordre des paragraphes : art. 322bis, ch. 2 CP); désormais, les fournisseurs d'hébergement sont soumis à la nouvelle réglementation de l'art. 322bis (nouveau), ch. 1 CP, alors que la

connexion automatique que permettent les fournisseurs d'accès demeure non punissable conformément à l'art. 27 (nouveau), ch. 4 CP.

La nouvelle réglementation proposée pour les fournisseurs d'hébergement va, d'une part, un peu moins loin que l'actuelle puisque l'action par négligence n'est plus prise en compte, toutefois, d'autre part, elle est considérablement plus sévère parce que la responsabilité pénale intervient indépendamment du fait qu'un auteur ou un rédacteur puisse être rendu responsable de la publication [222].

9.24 Art. 27 (nouveau), ch. 3 CP (fournisseurs d'hébergement, moteurs de recherche)

9.241 Informations d'autrui

La réglementation de l'art. 27 (nouveau), ch. 3, 1ère phrase, CP restreint son champ d'application aux « informations d'autrui » puisque la mise à disposition de ses *propres* informations, même si elle est automatisée, ne devrait pas être couverte par la disposition spéciale que représente l'art. 27 (nouveau), ch. 3 CP.

L'information est *d'autrui* lorsque l'auteur ne l'a ni créée, ni ne se l'est appropriée (par ex. en la sélectionnant, la modifiant ou la constituant sciemment) de sorte que même des informations appartenant à l'origine à autrui sont à qualifier d'informations propres si ces actions ont eu lieu. Une réglementation spéciale est prévue pour les moteurs de recherche qui, s'ils sont automatisés, constituent intrinsèquement des constitutions d'informations (voir à ce propos ci-dessous ch. 9.244).

Si l'auteur met à disposition des informations qui lui sont *propres*, on ne peut plus le qualifier de simple fournisseur d'hébergement ; en effet, dans ce cas, il est désormais soumis aux règles générales applicables aux auteurs d'infractions en vertu de l'art. 27 (nouveau), ch. 1 CP, éventuellement comme auteur ou rédacteur conformément au droit pénal des médias (art. 27bis (nouveau), ch. 2 CP).

9.242 « Mettre à disposition selon un procédé automatisé »

La formulation « mettre à disposition selon un procédé automatisé » désigne - en relation avec le fait que les informations mises à disposition sont des d'informations d'autrui - pour l'essentiel ce que recouvre actuellement la notion d' « *hébergement* ». Lorsque l'hébergeur met à disposition des informations d'autrui, il est essentiel que cette mise à disposition soit *automatisée*.

Le fournisseur d'hébergement fournit à ses clients, sur de gros ordinateurs, un certain espace de mémoire que le client peut utiliser. Une fois le droit d'accès à la capacité de mémoire accordé au client, celui-ci peut l'utiliser sans que le fournisseur d'hébergement ait quoi que ce soit d'autre à faire. Les informations que le client charge sur son espace mémoire peuvent être interrogées à partir d'une adresse propre. Héberger pourrait être comparé à la location d'un appartement : une fois les clés remises, le locataire peut faire usage des locaux.

[222] Cf. ci-dessus chapitre 6.

Le critère de l'automatisation différencie aussi sensiblement la mise à disposition d'informations par rapport à d'autres circonstances. Certes, la mise à disposition d'information est nécessaire pour que l'auteur puisse permettre l'accès publicà ses informations. Mais du fait qu'il utilise la capacité de mémoire sur la base d'un procédé automatisé (donc de manière analogue à un appartement ou un local professionnel) - c'est-à-dire charge, efface, modifie, etc. des informations - le fournisseur d'hébergement ne sait en général absolument pas ce que le gros ordinateur en question héberge. Il ne peut en avoir connaissance que si son attention est attirée délibérément sur une information par un tiers ou s'il effectue lui-même des contrôles à titre préventif (par analogie avec le locataire : si le propriétaire inspecte régulièrement les locaux loués).

9.243 Renvoi à l'art. (nouveau) 322bis, ch. 1

En proposant l'introduction d'une norme pénale distincte dans la Partie spéciale du code pénal, la commission d'experts suit le modèle de réglementation déjà adopté pour la punissabilité des responsables de médias à l'art. (nouveau) 322bis, ch. 2 CP [223].

9.244 Répertoire intégrant des informations d'autrui selon un procédé utomatisé (moteurs de recherche), art. 27 (nouveau), ch. 3, 2ème phrase

Beaucoup d'utilisateurs commencent leurs recherches sur la Toile en recourant aux services d'un *moteur de recherche* (par ex. google.com, hotbot.com, altavista.com). Un moteur de recherche est un serveur web (ordinateur fournissant des pages web par Internet) permettant une interrogation par mots-clés dans une banque de données ; cette banque de données saisit les informations automatisées offertes (textes, images, musique, œuvres multimédia, etc.) et les raccorde par hyperlien (lien permettant de passer d'un document à l'autre). Les programmes Spider et Cawler passent toute la Toile en revue, constituent un index des nouveaux sites par mot-clé et les déposent, accompagnés des hyperliens nécessaires, dans la banque de données du moteur de recherche. L'exploitant du moteur de recherche n'intervient pas puisque ces procédés sont automatisés. Mais il met l'index à la disposition des utilisateurs en offrant des renvois de liens sur son serveur.

Du point de vue du droit pénal, l'art. 27 (nouveau), ch. 3 CP met désormais les exploitants de ces moteurs de recherche sur un pied d'égalité avec les *fournisseurs d'hébergement*. Ce complément est nécessaire car les informations que contient l'index du moteur de recherche [224] ne sont plus d'autrui. Ce n'est pas un quelconque fournisseur de contenus qui met ses informations à disposition sur le serveur de l'exploitant du moteur de recherche, mais l'exploitant du moteur de recherche lui-même qui établit une banque de données selon un procédé automatisé. Ce qui se trouve dans l'index constitue un contenu propre et devrait en conséquence être apprécié à la lumière de l'art. (nouveau) 27, ch. 1 CP.

Exemple : une interrogation à partir des mots-clés « politicien X » et « petit con » mène à une liste d'objets sélectionnés. L'un d'entre eux, à côté de l'hyperlien menant au contenu d'autrui, contient la phrase suivante : « Car cet individu qui circule dans

[223] A propos des conditions de la punissabilité conformément à cette disposition, cf. ci-dessous 9.3.

[224] Qui ne sont donc pas les informations en lien sur de gros ordinateurs externes.

une grosse BMW n'est pas un misérable petit con quelconque, c'est l'homme politique bien connu et coureur de jupons X, de Y ».

Ces propos attentatoires à l'honneur peuvent être interprétés comme comportement punissable de l'exploitant du moteur de recherche car il les a intégrés librement dans son répertoire. Ne serait-ce qu'à cause de l'hyperlien qui mène à des sites d'autrui, on peut admettre - selon la définition des normes pénales de la Partie spéciale du CP- une punissabilité de la personne ayant établi le lien (en qualité d'auteur principal autonome de l'infraction ou en tant que complice) [225]. De même, on peut inférer une punissabilité lorsque l'exploitant d'un moteur de recherche indexe automatiquement des images qui sont stockées dans son répertoire comme petits fichiers-image (voir par ex. http://images.google.de).

Malgré ces différences quant à la fonction du fournisseur d'hébergement et celle de l'exploitant de moteur de recherche, il semble indoiqués de *traiter ces deux acteurs sur le même pied*. L'exploitant d'un moteur de recherche entretient aussi une infrastructure socialement adéquate et même socialement souhaitée. La recherche et l'indexation sur Internet - tout comme pour le fournisseur d'hébergement - fonctionnent selon des procédés automatisés. Si la punissabilité était définie d'après les règles générales, des problèmes déjà connus referaient surface : on pourrait soumettre l'exploitant d'un moteur de recherche à l'obligation de vérifier les informations indexéesm, obligation dont la violation entraînerait une punissabilité pour omission. En définitive, une telle obligation entraverait l'exploitation efficace des moteurs de recherche.

La nouvelle réglementation proposée vise une définition claire des limites de la punissabilité des exploitants de moteurs de recherche. Sachant avec certitude que des informations pénalement répréhensibles se trouvent sur son répertoire électronique, il devra en empêcher l'accès, tout comme le fournisseur d'hébergement. De plus, averti de la présence de ce genre d'informations, il a l'obligation d'en informer les autorités de poursuite pénales (cf. pour plus de détails le commentaire de l'art. 322bis (nouveau), ch. 1 CP). S'il respecte cette obligation, son activité demeure impunie.

Par contre, les fournisseurs de listes de liens sélectionnées et constituées de manière *non* automatisée telles que les fameux répertoires web de Yahoo ou de Google (www.yahoo.com ou http://directory.google.co, entre autres) ne bénéficient pas de cette limitation de la punissabilité. Lorsque les collaborateurs d'un prestataire de services introduisent dans un but précis des contenus dans un répertoire, cet acte est intentionnel ou, pour le moins sous-tendu par un dol éventuel. Ce genre de comportement ne doit pas bénéficier d'un traitement spécial. Il en va de même pour la personne qui renvoie sciemment par hyperlien à des informations d'autrui qui réunissent les éléments constitutifs d'une infraction sanctionnés par une norme pénale. Il convient donc dans ces deux cas d'appliquer les règles générales.

[225] Pour plus de détails, cf. CHRISTIAN SCHWARZENEGGER/MARCEL ALEXANDER NIGGLI, Über die Strafbarkeit des Hyperlink-Setzers. Zum Urteil des Bezirksgerichts Zürichs vom 10. September 2002. medialex 2003, p. 27 ss.

9.25 Art. 27 (nouveau), ch. 4 CP (fournisseurs d'accès, bref stockage intermédiaire)

9.251 Motifs de l'impunissabilité en cas de simple transmission d'accès sur les réseaux de communications électroniques

Ainsi que nous l'avons mentionné au chapitre 6 (voir ch. 6.2 et 6.3 in fine), l'application des règles générales du CP n'exclut pas que le fournisseur d'accès soit considéré comme complice à l'infraction principale. Il en va de même du domaine spécial des délits de média lorsqu'on considère le fournisseur d'accès comme une personne responsable de la publication au sens de l'actuel art. 27, al. 2 CP. Tant en Suisse qu'à l'étranger, la doctrine a adopté le point de vue selon lequel la transmission et la fourniture d'accès automatisées ne peuvent être punissables 226. Cette conception repose sur *diverses considérations* :

- Si l'on examine de plus près le rôle principal du fournisseur d'accès, on note que son activité essentielle consiste à « *assister » son client*, l'utilisateur. Celui-ci utilise les différents services Internet à des fins de communication ou de collecte d'informations et a besoin, pour ce faire, d'un accès au réseau. Cela dit, le soutien actif du fournisseur d'accès dans l'établissement d'un accès momentané ne constitue pas un comportement pénalement répréhensible car en elle-même, l'action de l'utilisateur n'est pas punissable, même lorsque l'utilisateur consulte des sites sur lesquels des informations répréhensibles ont été chargées.

- Par contre, le fournisseur d'accès remplit une simple fonction indirecte dans la mise à disposition d'informations illégales par le fournisseur de contenus. Dans le cas par exemple de la diffusion de doctrines prônant la discrimination raciale, il faut - suivant le flux d'informations - considérer comme premiers auxiliaires le fournisseur d'accès *du fournisseur de contenus* et son fournisseur d'hébergement. Viendrait ensuite le fournisseur de réseau qui assure la liaison entre fournisseur d'hébergement et Internet. Les auxiliaires ultérieurs seraient les exploitants des routeurs ou des *gateways* (passerelles), puis en dernière position à nouveau les fournisseurs locaux de réseaux. Cf le diagramme du ch. 2.31, à propos des différents types de fournisseurs.

  Ce n'est qu'au terme de ce long cheminement qu'il convient de situer l'assistance apportée à la diffusion des informations du fournisseur de contenus par le fournisseur d'accès *de l'utilisateur*. Avant de considérer la punissabilité de ce dernier, il faudrait prouver celle des participants situés en amont dans la chaîne de la complicité. Néanmoins, la question n'est même pas soulevée parce que la contribution de ces participants est tout naturellement considérée comme *socialement adéquate*.

- Ces considérations reposent en outre sur une condition : l'action du fournisseur de contenus doit être encore en cours, donc n'être ni accomplie ni achevée. La question qui se pose ici est celle de la durée des différents délits d'expression et de diffusion car le soutien actif à l'infraction principale n'est, en général, possible qu'*avant* son accomplissement ou son achèvement. Si l'on admet - comme pour

226 Voir uniquement art. 12 de la directive européenne sur le commerce électronique.

les délits de mise en danger abstraite par définition (cf. tableau figurant au chapitre 6, ch. 6.2) - que le délit d'expression est déjà accompli et achevé au moment de la première mise à disposition par le fournisseur de contenus, toute fourniture d'accès ultérieure ne pourrait plus être taxée de complicité. En pareil cas, une punissabilité du fournisseur d'accès ne serait absolument pas envisageable.

- Etant donné que l'on ne peut rattacher aucun comportement actif du fournisseur d'accès à la mise à disposition d'informations illégales par le fournisseur de contenus, il faudrait fonder l'attribution de la responsabilité pénale sur l'omission des mesures techniques de blocage. Si l'on reconnaît qu'il peut y avoir complicité par omission, il faudrait pouvoir établir que le fournisseur d'accès a une *responsabilité de garant*.

  Du fait que le comportement préalable du fournisseur d'accès n'est ni contraire à ses devoirs ni spécifiquement facteur d'augmentation du danger, une responsabilité en raison de l'ingérence n'entre pas en ligne de compte. Pas plus qu'on ne peut établir à propos du fournisseur d'accès une responsabilité à raison du contrôle sur une source de dangers car, sinon, toute l'infrastructure d'Internet devrait être considérée comme foyer de dangers dont un fournisseur d'accès serait toujours responsable.

- Les mesures de blocage souvent requises à l'encontre des fournisseurs d'accès n'ont au fond rien à voir avec la poursuite pénale. Elles relèvent du domaine juridique administratif de la sécurité (cf. ci-dessus chapitre 7). Pour qu'une punissabilité pour complicité de diffusion puisse naître, il faudrait prouver en l'espèce qu'une transmission concrète des données a eu lieu directement au travers de l'infrastructure du fournisseur d'accès en question. Or les mesures de blocage visent un tout autre but, à savoir la prévention. Les clients d'un fournisseur d'accès ne doivent (plus) avoir accès aux informations incriminées. Du fait de l'absence de contribution concrète à l'encouragement du fournisseur d'accès, il n'y donc pas non plus de condition objective de punissabilité pour participation.

- De même, le champ d'application du droit pénal des médias est, dans la majorité des cas, compris en ce sens que le fournisseur d'accès ne doit pas être compté parmi les personnes responsables d'une publication (cf. ci-dessus 6.2),de sorte qu'il ne peut en découler une punissabilité en vertu de l'art. 322bis CP.

Ces arguments s'opposent clairement à la responsabilité pénale du fournisseur d'accès. C'est également la norme légale qui a été choisie par l'Union européenne, les Etats-Unis ainsi que par d'autres pays, ainsi que dans la recommandation du Comité des ministres du Conseil de l'Europe. Etant donné la place qu'on pris les réseaux de communications électroniques dans la société moderne de l'information, il s'impose de fixer de manière explicite dans le code pénal l'impunissabilité de l'accès automatisé sur les réseaux de communications électroniques. Tel est le but de l'art. 27 (nouveau), ch. 4 CP.

9.252 Remarques concernant la formulation de l'art. 27 (nouveau), ch. 4, phrase 1 CP

Une *définition de la fourniture d'accès* est donnée plus haut, au ch. 2.314.

Cette disposition ne s'applique qu'à la personne qui permet *exclusivement* l'accès à Internet. Par contre, si un fournisseur d'accès s'associe activement à la préparation ou à la mise à disposition d'informations illégales, par exemple en participant aux infractions du fournisseur de contenus en qualité de coauteur, d'instigateur ou de complice, ou même s'il s'agit de ses propres informations, il tombe sous le coup de l'art. 27 (nouveau), ch. 1 CP (punissabilité conformément aux règles générales). L'impunissabilité ne dépend donc pas d'un statut, mais du rôle concret que joue le fournisseur d'accès dans chaque processus de communication.

On rencontre dans diverses normes l'impunissabilité telle que la prévoit l'art. (nouveau) 27, ch. 4 CP. Parfois, on trouve l'expression «n'est pas puni » « n'est pas punissable » » 227, parfois « exempté de peine » 228, ce qui nécessite presque toujours une justification. Prenons par exemple l'art. 32 CP, 2e partie de la phrase : « Ne constitue pas une infraction … l'acte que la loi déclare permis ou non punissable ». 229 La formulation choisie (« non punissable ») est préférable car elle implique la qualification sur le plan de la dogmatique pénale en tant qu'exclusion de l'infraction.

9.253 Stockage automatique et temporaire d'informations d'autrui, art. 27 (nouveau), ch. 4, phrase 2 CP

Conformément à cette disposition, le stockage automatique, temporaire et intermédiaire d'informations d'autrui doit être compris comme fourniture d'accès au sens de l'art. 27, ch. 4, phrase 1 CP s'il résulte de la consultation de données par un utilisateur. Contrairement à la directive européenne 230, la réglementation proposée ici ne fait pas de distinction entre le stockage intermédiaire exigé par des impératifs techniques durant un transport spécifique de données et la forme de stockage dite « *caching* » (stockage automatique intermédiaire). Le *caching* correspond aussi à un stockage intermédiaire temporaire opéré par le fournisseur d'accès. Néanmoins, il ne sert pas à un seul et unique transport 231 de données, mais permet de rationaliser l'interrogation de données pour tous les clients du fournisseur d'accès s'agissant de contenus souvent consultés.

---

227 Par ex. à l'art. 100 ch. 4 LCR (Conditions de la répression); art. 53 loi fédérale sur la navigation intérieure [RS 747.201] (Courses officielles urgentes); art. 19b LStup (« Celui qui se borne à préparer pour lui-même la consommation de stupéfiants ou à permettre à des tiers d'en consommer simultanément en commun après leur en avoir fourni gratuitement, n'est pas punissable s'il s'agit de quantités minimes »).

228 Notamment en accompagnement des motifs justificatifs (par ex. à l'art. 33, al. 2, phrase 2; art. 34, ch. 1 et ch. 2; art. 119, Interruption non punissable de la grossesse; art. 260bis, al. 2 CP).

229 Quant à la portée de ce terme, voir TRECHSEL (Bibl.), art. 33, n. 17: « … so bleibt er «straflos», was prozessual einen *Freispruch* bedeutet, ATF 73 IV 261, 101 IV 121. »

230 Art. 12, al. 2 et art. 13 de la directive européenne sur le commerce électronique.

231 Par ex. le stockage intermédiaire d'un message électronique adressé à un utilisateur déterminé sur le serveur de courrier électronique du fournisseur d'accès.

Des processus programmés assurent un stockage intermédiaire, adapté au comportement de l'utilisateur des sites web les plus visités sur un serveur *proxy* du fournisseur d'accès. Ils demeurent à disposition sur ce serveur pendant un certain temps, mais ressortent automatiquement de la mémoire lorsqu'ils sont obsolètes ou ne sont plus consultés. Les deux variantes peuvent être rangées sous la notion de stockage automatique et temporaire d'informations d'autrui ; il appartient à la jurisprudence d'établir la délimitation entre stockage intermédiaire temporaire et la mise à disposition plus longue d'informations.

Cette *solution flexible* est préférable à une réglementation explicite car une délimitation sous forme généralement abstraite est pratiquement vouée à l'échec dans un environnement technique en constante mutation. Ainsi, en Allemagne, malgré un texte de loi explicite, l'incertitude règne encore sur le temps maximum qu'il convient d'accorder à un stockage intermédiaire, ou sur la nature des « standards de l'industrie largement reconnus et utilisés » (cf. § 10 TDG nouvelle version) dans le p*roxy caching*. Au demeurant, l'utilisation des serveurs proxy a entre-temps fortement reculé en raison de l'accroissement des capacités de transmission des informations.

Le « mode mirroir » (*mirroring*) ne figure pas dans la réglementation proposée. Donc si un prestataire, par le fait d'un comportement actif, copie de manière identique 232 un certain contenu Internet sur un autre serveur - par ex. afin de raccourcir les intervalles d'accès à un serveur particulièrement éloigné et particulièrement encombré -, il devient fournisseur de contenus au sens de l'art. 27 (nouveau), ch. 1 CP. Dans ce cas, il ne s'agit justement pas d'un stockage intermédiaire automatique résultant de la consultation d'un utilisateur, mais d'une opération de stockage résultant d'une *sélection intentionnelle*.

Par contre, si une conversion en mode miroir se fait automatiquement, la personne qui en est à l'origine est soumise à la responsabilité en vertu de l'art. 27 (nouveau), ch. 3 CP. Ce point est particulièrement important dans le domaine des forums de discussion souvent automatisés et réenregistrés tels quels sur le serveur local du forum.

9.3 Commentaire relatif à l'art. 322bis (nouveau) ch. 1

9.31 Alinéa 1

9.311 En général

L'al. 1 régit la *punissabilité du fournisseur d'hébergement*, à savoir de celui qui met à la disposition de son client, le fournisseur de contenus, un serveur Internet sur lequel ce client peut offrir ses propres données [233]. D'ordinaire, le fournisseur

[232] Comme un miroir qui reflète exactement la même image.

[233] On entend ici, et plus loin aussi, par « propres données » les fichiers consultables sur Internet. Il s'agit essentiellement de sites web (mais aussi de données consultables par le biais d'autres services Internet, par ex. FTP).

d'hébergement ne participe pas à l'enregistrement des informations sur les sites web bien que cela se passe sur son serveur Internet. En effet, il s'agit là de programmes automatiques que seul le fournisseur de contenus déclenche et contrôle.

En soi, c'est sur cette base technique qu'il conviendrait d'apprécier la punissabilité du fournisseur d'hébergement en vertu des règles générales. Lorsque, par exemple, un fournisseur de contenus met à disposition sur son site du matériel de pornographie enfantine ou fait des offres frauduleuses, la question est de savoir si le fournisseur d'hébergement y participe sous l'une des formes sanctionnées par le droit pénal. Il est difficile de donner ici une réponse claire, et cela à divers égards. En premier lieu, il convient d'examiner s'il y a comportement actif. Le contrat que le fournisseur d'hébergement passe avec le fournisseur de contenus (dans lequel on pourrait voir un comportement actif) constitue *en quelque sorte un contrat en blanc* quant aux données que le fournisseur de contenus chargera plus tard sur le serveur Internet du fournisseur d'hébergement : ce contrat porte uniquement sur l'obligation, pour le fournisseur d'hébergement, de mettre à la disposition du client (le fournisseur de contenus) une certaine capacité de mémoire sur le serveur Internet et de créer les conditions nécessaires pour que le client puisse mettre en ligne les contenus sélectionnés par lui et leur donner la forme qu'il entend leur donner. De son côté, le client doit rémunérer cette prestation de services. Les contenus eux-mêmes ne font pas l'objet du contrat, à l'exception d'une éventuelle clause selon laquelle il est interdit de mettre en ligne des contenus illégaux. On ne peut donc pas rattacher une responsabilité pénale à la conclusion du contrat.

Une fois que le fournisseur de contenus a chargé ses contenus, la *contribution du fournisseur d'hébergement* se borne à l'exploitation du serveur Internet dont il a loué la capacité de mémoire à son client. La présence d'un comportement actif est, dans ce cas, contestable [234]. En outre, la détermination précise de la contribution du fournisseur d'hébergement dépend de manière décisive de la manière dont l'acte est décrit dans les éléments constitutifs (que le fournisseur de contenus réalise en tant qu'auteur de l'acte en question). La distinction entre « faire » et « omettre » est particulièrement floue précisément face à des actes qui consistent à « laisser à disposition » et notamment à « rendre accessible » (art. 135, 197, ch. 3 CP). Même s'il est permis d'admettre un comportement actif dans un cas d'espèce, il faudra continuer à apprécier cette contribution d'après son caractère d'acte relevant de l'auteur ou seulement du complice.

Sur ce point également, les résultats ne sont pas concluants, d'autant plus qu'entre ici en jeu le problème de la *complicité au travers des actes quotidiens* : dans une large mesure, ces actes gomment la différenciation traditionnelle entre le mode de perpétration de l'infraction en qualité d'auteur et le mode de perpétration en qualité de complice, et cela en faveur du premier. Ce qui pousserait souvent à admettre une responsabilité comme co-auteur, solution en définitive peu adéquate.

Au surplus, en considérant le fournisseur d'hébergement comme auteur de l'infraction, on laisse de côté la question de savoir si l'on peut se rendre (aussi) punissable pénalement comme complice par la prestation de services quotidiens dans la mesure où ceux-ci requièrent une action principale intentionnelle. Dans sa

[234] Cf. les renvois ci-dessus, ch. 6.3.

jurisprudence, le Tribunal fédéral a répondu jusqu'ici par l'affirmative, mais en ne donnant que des réponses au cas par cas et non générales, donc sans répondre de manière définitive à la question [235]. Qualifier d'acte principal la contribution du fournisseur d'hébergement à l'action donnée tire un trait sur la question. Certes, la situation s'en trouverait clarifiée, mais l'exposé objectif de la question en serait réduit de sorte que ce genre de solution doit être écarté pour cette même raison. Par contre, classifier la prestation du fournisseur d'hébergement comme complicité soulève la délicate question de la complicité au travers des activités usuelles (voir à ce sujet ch. 6.3).

Si le comportement actif est écarté, la question se pose de savoir si le fournisseur d'hébergement pourrait être frappé d'une peine pour omission au même titre que s'il avait commis l'infraction. Dans ce domaine également, il est difficile de parvenir à une solution juste et adéquate. Selon la doctrine et la jurisprudence, une *position de garant* (responsabilité) peut naître d'un comportement antérieur de mise en danger (ingérence). Celui qui met en danger de manière prévisible les biens juridiques de tiers par son comportement est tenu de tout entreprendre pour que ce danger ne se réalise pas dans une violation du droit. Le comportement du fournisseur d'hébergement consiste à mettre un espace de mémoire à la disposition de ses clients. C'est, là aussi, une action tout à fait quotidienne et en soit légale qui ne crée aucun danger particulier.

Le danger, ou l'infraction, résulte en premier lieu de *l'utilisation abusive de cette capacité de mémoire* par un tiers (le fournisseur de contenus) qui enfreint intentionnellement le droit en mettant en ligne des informations illicites. En agissant ainsi, il viole aussi le contrat passé avec le fournisseur d'hébergement car en général, les conditions générales du contrat interdisent l'offre d'informations illicites.

Le Tribunal fédéral pourrait contribuer à clarifier la question. Plusieurs années seraient nécessaires jusqu'à ce que les points pertinents soient portés devant le Tribunal fédéral. Au surplus, il n'est aucunement garanti que la plus haute instance judiciaire soit aussi effectivement saisie de ce sujet ; en fait, l'élément déterminant est ici la pratique des autorités de poursuite pénale (mise en accusation) que l'on ne peut prévoir. Un autre impondérable est la réaction des participants à la procédure aux jugements des tribunaux de première et de deuxième instance (utilisation des voies de droit).
Pour ces raisons, la commission d'experts a résolu de ne pas laisser à la pratique le soin de déterminer le degré de punissabilité du fournisseur d'hébergement, mais de *régler ce point dans une loi*, *en excluant les règles générales applicables à la qualité d'auteur de l'infraction et de participant*. On notera ici un parallèle avec le droit pénal des médias actuel dont la modification des règles générales est déjà légalement prévue (cf. art. 27, al. 2, 322bis CP). En outre, des problèmes similaires se posent dans un domaine connexe : les versions en ligne de médias imprimés doivent être soumises sur le fond au même régime que celui auquel les médias imprimés sont déjà sujets, cela, en tout cas, pour l'auteur et le rédacteur. Pour le reste, il convient néanmoins de relever que ce parallélisme a ses limites. La norme proposée n'est pas, à de nombreux égards, le pendant de l'art. 322bis CP pour les réseaux de communications électroniques :

[235] Cf. ci-dessus ch. 6.3.

- Elle a un *champ d'application plus large* car elle n'est pas seulement applicable aux délits de média au sens de la jurisprudence du Tribunal fédéral relative à l'art. 27 CP. Elle régit aussi les délits d'expression auxquels le Tribunal fédéral refuse la qualité de délits de média, comme par exemple les infractions prévues aux 135, 197, ch. 2 et 3 ou 261bis, al. 4 CP. Elle va en outre beaucoup plus loin que cette catégorie de délits auxquels on reconnaît la qualité de délits de média: toute infraction commise au travers des réseaux de communications électroniques tombe d'emblée sous le coup de l'art. 27 (nouveau) CP et de ce fait aussi sous le coup de l'art. (nouveau) 322bis, ch. 1 CP.

- Dans le droit pénal des médias, la responsabilité pénale du rédacteur responsable ou de la personne responsable de la publication est subordonnée à la condition que l'auteur ne puisse pas être découvert ou ne puisse pas être traduit en Suisse devant un tribunal. Cette exclusion de la punissabilité ne vaut pas pour les infractions commises au travers des réseaux de communications électroniques : même si l'auteur et/ou fournisseur de contenus peut être découvert ou traduit en Suisse devant un tribunal, *la punissabilité du fournisseur d'hébergement demeure possible en vertu de l'art. 322bis (nouveau), ch. 1 CP.*

- Le *rôle du rédacteur responsable* tel que le connaît l'art. 27, al. 2 CP et qui est couvert par l'art. 322, al. 2 CP (obligation de renseigner), n'existe pas obligatoirement dans le domaine des réseaux de communications électroniques. Mais lorsqu'il existe, la punissabilité du rédacteur responsable (comme celle de l'auteur) est déterminée par le droit pénal des médias (art. 27 (nouveau), ch. 2 CP).

- La *commission par négligence n'est pas punissable.*

9.312 En particulier

9.312.1 Systématique

Selon le nouveau concept et dans la mesure où elle est importante dans le présent contexte, la notion de réseaux de communications électroniques est prise dans *un sens plus large que celle de média*. Pour cette raison, la prescription relative aux infractions commises sur les réseaux de communications électroniques de l'art. 27 ss CP est placée tout au début de la réglementation (art. 27 (nouveau) CP) ; par voie de conséquence, l' « ancienne » norme du droit pénal des médias figure désormais à l'art. 27bis (nouveau) CP. La même permutation a lieu dans la norme pénale connexe de l'art. 322bis CP : le défaut d'opposition à une publication constituant une infraction, figurant à l'origine dans le seul paragraphe de cette disposition, passe au ch. 2, le ch. 1 réglant dorénavant le défaut d'opposition à l'utilisation d'informations « punissables » d'autrui sur les réseaux de communications électroniques.

9.312.2 Rapport avec la punissabilité du fournisseur de contenus

Considéré sous l'angle de son activité, le fournisseur de contenus correspond partiellement à *l'auteur* en droit pénal des médias, plus précisément s'il a lui-même

« la propriété intellectuelle » des données publiées par lui sur le serveur Internet de son fournisseur d'hébergement (textes, images, etc.). Si cette condition est remplie, sa punissabilité est régie par le droit pénal des médias (art. 27 (nouveau), ch. 2 CP); par conséquent, les règles d'exclusivité de cette disposition s'appliquent, mais selon la règle expresse de l'art. 27 (nouveau), ch. 2 CP, elles ne valent que pour l'auteur (et pour le rédacteur). Elles ne s'appliquent pas au fournisseur d'hébergement (qui, en tant que tel, n'est jamais auteur ou rédacteur, mais - transposé dans le domaine des médias - remplit éventuellement la fonction de la personne responsable de la publication). Dans ce cas, sa punissabilité est déterminée par l'art. 322bis (nouveau), ch. 1 CP.

Si le fournisseur de contenus n'est pas auteur, par exemple parce qu'il ne fait que reprendre des images de tiers (les faisant ainsi siennes), ou bien s'il est auteur, mais qu'il ne s'agit pas d'un délit de média au sens de l'actuel art. 27, al. 1 CP, les règles applicables sont les règles générales de l'art. 27 (nouveau), ch. 1 CP. Cela ne change rien pour le fournisseur d'hébergement : dans ce cas aussi, il est responsable en vertu de l'art. 322bis (nouveau), ch. 1 CP.

Dans le domaine des réseaux de communications électroniques, la responsabilité pénale du fournisseur d'hébergement n'est pas subordonnée à l'absence d'un responsable à titre principal. Cette absence de subordination résulte de la différence séparant la personne responsable de la publication et le fournisseur d'hébergement : alors que la première présente encore un lien avec les contenus publiés en ce sens qu'elle doit les surveiller et peut intervenir [236], ce n'est pas le cas du second : la mise en ligne des informations est le fait d'un procédé automatisé déclenché par le fournisseur de contenus et son fournisseur d'hébergement ignore tout de leur contenu. Par ailleurs, le classement en droit pénal des médias de la responsabilité est issu de la règle générale voulant qu'à l'intérieur d'une entreprise, lorsque l'auteur ou le rédacteur responsable fait défaut, c'est la personne responsable de la publication qui doit rendre des comptes. Cette condition n'est pas remplie non plus dans la relation fournisseur de contenus/fournisseur d'hébergement.

La légère modification de la réglementation par rapport au droit pénal des médias se traduit pour le fournisseur d'hébergement par un *renforcement des exigences* dans la mesure où la punissabilité d'un auteur ou d'un rédacteur ne lui procure pas obligatoirement l'exonération de punissabilité. Mais d'autre part, la nouvelle disposition implique pour lui un allègement car les fournisseurs d'hébergement ne tombent pas sous le coup de la responsabilité pour négligence prévue à l'art. 322bis, phrase 2 CP.

9.312.3 Auteurs de l'infraction

L'art. 322bis (nouveau), ch. 1 CP sanctionne un *délit véritablement spécial* : l'auteur de l'infraction ne peut être que la personne qui met à disposition, selon un procédé automatisé, des informations d'autrui sur un réseau de communications électroniques ; si tel n'est pas le cas, cette personne est d'emblée exclue du cercle des auteurs potentiels de l'infraction. Cette définition englobe les fournisseurs d'hébergement dont les clients (fournisseurs de contenus) utilisent les serveurs pour

[236] ATF 128 IV 53, 67 cons. 5c; ZELLER (Bibl.), n. 55

mettre en ligne des informations sans que les hébergeurs puissent avoir une quelconque influence. Ce procédé d'ordinaire automatisé dépend à tous égards (la forme et le contenu de l'information, sa modification ou sa suppression, le moment de la mise en ligne) uniquement du fournisseur de contenus. La disposition précise également qu'il s'agit d'informations *d'autrui*, c'est-à-dire d'informations qui, de par leur forme et leur contenu, n'émanent que du fournisseur de contenus. Si le fournisseur d'hébergement influe lui-même sur l'information, celle-ci devient sa propre information avec pour conséquence qu'il n'est plus soumis au régime de l'art. 322bis (nouveau), ch. 1 CP, mais à la réglementation de l'art. 27 (nouveau) ch. 1 CP.

Le libellé de la disposition précise dès le début ce qui qualifie l'auteur de l'infraction (à savoir, mettre des informations à disposition sur un réseau de communications électroniques) afin d'établir d'emblée clairement la catégorie potentielle à laquelle appartiennent les auteurs concernés. Le terme « automatisé » a été aussi repris ici pour que le libellé de la norme « première » de l'art. 27 (nouveau), ch. 3 CP, qui renvoie à l'art. 322bis, ch. 1 CP, et celui de la présente norme se recouvrent le plus possible.

Si le fournisseur d'hébergement est constitué en la forme de *personne morale*, la caractéristique spéciale ne concerne en premier lieu que la personne morale en tant que telle, mais pas les personnes physiques qui agissent en tant que responsables. La transmission de la position de l'obligé fondant la punissabilité aux personnes physiques agissantes avait en soi besoin d'une réglementation légale explicite telle que la connaît l'actuel CP (art. 172 CP) pour (et uniquement pour) les infractions du Titre deuxième (Infractions contre le patrimoine). Considérant la réglementation des rapports de représentation figurant dans la nouvelle Partie générale du CP, qui créent à l'art. 29 une telle norme applicable à toutes les infractions, la commission d'experts a toutefois décidé de ne pas opter pour une norme spéciale de ce type. Si l'entrée en vigueur de la nouvelle Partie générale devait être retardée, force serait de revoir cette décision.

9.312.4 Acte

L'art. 322bis (nouveau), ch. 1 CP consacre une punissabilité de l'*omission* : il est fait grief au fournisseur d'hébergement de ne pas être intervenu contre l'utilisation d'un fichier qui présente par exemple des propos racistes ou fait l'apologie de la violence. Cette intervention consisterait à *bloquer* l'accès au site (par contre, une injonction adressée au fournisseur de contenus de supprimer sur-le-champ les contenus n'entre pas en considération parce qu'elle pourrait renfermer une entrave à l'action pénale [art. 305 CP]). La disposition mentionne expressément que cette règle ne s'applique que si on peut *techniquement* et *raisonnablement l'exiger de lui*, une condition constituant une évidence reconnue [237] pour les délits d'omission, mais qui est répétée ici pour des raisons de clarté.

[237] Cf. KURT SEELMANN, in Niggli/Wiprächtiger, Basler Kommentar, n. 62, 92 ad art. 1; GÜNTER STRATENWERTH, Schweizerisches Strafrecht, Allgemeiner Teil I, 2^{e} édition, Berne 1996, § 14, n. 37.

9.312.5 Objet de la cessation du trouble

Celui-ci ne consiste pas à empêcher une infraction en tant que telle. Lorsque le fournisseur de contenus a mis en ligne un contenu constitutif d'une infraction, ce n'est pas en demandant au fournisseur d'hébergement de bloquer l'accès au fichier que l'on en finira avec l'acte en question. Cela ne vaut en tout cas pas pour les délits d'expression dont l'illicéité réside dans l'expression en tant que telle (voir les exemples déjà cités des art. 135 ou 261, mais aussi 173 ss, 197 ou 259 CP [Provocation publique au crime ou à la violence]). Il en va de même d'autres délits à cette différence près qu'ici, on peut imaginer que le blocage de l'accès empêche l'accomplissement du délit et que celui-ci n'en demeure qu'au stade de la tentative, par ex. lorsque l'accès à un site présentant des contenus relevant de la tromperie astucieuse est bloqué .

La violation du droit que le fournisseur de contenus a commise demeure. Mais les *effets* de cette infraction peuvent être limités par le blocage empêchant les utilisateurs d'Internet d'accéder au fichier. Peu importe que ces derniers se rendent, pour leur part, punissables parce qu'ils ont fait usage du fichier (ils ne sont en général pas encore punissables en raison du simple accès, mais ils le deviennent lorsqu'ils stockent ensuite les données en question, cf. art.197, ch. 3^{bis} CP). Ainsi, l'objectif *politico-juridique* visant à impliquer les fournisseurs d'hébergement dans la lutte contre les contenus illicites sur Internet est également atteint. On ne peut leur demander d'empêcher les infractions que leurs clients, à savoir les fournisseurs de contenus, commettent en publiant leurs fichiers sur le serveur des hébergeurs ; ceux-ci n'ont, en effet, aucune espèce d'influence sur le processus de mise en ligne des contenus concrets. Néanmoins, on peut très bien les exhorter - et c'est justement là le véritable objectif de la loi - à *limiter ces infractions dans leurs répercussions,* en rendant impossible la prise de connaissance des contenus en question.

Il s'agit d'une autre orientation des objectifs par rapport à la variante prônant la responsabilité des fournisseurs d'hébergement pour leur participation aux actes du fournisseur de contenus. Selon les règles générales déterminant la fonction d'auteur et de participant à une infraction, la question qui se pose s'agissant du fournisseur d'hébergement est toujours celle de savoir si et de quelle manière il participe au délit du fournisseur de contenus. *Dans la mesure où* il se rend punissable, sa punissabilité découle de l'illicéité que le fournisseur de contenus réalise. La norme proposée déplace le grief. Même du fait d'une omission éventuelle, ce n'est pas la participation au délit principal qui est au cœur même de l'illicéité causée, mais l'absence de réaction face à l'utilisation par des tiers de contenus illicites. L'illicéité de l'acte principal commis par le fournisseur de contenus constitue l'arrière-plan nécessaire pour que cette règle soit pertinente. Cette illicéité ne se concrétise que lorsque des tiers prennent connaissance de ces contenus, par exemple lisent des déclarations racistes ou regardent des représentations de la violence. Sous cet aspect, la solution préconisée maintient absolument le lien avec l'acte principal.

Ainsi, la nouvelle réglementation atteint deux objectifs en même temps : elle désamorce le débat autour de la prise en compte adéquate de la participation du fournisseur d'hébergement à l'acte principal du fournisseur de contenus, et lui ôte même sa portée pratique; en outre, elle circonscrit les effets de cet acte principal (cf. les exemples cités plus haut) sur les utilisateurs du contenu incriminé.

Cette modification de l'illicéité a donc *deux raisons principales* : l'impossibilité d'empêcher la commission de délits au travers d'Internet par le fournisseur de contenus ainsi que la possibilité, garantie par le droit pénal, d'empêcher l'utilisation des données illicites par des tiers.

S'ajoute à cela une *troisième raison importante*: les règles d'application des peines (art. 3 ss CP), selon lesquelles le fournisseur de contenus commet l'infraction là où il actionne la commande de stockage menant, selon un procédé automatisé, à la transmission des données incriminées vers le fournisseur d'hébergement. Si cet acte intervient à l'étranger, la Suisse n'a pas, selon la jurisprudence du Tribunal fédéral, la compétence de juger les participants ; le fournisseur d'hébergement est considéré comme l'un d'eux (la compétence juridictionnelle ne s'étend de toute façon pas au le fournisseur de contenus agissant à l'étranger en tant qu'auteur de l'infraction ; cf. ci-dessus ch. 6.43). La solution attribuant une responsabilité par omission au fournisseur d'hébergement dans la mesure où celui-ci a son siège en Suisse permet précisément d'éviter ce problème (s'il n'a pas son siège en Suisse, celle-ci n'a pas de compétence juridictionnelle même en vertu de la nouvelle réglementation proposée ici).

9.312.6 Devoir d'intervention du fournisseur d'hébergement

La disposition requiert qu'une infraction ait été commise au moyen d'informations d'autrui. Cette infraction, commise par le fournisseur de contenus, n'est pas limitée dans ses manifestations ; elle peut prendre les formes les plus diverses. D'un point de vue phénoménologique, on peut en distinguer *deux catégories* :

D'une part, les infractions qui ont donné naissance à cet appel en faveur d'une plus grande sévérité pénale à l'égard de la criminalité via Internet comme les représentations de la violence (art. 135 CP), la pornographie (art. 197 CP) ou la discrimination raciale (art. 261bis CP).

D'autre part, sont considérées comme infractions potentielles toutes les infractions pour la commission desquelles le recours à des moyens de communications électroniques est envisageable, par ex. donner des informations trompeuses en vue d'une escroquerie, proférer des menaces notables en vue d'un chantage ou encore proposer au public ou mettre en circulation, en violation du droit d'auteur, des exemplaires d'une œuvre (art. 67, al. 1, let. f, LDA) ou les exemplaires reproduits d'un phonogramme (art. 69, al. 1, let. f, LDA).

En l'occurence, le seul élément déterminant est que *les informations d'autrui* constituent *le moyen permettant de commettre l'infraction* (« par voie de »). Non seulement il n'est pas nécessaire que l'infraction soit consommée sous forme de publication, mais en outre elle peut requérir que d'autres conditions d'infraction soient remplies, par ex. celles d'un dommage patrimonial en cas d'escroquerie. Cela signifie que l'infraction telle que la présume l'art. (nouveau) 322bis, ch. 1, al. 1 CP ne doit pas être consommée au moment de la naissance de l'obligation d'agir du fournisseur d'hébergement, une tentative suffit.

Au demeurant, les informations doivent déjà constituer une partie des éléments constitutifs de l'infraction. Si tel n'est pas le cas - si elles servent par ex. uniquement

à la préparation d'une escroquerie -, il n'y a pas encore d'obligation d'intervenir. Ce n'est qu'à partir du moment où l'infraction est liée à l'utilisation d'un serveur internet que naît le devoir d'intervention du fournisseur d'hébergement. En effet, l'idée de la participation au délit commis au travers d'Internet constitue l'arrière-plan de cette réglementation. Si l'acte punissable n'est pas (encore) réalisé, la condition de l'art. 322bis (nouveau), ch. 1, al. 1 CP n'est pas remplie (ce qui a en même temps pour conséquence, eu égard à l'al. 2 de la nouvelle disposition, que les renseignements sur des actes non punissables ne doivent pas être transmis).

La limitation de l'applicabilité aux informations *d'autrui* est motivée par le fait que c'est uniquement dans ce cas spécifique qu'une réglementation spéciale pour le fournisseur d'hébergement se justifie. Les difficultés décrites plus haut de la prise en compte adéquate de sa participation à l'acte principal apparaissent uniquement à la condition qu'il n'ait rien à voir avec le contenu de l'information, donc que cette dernière lui soit étrangère. Par contre, s'il s'agit d'une information qui lui est propre, le fournisseur d'hébergement n'est justement plus fournisseur d'hébergement, mais fournisseur de contenus et tombe sous le coup de l'art. 27 (nouveau), ch. 1 CP.

On entend par *infraction* (uniquement) la réalisation d'un d'un acte contraire au droit et réunissant tous les éléments constitutifs de l'infraction. Que l'auteur de l'infraction (le fournisseur de contenus) agisse de façon coupable ne tire pas à conséquence. En effet, d'un point de vue pratique, on ne peut déceler au travers de l'information elle-même si elle émane d'un auteur (non) responsable. En outre, même en considérant le fournisseur d'hébergement comme participant, peu importerait qu'il agisse de façon coupable (accessoirité limitée). Enfin, l'exigence voulant empêcher dans toute la mesure du possible que l'utilisateur prenne connaissance de l'information incriminée dépasse la question de la responsabilité du fournisseur d'hébergement.

9.312.7 Eléments subjectifs de l'infraction

La nouvelle disposition requiert comme premier élément subjectif de l'infraction *l'intention* au sens de l'art. 18, al. 2 CP eu égard à toutes les circonstances objectives ; en principe, le dol éventuel en fait aussi partie. *Deux difficultés* en découlent dans la perspective de l'art. 322bis (nouveau), ch. 1, al. 1 CP :

- Dans la pratique, le dol est interprété dans ce sens qu'une personne a agi par dol éventuel dès que « *der Erfolg seines Verhaltens als so wahrscheinlich aufdrängte, dass sein Verhalten vernünftigerweise nur als Inkaufnahme dieses Erfolges ausgelegt werden kann* » [238]. Quoi que l'on pense de cette formulation, dans le domaine ici examiné de la punissabilité des fournisseurs d'hébergement, elle pourrait se traduire pour eux, au travers du dol éventuel, par l'imposition d'une obligation positive de contrôle :

  Si le fournisseur d'hébergement reçoit des avertissements soulignant la présence d'informations présumées illicites dans un fichier domicilié sur son serveur

[238] ATF 109 IV 140 « le résultat de son comportement s'imposait de manière si vraisemblable que son comportement ne peut être interprété autrement que comme l'acceptation de ce résultat ».

Internet et s'il ignore ces avertissements, se pose alors dans la procédure pénale ultérieure la question de son intention (les délits pertinents dans la pratique ne sont commis qu'intentionnellement), à condition qu'il s'agisse de manière effectivement objective d'une infraction. Selon la crédibilité de la personne à l'origine de l'avertissement et selon la fréquence avec laquelle elle a communiqué des renseignements de cet ordre (s'avérant en définitive justes), on ne peut éviter en l'espèce la conclusion que le comportement du fournisseur d'hébergement ne peut s'interpréter autrement que comme l'acceptation du fait qu'une infraction est commise au travers d'informations d'autrui sur son serveur Internet. Pour échapper au grief de dol éventuel, le fournisseur d'hébergement devrait donc, dans tous les cas, réagir aux avertissements crédibles et donnés avec insistance ; ce qui équivaut à lui imposer une obligation positive de contrôle.

Cela dit, il ne s'agit pas d'exonérer les fournisseurs d'hébergement d'une punissabilité qu'en soi ils mériteraient et de les placer injustement en position de privilégiés. Mais il faut souligner les *répercussions* qu'aurait une telle réglementation. Elle impliquerait la mise en place d'un système de contrôle afin de pouvoir se renseigner soi-même à propos d'avertissements reçus sur des fichiers présumés illicites. Cela ne suffirait encore pas à justifier la réglementation proposée.

Toutefois, si l'on réalise que les avertissments en eux-mêmes ne sont pas un gage de la crédibilité de leurs auteurs, et que la répétition opiniâtre d'un avertissement ne constitue pas un indicateur fiable de son exactitude, il devient clair que si l'on se contente du dol éventuel à propos de l'infraction, le système mène à l'absurde: dans les faits, le fournisseur d'hébergement devrait se renseigner sur *chaque* avertissement reçu. S'il en reçoit un grand nombre, les recherches à leur sujet nécessiteraient des ressources telles qu'on ne pourrait plus les qualifier de proportionnées étant donné le nombre largement supérieur d'utilisations légales d'Internet.

En outre, il est à craindre que les avertissments donnés soient exploités pour faire passer au plan pénal des litiges relevant purement du droit privé, phénomène typique, par exemple, en cas de violation de la LDA : un fournisseur d'hébergement recevant un avertissement serait obligé d'interdire l'utilisation d'un fichier hébergé sur son serveur et abritant des contenus présumés contraires à la LDA (sans constatation préalable par le juge). Ces considérations prendraient un poids encore plus grand si le dol éventuel était admis non seulement en présence d'avertissements donnés au fournisseur d'hébergement, mais encore en vertu du fait – de notoriété publique - que les prestations d'hébergement sont utilisées abusivement aussi pour commettre des infractions. Dans ces conditions, le fournisseur d'hébergement devrait contrôler préventivement les contenus stockés par ses clients pour pouvoir échapper à la punissabilité [239].

- La *seconde difficulté* réside dans la nature même de certains éléments constitutifs apparaissant souvent dans le contexte des réseaux de communications électroniques. Les représentations de la violence (art. 135 CP), la pornographie (art. 197 CP) ou la discrimination raciale (art. 261bis CP) incarnent

[239] Cf. NIGGLI/RIKLIN/STRATENWERTH, Die strafrechtliche Verantwortlichkeit von Internet-Providern, medialex, édition spéciale 1/2000, en part. p. 31 s.

des états de faits contenant des caractéristiques normatives. Leur contenu ne relève pas simplement d'un savoir préalable ordinaire généralement existant, mais requiert une appréciation.

Dans bien des cas, il n'est pas évident pour l'observateur de déterminer ce qu'est un acte de « cruauté », si sa représentation a « une valeur culturelle ou scientifique digne de protection », si elle porte « gravement » atteinte à la « dignité » humaine (art. 135 CP), ce qu'est un « écrit pornographique » au sens de l'art. 197 CP, si une idéologie vise à rabaisser « de façon systématique » une catégorie d'individus, ou encore si une personne est abaissée en raison de sa religion « d'une façon qui porte atteinte à la dignité humaine » (art. 261bis CP).

Néanmoins, un fournisseur d'hébergement prudent ne devrait pas attendre la confirmation du juge établissant par exemple la « cruauté » de l'acte de violence en question, mais bloquerait l'accès au fichier incriminé si, pour autant que l'on puisse en juger, le cas n'est pas à exclure avec certitude. Cette situation mène à une sorte de censure privée étrangère à une société démocratiquement constituée.

Pour ces motifs, le projet propose que la punissabilité du fournisseur d'hébergement soit restreinte aux cas « *dont il est sûr»* qu'ils *« constituent une infraction* » (libellé de la législation proposée)*,* en d'autres termes les cas dans lesquels le fournisseur d'hébergement a une *connaissance sûre du caractère punissable* du fichier contesté ; par contre, tous les autres cas de comportement intentionnel ne sont pas constitutifs de l'infraction. La portée première de cette limitation est d'exclure le dol éventuel comme fondement de la punissabilité ; il y a dol éventuel, lorsque l'auteur de l'infraction considère comme possible, mais sans le savoir avec certitude, que le contenu du fichier incriminé constitue une infraction bien déterminée. L'exclusion du « dessein éventuel » (une variante de l'intention directe) - qui a un lien plus éloigné avec la restriction à la connaissance sûre - ne devrait guère avoir de portée pratique ; lorsqu'il y a dessein éventuel, certes l'auteur envisage le résultat dommageable, mais il ne considère pas sa survenance comme sûre ; il la considère seulement comme possible [240].

En général, le simple avertissement qu'un fichier déterminé contient des données punissables pénalement ne suffit pas à fournir une connaissance sûre de la punissabilité de l'acte incriminé. Mais il peut arriver que le fournisseur d'hébergement ne reçoive pas seulement un avertissement à propos du fichier, mais le contenu même de ce fichier [241]. Si par exemple le caractère raciste de ce contenu saute aux yeux, il est évident que le fournisseur d'hébergement a, par-là, acquis la connaissance sûre qui fonde, en vertu de l'art. 322bis (nouveau), ch. 1, al. 1 CP, la punissabilité de l'acte en question (bien que le caractère manifeste de la punissabilité ne permette pas en soi de déduire l'avertissement est sûr).

---

[240] Cf. TRECHSEL/NOLL (Bibl.), p. 98.

[241] A cet égard, il ne relève pas du présent rapport de déterminer dans quelle mesure celui qui envoie au fournisseur d'hébergement le contenu même du fichier afin de le lui signaler se place lui-même en position de punissabilité (par ex. rendre accessible ou mettre à la disposition des représentations de pornographie dure, art. 197, ch. 3 CP). Dans un cas structurellement similaire, le Tribunal fédéral a dénié la qualité de comportement contraire au droit, sous mention du risque admissible, le transport de stupéfiants (art. 19, ch. 1, al. 3 LStup) à des fins (réalisées) de destruction.

Estimant que les avertissements émanant de particuliers quelconques étaient insuffisants, une *minorité parmi les membres de la commission d'experts* entendait lier l'acquisition de la « connaissance sûre » à la condition que le fournisseur d'hébergement reçoive un avertissement *émanant d'une source fiable* (par ex. des autorités de poursuite pénale). Ils estimaient, à l'appui de cette limitation supplémentaire, que le fournisseur d'hébergement ne devait pas être obligé d'apprécier lui-même l'illicéité d'un contenu. Leur argumentation était la suivante : les cas limites dans le domaine de la libre communication sont courants et le fournisseur d'hébergement ne saurait déterminer, au moment d'apprécier le cas, si un tribunal estime ultérieurement que l'illicéité du fichier était manifeste ; qu'un élément saute au yeux ou non dépend de l'optique dans laquelle se place l'observateur ; prudent, le prestataire bloquerait alors dans le doute l'accès au fichier incriminé par crainte de se rendre punissable. Ce qui mettrait les fournisseurs d'hébergement en grand danger de bloquer aussi des contenus conformes à la loi - comportement en contradiction avec le principe fondamental de la libre communication dans une société démocratique. Enfin, le fournisseur d'hébergement risquerait d'être attaqué civilement par le fournisseur de contenus pour un blocage se révélant ultérieurement inutile.
La *majorité des membres de la commission* n'a pas suivi cet avis. Elle s'est prononcée *contre une limitation supplémentaire de la punissabilité* pour les motifs suivants :

Tout d'abord, la responsabilité par rapport au cas normal du dol éventuel est déjà réduite par la nécessité de la « connaissance sûre » du caractère punissable de l'acte. *Deuxièmement*, la condition de la connaissance sûre permet d'assurer - si les cas de doute deviennent la règle – qu'un fournisseur d'hébergement ne soit pas confronté à la situation suivante : lorsque le caractère répréhensible du contenu d'une représentation semble objectivement douteux, il l'est en général aussi pour lui et, dans ce cas, l'hébergeur peut considérer la punissabilité de l'acte comme possible, mais non comme certaine ainsi que l'exigerait l'al. 1.

Troisièmement, la commission a estimé à la majorité qu'il n'était pas conforme de faire dépendre la « connaissance sûre » de la condition que l'information provienne d'une source fiable, par exemple d'une autorité de poursuite pénale. D'une part, parce qu'un avertissement émanant d'une telle autorité peut aussi être faux et que dans ce cas, la condition objective d'une « infraction » n'est pas remplie (ce qui exclue d'emblée une responsabilité pour acte réalisé). Si le fournisseur d'hébergement le remarque, il n'a alors (à bon droit) aucune connaissance sûre du caractère punissable. D'autre part, l'avertissement émanant d'un particulier peut aussi être à l'origine d'un « cas de connaissance sûre ». Si l'on considère l'information émanant d'une source fiable uniquement comme condition nécessaire, mais pas suffisante, à une connaissance sûre [242], il reste à savoir quelles autres conditions devraient être réunies.

Cette difficulté souligne - *quatrièmement* - que la notion d'«avertissement émanant d'une source fiable » - n'est pas compatible avec la nécessité de la connaissance sûre. Son point d'ancrage n'est pas la qualité de la connaissance du fournisseur d'hébergement, mais la *source* d'où émane l'information : le fait qu'elle vienne d'une

[242] En effet, de par son mandat, l'autorité de poursuite pénale est nécessairement tenue de se placer dans une perspective d'accusation, ce qui tend à se traduire par une limitation de la liberté de communication.

source fiable, par ex. d'une autorité de poursuite pénale, et non d'un particulier. Mais dans ce cas, à y regarder de près, il ne s'agit pas du tout d'un simple *avertissement* de cette autorité, mais d'une *ordonnance* de cette autorité.

La proposition de la minorité revient à pénaliser le fournisseur d'hébergement s'il ne donne pas suite à une ordonnance de blocage des autorités de poursuite pénale. Ce qui équivaut sur le fond à biffer l'art. 322bis (nouveau) ch. 1, al. 1 CP. En effet, l'inobservation d'une telle ordonnance est déjà punissable en vertu du droit actuel, et cela dans les conditions prévues à l'art. 292 CP.

Pour ces raisons, la *majorité de la commission* estime que la réglementation proposée est adéquate et que l'on peut raisonnablement exiger du fournisseur d'hébergement qu'il *assume sa propre responsabilité* dans la mesure décrite.

La limitation à la connaissance sûre ne porte que sur la condition de la punissabilité de l'acte en question (infraction = acte « punissable »). Le code pénal formule ce point dans d'autres articles par la tournure « wider besseres Wissen » (traduit par « sciemment », « connaissant la fausseté de ses allégations », « personne … qu'il savait innocente » aux art. 128bis, 174 et 303 s. CP) ou encore par « wissentlich » (« sciemment », « intentionnellement » [243]), de sorte que l'al. 1 serait ainsi libellé : « Celui qui aura mis à disposition, selon un procédé automatisé, sur un réseau de communications électroniques, des informations d'autrui au moyen desquelles une infraction est commise (art. 27, ch. 2) et aura négligé sciemment de … »

Jusqu'ici, les formes adverbiales susmentionnées n'ont pas causé de difficultés dans la pratique. En effet, il est évident qu'en ce qui concerne l'art. 174 CP (calomnie), par exemple, ce n'est pas le fait d'accuser une personne qui est en cause, mais celui de le faire "en connaissant la fausseté de ses allégations".[244]. Toutefois, à des fins de précision, la majorité des membres de la commission opte pour l'incise suivante (du reste absolument synonyme) « wie er sicher weiss/ dont il est sûr». Ainsi, il est également clair au plan linguistique que le point de référence de la « connaissance sûre » est uniquement la punissabilité de l'acte.

La *commission n'entend pas introduire la responsabilité pour négligence.* Cette dernière aurait pour effet de saper les bases mêmes de la réglementation qui, pour une part, vise à priver de toute pertinence le point, délicat au plan dogmatique, de savoir sous quelle forme le fournisseur d'hébergement participe à l'acte du fournisseur de contenus ; pour qu'il y ait participation, il faut que le délit ait été intentionnel, cela presque sans exceptions. S'ajoutent à cela les raisons pour lesquelles un dol éventuel du fournisseur d'hébergement ne saurait suffire du point de vue de la punissabilité de l'acte incriminé .L'option prise par la commission serait contrecarrée si l'on devait en même temps établir une responsabilité pour négligence.

Pour conclure, la différenciation est établie à partir du degré de participation automatisée : un rédacteur a l'information (illicite) devant lui de manière suivie et la

[243] Surtout dans les cas de délits de mise en danger, cf. art. 221, al. 2, 223, ch. 1, al. 1, 227, ch. 1, al. 1, 228, ch. 1, al. 4, 229, al. 1, 230, ch. 1, al. 3, 237, ch. 1, 238, al. 1 CP.

[244] Cf. GÜNTER STRATENWERTH, Schweizerisches Strafrecht, Besonderer Teil I I, 5^{E} édition, Berne 1995, § 11, n. 58.

connaît ou devrait pour le moins la connaître. Les deux conditions ne sont pas remplies dans le cas du fournisseur d'hébergement : il n'a pas l'information devant lui et il ne peut pas la connaître au moment de la mise en ligne, mais seulement lorsqu'on a attiré son attention sur cette information.

9.312.8 Sanctions

La nouvelle disposition menace de l'emprisonnement ou de l'amende et rejoint ainsi l'art. 322bis CP. La participation positive à l'infraction du fournisseur de contenus constituant l'arrière-plan de l'art. 322bis (nouveau), ch. 1, al. 1 CP, il convient de garantir que les sanctions dans les deux cas ne divergent pas démesurément. Un coup d'œil sur les délits dans lesquels la non-intervention du fournisseur d'hébergement pourrait mener à une punissabilité montre que cette concordance est pratiquement continue ; les art. 135, 197 et 261bis CP notamment menacent aussi d'une peine d'emprisonnement ou d'amende.

Dans les *cas d'exception* seulement qui, toutefois, sont négligeables au regard de l'ensemble, la limite supérieure de peine pour l'acte commis par le fournisseur de contenus est plus élevée, par ex. à l'art. 273 CP (Cas graves de service de renseignements économiques), alors que les art. 258 (Menaces alarmant la population) et 259 CP (Provocation publique au crime ou à la violence) prévoient comme limite supérieure la réclusion pour trois ans au plus à la place de l'emprisonnement (différence qui est supprimée par la révision du code pénal, voir art. 10).

Ce dispositif est également approprié dans la mesure où la limite inférieure de la sanction prévue (simple amende) à l'art. 322bis (nouveau) ch. 1, al. 1 CP est plus basse que celle qu'encourt le fournisseur de contenus (emprisonnement). En effet, le fournisseur d'hébergement n'est considéré que comme un complice et, dans ce cas, l'art. 25 en liaison avec l'art. 65, al. 5 CP autorise de prononcer, au lieu de l'emprisonnement, (les arrêts ou) l'amende.

9.32 Alinéa 2

9.321 En général

L'art. 322bis (nouveau), ch. 1, al. 1 CP requiert une connaissance sûre de la punissabilité de l'acte. Cela pose la question de savoir ce qu'il doit advenir du fournisseur d'hébergement qui n'a pas obtenu cette connaissance sûre, par exemple parce que les informations qui lui sont parvenues ne contiennent que l'adresse URL du site incriminé, sans plus de détails. Si le fournisseur d'hébergement demeure alors passif, il ne pourra jamais obtenir la connaissance requise au regard de l'al. 1. Le prix à payer pour l'inobservation de l'al.1, dont le libellé est, à juste titre, strict, serait trop élevé. Il faut donc que la limitation de la responsabilité à l'al. 1 soit (ré)équilibrée de ce point de vue.

Telle est la fonction de l'art. 322bis (nouveau), ch. 1, al. 2 CP.
Eu égard à cette option, il serait évident de concevoir l'al. 2 comme une norme axée sur l'« entrave », telle qu'on la connaît, par exemple, dans l'entrave à une prise de

sang (art. 91, al. 3 LCR). Le projet de réglementation y renonce *pour diverses raisons* :

- Une version de la norme axée sur l'entrave devrait être ainsi libellée : « Celui qui entrave l'obtention des informations requises en vertu de l'al. 1 est passible de la même sanction ». Néanmoins, il ne fait aucun doute qu'elle ne s'appliquerait qu'à l'auteur (de l'infraction) qui, par son comportement actif, entrave la prise de connaissance des informations qui lui sont adressées - pour s'exprimer de façon imagée : celui qui construit un mur autour de lui pour que l'information ne lui parvienne pas. Mais là n'est pas le problème. Il est beaucoup plus délicat de déterminer les circonstances dans lesquelles le fournisseur d'hébergement ne se coupe pas activement de l'extérieur, mais demeure simplement inactif, et les informations ne l'atteignent pas [245] ou il ne les recherche pas. En d'autres termes, les circonstances dans lesquelles l'information ne peut déployer ses effets. C'est donc surtout *l'omission* que l'al. 2 doit viser.

- Il faudrait par conséquent compléter le libellé de la disposition de la façon suivante : « … ou qui permet leur non-obtention ». On pourrait également dire : «Celui qui agit de telle sorte ou permet qu'il n'obtienne pas la connaissance nécessaire en vertu de l'al. 1 est passible de la même sanction ». Abstraction faite de la tournure, qui n'est pas très heureuse, et de la formulation, très technique, cette variante est entachée d'un désavantage majeur : elle induit de nouveau une obligation de contrôle positive pour le fournisseur d'hébergement. Or si la réglementation de l'al. 1 aspire à exclure une telle obligation par la limitation aux informations sûres, il doit en être de même, et à plus forte raison, de la réglementation de l'al. 2 qui vise à contrebalancer les déficits de l'al. 1.

  Or contrebalancer ne peut vouloir dire ici introduire une obligation de contrôle alors qu'elle avait été rejetée dans l'alinéa précédent. Indépendamment de cela, une obligation de contrôle, à condition qu'on veuille en admettre le principe, poserait la question de savoir dans quelle mesure le fournisseur d'hébergement est tenu d'explorer son serveur pour y trouver des informations de nature illégale. Il est impossible d'y répondre dans l'abstrait. L'introduction d'une responsabilité pour omission se traduirait donc par une grande insécurité du droit - à laquelle la nouvelle disposition entendait justement parer.

- Au vu de ces considérations, la seule solution serait de rajouter un élément supplémentaire à la version « entrave » déjà complétée par la variante de l'omission ; cet élément pourrait être ainsi exprimé : « Sans avertissement de tiers, nul n'est tenu de faire des recherches, sur un réseau de télécommunication, à propos d'informations au sens de l'al. 1». Cela dit, cette solution ne résout pas le problème de contrôle. En effet, elle reviendrait à dire de manière explicite qu'il y a obligation de recherches lorsque le fournisseur d'hébergement reçoit des avertissements de tiers. C'est justement pour éviter ce genre d'obligation qu'il a été décidé à l'al. 1 de restreindre à la connaissance « sûre » l'élément subjectif fondant la punissabilité de l'acte.

[245] Pour s'exprimer à nouveau de manière imagée : celui qui ne doit pas construire un mur parce que l'information ne parvient d'emblée pas jusqu'à lui par exemple parce qu'un fossé le sépare de « l'extérieur ».

Cette option serait également éludée si une obligation de procéder à des recherches naissait uniquement de la réception d'avertissements de tiers. Si on laissait de côté le membre de phrase « sans avertissement de tiers », on déboucherait sur une contradiction par rapport à la première phrase qui établit de manière explicite que celui qui « *permet* qu'il n'obtienne pas la connaissance nécessaire en vertu de l'al. 1 » remplit aussi l'élément constitutif de l'infraction. Au demeurant, ce genre de restriction d'obligation serait un cas unique n'apparaissant nulle part ailleurs dans le code pénal.

Pour cette raison, la commission opte pour une *mesure radicale*. Au lieu de chercher à contrebalancer la limitation de la punissabilité selon l'al. 1 par la connaissance sûre qu'il y a infraction au moyen d'une solution « d'entrave », quelle que soit sa formulation, le fournisseur d'hébergement se voit imposer l'obligation positive de répercuter aux autorités de poursuite pénale les avertissements concernant des infractions (présumées) figurant sur son serveur Internet. Cette solution garantit également que l'appréciation de la punissabilité - sous réserve de l'al. 1 - est effectuée par l'autorité compétente et non par un particulier ; il y a d'autant plus de raisons à cela que de nombreux éléments constitutifs qui peuvent acquérir ici une importance pratique – par ex. l'art. 135, 197 ou 261bis CP –, offrent des marges d'interprétation normative ; c'est justement dans les cas de doute que leur appréciation doit être réservée à une autorité compétente.

9.322 Points particuliers

9.322.1 Auteurs de l'infraction

L'al. 2 correspond en tous points à l'al. 1 quant à la définition des auteurs de l'infraction. N'est considéré comme auteur de l'infraction que la personne mettant à disposition, selon un procédé automatisé, des informations d'autrui sur un réseau de communications électroniques, c'est-à-dire le fournisseur d'hébergement. La disposition possède donc la même structure que l'al. 1 ; les commentaires relatif à l'al. 1 valent donc également pour l'al. 2.

9.322.2 Actes punissables

Tout comme l'al. 1, l'al. 2 établit un v*éritable délit d'omission* : le fournisseur d'hébergement omet de répercuter les avertissements reçus sur des fichiers (hébergés sur son serveur Internet) au travers desquels une infraction est commise. En d'autres termes, il ne porte pas ces informations à la connaissance des autorités de poursuite pénale. Là aussi, la possibilité et l'acceptabilité de la transmission sont bien entendu présupposées. Le projet n'impose pas de *délai* à cette transmission car elle résulte, dans le cas d'espèce, des possibilités du fournisseur d'hébergement ainsi que de considérations relatives à cette acceptabilité. La *forme* de la transmission, elle non plus, n'est pas réglementée ; toutes les formes de communication qui portent de manière fiable le contenu de l'information à la connaissance des autorités de poursuite pénale entrent ici en considération.

Enfin, le texte de loi ne dit pas à quelle autorité de poursuite pénale l'information doit être transmise. Préciser qu'il convient de la transmettre à l'autorité « compétente » de poursuite pénale serait une formule creuse : si l'on veut dire par là la transmettre à l'autorité ayant compétence de poursuivre l'infraction du fournisseur de contenus, il y a là problème car le fournisseur d'hébergement ne sait pratiquement jamais qui est compétent à cet égard ; par contre, si cela signifie que l'information doit être transmise à l'autorité de poursuite pénale ayant compétence de recevoir l'information, il s'agit alors d'une évidence qu'il est superflu de mentionner. Le point décisif quant à l'objectif normatif de l'al. 2 est que l'information soit portée à la connaissance d'une autorité de poursuite pénale et ne demeure pas sur le serveur Internet sans que cette autorité en ait connaissance. Du reste, dans la pratique, les voies de transmission des informations s'imposeront d'elles-mêmes.

Il convient de circonscrire avec plus de détails les *avertissements* que le fournisseur d'hébergement omet de répercuter - ce dont il lui est fait grief :

- En premier lieu, on entend par « avertissements » ceux qui sont *adressés* au fournisseur d'hébergement. Deux précisions sont à apporter à cet égard : l'obligation de transmission n'est créée que par les communications adressées individuellement au fournisseur d'hébergement, et non par des informations généralement accessibles au public, émanant par exemple de la presse écrite, de la radio ou de la télévision. Par ailleurs, elle n'est créée que lorsque l'avertissement lui est adressé à ce titre. Ainsi, s'il est abonné à un journal (*lequel* lui est adressé) dont il retire des indications sur un contenu illégal abrité sur son serveur Internet, cela ne suffit pas car un rapport spécifique entre l'indication elle-même et le processus de communication de cette indication fait défaut. Il en va de même si le fournisseur d'hébergement est abonné en ligne à des lettres d'information.

- Toutefois, il ne suffit pas que les avertissements « lui soient adressés ». N'est pas décisif le fait qu'ils aient été envoyés au destinataire « fournisseur d'hébergement », mais qu'ils soient *arrivés* jusqu'à lui et *l'atteignent effectivement*. C'est pour cette raison que le projet parle d'avertissements « qui lui sont effectivement parvenus ». Par contre, il n'est pas indiqué d'adopter une formulation selon laquelle les avertissements ont été « portés à sa connaissance ». Cela ferait entrer un élément subjectif dans la définition des conditions objectives de l'infraction. Le fait que le fournisseur d'hébergement doive prendre connaissance des informations pour agir intentionnellement est une question touchant l'élément subjectif de l'infraction qu'il convient de traiter en tant que telle.

  En théorie, il est possible d'entraver la réception - dans le domaine de la communication électronique - de ces avertissements de deux manières : soit une barrière est érigée (voir l'exemple déjà mentionné de la personne se coupant du monde extérieur en érigeant un « mur »), soit il n'existe pas de possibilité de prise de contact électronique (l'exemple du « fossé préexistant »). Dans la pratique, ces craintes n'ont probablement pas lieu d'être car les fournisseurs d'hébergement sont tributaires de la communication et disposent des canaux - ouverts - requis.

- La responsabilité du fournisseur d'hébergement est *limitée au cas des avertissents émanant de « tiers »*. Là aussi, cette précision a d'une part pour objectif de garantir que des informations généralement accessibles au public (radio ou télévision) ne créent pas d'obligation de transmission, et d'autre part de souligner à nouveau que le fournisseur d'hébergement ne doit pas rechercher lui-même des « informations ». Ce qui signifie que le fournisseur d'hébergement n'est pas tenu de répercuter, conformément à l'al. 2, les informations (à propos d'infractions) qu'il aurait *lui-même* découvertes (donc des « avertissements» qui n'émanent pas de tiers) dans la mesure où il considère leur punissabilité uniquement comme possible, mais pas comme certaine ; par contre, s'il est sûr de la punissabilité de l'acte, il doit bloquer l'accès au fichier faute de quoi il est tenu pour responsable en vertu de l'al. 1.

- Le fournisseur d'hébergement doit répercuter uniquement les informations concernant des fichiers qu'il héberge *lui-même*. Un avertissement adressé au fournisseur A selon lequel le fichier XY est de nature pornographique ne doit pas être transmise si le fichier incriminé est hébergé non par le fournisseur A, mais par le fournisseur B. En décider autrement se serait traduit par une obligation générale de dénoncer, limitée à une catégorie (les délits commis via Internet), sans que cette obligation ait un lien avec l'activité propre du fournisseur d'hébergement. Cette solution procède par ailleurs de la réflexion suivante : l'art. 322bis (nouveau), ch. 1, al. 2 CP établit lui aussi une norme positive de la participation (à l'acte du fournisseur de contenus) pour un domaine partiel et, dans une certaine mesure, en « seconde dérivation » ; mais il va bien sûr de soi que le fournisseur d'hébergement ne participe qu'à l'infraction commise sur son propre serveur Internet.

- *Ces avertissements* ont pour *objet* les données mises à disposition par le fournisseur d'hébergement au moyen desquelles une infraction est commise. Sur ce point, l'al. 2 correspond absolument à l'al. 1 ; les commentaires relatifs à l'al. 1 valent donc également pour l'al. 2.

  Sous le régime de l'art. 322bis (nouveau), ch. 1, al. 2 CP, un fournisseur d'hébergement prudent répercuteraa *tous les avertissements* aux autorités de poursuite pénale. Il échappera ainsi à la réalisation de l'illicéité telle que la prévoit la nouvelle disposition dans la mesure où l'avertissement ne contient pas déjà des données qui induisent, chez lui, la connaissance sûre de la punissabilité de l'acte incriminé. Par contre, si tel est le cas, et s'il se contente de répercuter l'information, il remplit les conditions posées par l'art. 322bis, ch. 1, al. 1 CP. Inversement, s'il renonce à répercuter une simple avertissement (« Le site XY contient des représentations de la violence »), les conditions de l'art. 322bis (nouveau), ch. 1, al. 2 CP ne sont pas remplies si les représentations ne réunissent pas les éléments objectifs de l'infraction au sens de l'art. 135 CP et si le fournisseur d'hébergement le sait (sinon, il y a délit impossible).

9.322.3 Eléments subjectifs de l'infraction

L'*intention* est une fois encore requise. Mais ici, même le dol éventuel suffit pour tous les éléments constitutifs de l'infraction : est punissable selon l'art. 322bis (nouveau), ch. 1, al. 2 CP celui qui considère comme sérieusement possible et accepte qu'un

avertissement reçu porte effectivement sur un fichier au contenu illicite, hébergé sur son serveur (l'information en question étant « mise à disposition » au sens de l'al. 2 par lui-même), et que malgré tout, il ne le répercute pas.

Il doit en aller de même pour le fournisseur d'hébergement qui ignorerait systématiquement les avertissements reçus. Si un certain nombre d'avertissements lui sont parvenus de diverses parts, il sera difficile d'interpréter son comportement autrement que comme l'acceptation du fait que parmi ces avertissements, il s'en trouve certains qui portent effectivement sur l'existence de fichiers pénalement répréhensibles. Il ne lui sera pas fait grief de ne pas avoir contrôlé ce fait (donc pas d'obligation de contrôle), mais de ne pas avoir répercuté les avertissements en dépit de leur plausibilité. transmis une possibilité qui semble évidente. En revanche, si le fournisseur d'hébergement pense à juste titre que lavertissement est fondé, mais qu'il ne s'agit pas d'un fichier hébergé chez lui, mais chez un concurrent XY, l'intention et, partant, la punissabilité selon l'al. 2 disparaissent s'il ne répercute pas l'information.

9.322.4 Sanctions

L'al. 2 menace également de l'*emprisonnement* ou de l'*amende*. A première vue, cela peut sembler sévère au regard de la simple inexécution d'une obligation de répercuter un avertissement. Mais lorsqu'on réalise que la disposition s'appuie, comme l'al. 1, sur la participation du fournisseur d'hébergement à l'acte principal et doit contrebalancer la limitation - nécessaire pour d'autres raisons - à la « connaissance sûre » prévue à l'al. 1 -, la sanction devient alors admissible.

9.33 Alinéa 3

9.331 Principe

La teneur proposée de l'al. 2 peut déboucher sur la situation suivante : un fournisseur d'hébergement ne répercute pas un avertissement exact sur une infraction au sens de l'al. 1, et l'auteur de cette infraction n'est pas poursuivi, et encore moins puni, parce qu'il n'y pas eu dépôt de plainte. Or la plainte est nécessaire (par ex. en cas d'atteinte à l'honneur, art. 173 ss CP ou de violation du droit d'auteur, art. 67 ss LDA). On observe une situation similaire dans le cas du recel (art. 160 CP). Lorsqu'une infraction préalable constitue un délit poursuivi sur plainte, - délit qui n'implique toutefois pas de poursuite pénale en raison de l'absence de plainte - le ch. 1, al. 3 de l'art. 160 CP prévoit que même le recel n'est pas poursuivi.

La commission d'experts propose une *réglementation analogue* pour l'art. 322bis (nouveau), ch. 1 CP: aucune procédure ne sera introduite contre le fournisseur d'hébergement si l'infraction ne constitue qu'un délit punissable sur plainte et qu'aucune plainte n'a été déposée.

Une réglementation allant dans un autre sens aurait mené au paradoxe selon lequel, par exemple en cas d'atteinte à l'honneur, le lésé présumé ne veut pas entamer de

poursuite alors que le fournisseur d'hébergement, qui reçoit l'avertissement sur l'infraction, serait toutefois obligé de le répercuter. S'il omettait de le faire, il faudrait introduire contre lui une procédure pour soupçon de violation de l'art. 322bis (nouveau) ch. 1, al. 2, CP. Dans cette procédure, il faudrait aborder publiquement l'atteinte présumée à l'honneur bien que ce soit justement ce que le lésé ne désire pas et qu'il ait renoncé à déposer une plainte.

Par ailleurs, l'al. 3 est également judicieux étant donné que l'art. 322bis (nouveau), ch. 1 CP consiste en définitive à prendre en compte dans le droit la contribution du fournisseur d'hébergement à l'infraction du fournisseur de contenus, c'est-à-dire à l' « acte principal ».

De par son caractère et au-delà de toute description spécifique des éléments constitutifs, cette contribution constitue un acte de complicité. Mais dans la mesure où aucune plainte n'est déposée contre l'auteur principal, cela signifie qu'il n'y en a également aucune à l'encontre du complice. En effet, s'il y avait dépôt de plainte contre le complice, l'auteur principal devrait également être poursuivi (art. 30, al. 1 CP). Sous cet angle également, la réglementation proposée est donc adéquate. Il convient néanmoins d'ajouter, uniquement à des fins de clarté, que les infractions traitées à l'art. 322bis, ch. 1, al. 1 et 2 CP ne deviennent pas, de ce fait, des infractions poursuivies sur plainte. L'al. 3 établit uniquement un blocage de la poursuite là où *l'infraction* au sens des al. 1 et 2 est une infraction poursuivie sur plainte, qui n'est toutefois pas poursuivie pour défaut de plainte.

9.332 Incertitude sur la plainte

Lorsqu'il réçoit un avertissement ayant trait à une infraction poursuivie sur plainte, le fournisseur d'hébergement ne sait pas, dans bien des cas, si une plainte a été effectivement déposée ; ignorant qu'il s'agit d'une infraction poursuivie sur plainte, il répercutera en tout cas l'avertissement. Il lui est donc recommandé de répercuter les avertissements sans se préoccuper de ce que plainte ait été déposée ou non. En effet, s'il y a eu dépôt de plainte, mais si le fournisseur d'hébergement estime par erreur qu'elle fait défaut, cette erreur ne concerne pas son intention, mais une condition de recevabilité et, de ce fait, n'entre pas en ligne de compte. Ce qui clarifie une fois encore la fonction de l'al. 3 : la disposition ne vise pas directement le fournisseur d'hébergement en ce sens qu'elle restreindrait la portée de son obligation de répercuter un avertissement. Elle a pour objectif de prévenir un résultat choquant, à savoir que le fournisseur d'hébergement serait puni pour avoir omis de répercuter un avertissement au sens de l'al. 2, alors que la personne concernée par l'infraction présumée refuse que cette dernière soit poursuivie et, de ce fait, punie.

9.333 Infraction poursuivie uniquement sur plainte, dont le dépôt fait défaut

L'al. 3 n'est pas seulement en relation avec l'al. 2, mais aussi avec l'al. 1 : même si le fournisseur d'hébergement est sûr que l'information d'autrui permet de commettre une infraction, il n'y a pas de poursuite pénale à son encontre lorsqu'il s'agit d'une infraction poursuivie uniquement sur plainte, mais qui n'a justement pas fait l'objet d'un dépôt de plainte. Les commentaires relatifs à l'al. 2 sont ici applicables par analogie : il n'y a aucun sens à empêcher l'utilisation d'un fichier au moyen de

laquelle une infraction est commise lorsque le présumé lésé refuse que l'infraction soit poursuivie et punie. Sinon, le fournisseur d'hébergement devrait également être pénalisé lorsque la personne dont l'honneur a été atteint lui signale elle-même le fichier incriminé, tout en lui annonçant qu'elle n'entend pas entamer de poursuite. A l'inverse : si le lésé veut que barrage soit fait à l'utilisation du fichier incriminé sur la base d'une norme pénale, il doit déposer une plainte.

9.34 Alinéa 4

9.341 Principe

La communication par Internet ignore les frontières. Cette disparition virtuelle des limites nationales est une source de difficultés dans l'application du droit (art. 3 ss CP). La réglementation ici proposée a résolu la première de ces difficultés : selon la jurisprudence du Tribunal fédéral, les actes de participation sont réputés commis au lieu de l'acte principal. Si ce lieu est à l'étranger, l'acte de participation - dans la mesure où il s'agit d'un acte de participation du fournisseur d'hébergement et non d'un cas de participation en tant qu'auteur - ne devrait en principe pas être punissable en Suisse.

Le présent projet contourne le problème en détachant partiellement la punissabilité du fournisseur d'hébergement de celle du fournisseur de contenus dans une perspective constructive. Si l'acte principal a lieu à l'étranger et si le fournisseur d'hébergement se trouve en Suisse, l'art. 322bis, ch. 1, al. 1 et 2 CP est applicable ; si le fournisseur d'hébergement se trouve aussi à l'étranger, la Suisse n'a pas de compétence juridictionnelle.

9.342 Punissabilité du délit

Un point néanmoins reste ouvert : en vertu de quel droit doit-on décider s'il y a *infraction*. En droit privé, la question du droit applicable s'apprécie selon les règles consacrées dans le droit international privé (art. 13 ss LDIP, ainsi que les dispositions spéciales concernant un domaine spécifique). C'est en vain que l'on chercherait ce genre de règles en droit pénal. Il y manque les dispositions légales explicites qui indiqueraient selon quel droit il convient de juger la punissabilité d'une infraction dans un contexte international. Les art. 3 ss CP ne sont pas applicables car (à l'exception des art. 5, al. 1, 2ème phrase, 6, al. 1, 2ème phrase et 6bis, al. 1, 2ème phrase), ils règlent la compétence internationale et non le droit applicable.

Le droit pénal actuel ne contient manifestement pas de structures parallèles permettant de résoudre la question du droit applicable : le CP ne renferme aucune norme indiquant en vertu de quel droit il conviendrait d'apprécier la punissabilité d'un acte qui relève des éléments constitutifs objectifs. Dans le cas « normal » de la complicité, cette question ne se pose pas lorsque l'acte principal a été commis à l'étranger: la complicité est également réputée commise à l'étranger ; la Suisse n'a pas de compétence juridictionnelle de sorte que la question du droit applicable ne peut se poser. Donc, dans un acte de complicité, la question du droit selon lequel il convient de juger l'acte principal commis à l'étranger ne se pose pas.

Il est toutefois évident que la question de la punissabilité du délit doit être jugée selon le *droit suisse*. A défaut, on ferait fi de la raison qui a présidé à l'introduction, dans le projet, de la punissabilité autonome du fournisseur d'hébergement : la nouvelle norme n'entend pas seulement réglementer les questions si contestées de la participation, mais empêcher aussi que l'information « punissable » puisse continuer à être consultée à partir d'un serveur suisse. Il tombe sous le sens à cet égard qu'un blocage ne peut revêtir un intérêt que si le fichier contient des informations punissables selon le droit *suisse* puisqu'il s'agit de l'application *de ce dernier*. La seule question qui demeure est de savoir s'il faut mettre en place une réglementation légale explicite [246].

9.343 Motifs en faveur d'une norme explicite

La considération selon laquelle l'art. 322bis (nouveau), ch. 1 CP constitue, au plan fonctionnel, une disposition régissant la participation, parle en faveur d'une solution explicite. La participation suit le sort de l'acte principal ; les autorités étrangères ont la compétence de l'appréciation de celui-ci et le droit étranger est applicable. S'ajoute à cela le fait que la nouvelle disposition renonce au principe de la double punissabilité pour autant qu'il s'agisse de l'appréciation de la punissabilité de l'infraction. Mettre en cause le fournisseur d'hébergement doit aussi être possible lorsque l'acte incriminé n'est pas punissable selon le droit du lieu où il a été exécuté. Certaines positions des milieux juridiques américains ou australiens, considérées comme racistes et discriminatoires selon le droit suisse, pourraient revêtir ici une portée pratique. Dans la mesure où ces deux modifications contiennent des divergences par rapport aux règles générales, elles plaident en faveur d'une réglementation légale explicite de la question du droit applicable.

9.344 Fonction du nouvel alinéa

Eu égard à la compétence internationale de la Suisse dans de tels cas, il est permis de dire que même sans la réglementation spéciale proposée, l'appréciation de la punissabilité de l'infraction devrait se faire selon le droit suisse. Si l'omission du fournisseur d'hébergement tombe incontestablement sous le coup de la compétence juridictionnelle suisse, elle doit donc aussi s'apprécier selon le droit suisse. Les dispositions d'exception déjà mentionnées des art. 5, 6, et 6bis CP (pour les trois articles, ch. 2, phrase 2) attestent que le législateur suisse est de cet avis. Mentionner que la loi du lieu de commission doit être appliquée lorsqu'elle est la plus clémente pour l'auteur de l'infraction n'a de sens que dans le contexte de l'applicabilité en soi du droit suisse.

---

[246] On ne peut rien déduire de la réglementation spéciale sur le blanchiment d'argent concernant le cas où l'acte préalable a été commis à l'étranger (art. 305bis, ch. 3 CP). Elle concerne en effet une situation spéciale d'entrave à la confiscation (sans le ch. 3, il y aurait impunissabilité parce que le Titre dix-septième ne protège que l'administration de la justice suisse ; toutefois, en cas d'actes préalables commis à l'étranger, elle protègerait l'administration de la justice étrangère) - , entrave qui n'a rien à voir avec l'art. 322bis, ch. 1 CP (il n'est pas ici fait grief au fournisseur d'hébergement de faire entrave à une confiscation ou à un blocage, mais d'avoir omis d'empêcher l'utilisation d'un fichier incriminé par le blocage de son accès).

Pour les art. 3 à 7 CP, l'applicabilité du droit suisse découle du fait que l'acte incriminé relève de la compétence juridictionnelle suisse. La répercussion tacite, mais en général contraignante (selon les art. 3 à 7 CP) de la compétence internationale est donc, selon le point de vue suisse, l'application du droit matériel suisse. Vu sous cet angle, le nouvel al. 4 ne ferait qu'apporter une *clarification*.

L'art. 322bis (nouveau), ch. 1, al. 4 CP rend d'emblée superflues les éventuelles discussions sur le droit applicable. Néanmoins, sous l'angle de la technique législative, la nouvelle disposition ne peut être intégrée à la disposition pénale matérielle (c'est-à-dire au nouvel art. 322 ^{bis}, ch. 1, al. 1 et 2 CP) car les infractions qui entrent ici en ligne de compte ne seraient pas d'emblée restreintes à une seule ou à un petit nombre seulement. Il faudrait en fait mentionner chaque infraction dont on pense qu'elle peut être commise à l'aide ou au travers des réseaux de communications électroniques. C'est le cas de *toutes* les infractions ; pour cette raison, la même teneur de la disposition figure dans un alinéa séparé.

Quelle que soit la décision qui serait prise en cas d'absence de réglementation, le libellé explicite disant que la punissabilité du délit doit être appréciée selon le droit suisse (étant entendu qu'il s'agit ici de l'application du droit matériel et non du droit de compétence [247]), élimine tout doute. Une telle clarté ne semble pas superflue dans un domaine où les normes du droit international d'application des lois ne sont pas très développées, le besoin de telles normes ne s'étant guère fait sentir jusqu'à présent..

9.35 Alinéa 5

Conformément à l'al. 5, les informations au sens des al. 1 et 2, à savoir celles au travers desquelles une infraction est commise, doivent être supprimées. La première question qui se pose ici est de savoir si cette disposition est nécessaire ou si une telle compétence ne découle pas de toute manière de l'application des règles générales de la confiscation.

[247] On tombe sinon dans un cercle vicieux : l'al. 4 renverrait à l'art. 3 ss CP, la Suisse aurait compétence juridictionnelle parce que le siège du fournisseur d'hébergement se trouve en Suisse ; pour cette raison, l'art. 322bis (nouveau), ch. 1 CP serait applicable. L'al. 4 permettrait de répondre à la question du droit auquel soumettre la punissabilité de l'infraction, et cet al. nous renverrait à l'art. 3 ss CP, etc.

9.351 Suppression dans le cas de l'al. 1

9.351.1 Principe

Le *sedes materiae* du droit de la confiscation est constitué, dans le présent contexte, par la confiscation d'objets dangereux conformément à l'art. 58 CP, ainsi que par d'éventuelles dispositions spéciales de confiscation dans certains cas d'infraction. Si dans une procédure pénale, par exemple pour pornographie dure (art. 197, ch. 3 CP), l'inculpé est condamné et si l'on trouve des données pornographiques sur le disque dur de son ordinateur, ce disque dur peut être confisqué en vertu des dispositions spéciales de l'art. 197, ch. 3, al. 2 et ch. 3bis, al. 2 CP. Mais cela ne veut pas dire que le condamné ne recevra plus son disque dur puisque le principe de la proportionnalité doit être respecté lors de la confiscation [248]. Les autorités d'exécution devront donc supprimer les données incriminées et rendre l'objet sous cette forme à l'ayant droit ; cela, uniquement si une autre utilisation délictueuse ne semble pas vraisemblable. L'objet de la confiscation demeure néanmoins un objet (matériel) au sens de l'art. 58 CP ; mais, du fait de la suppression des fichiers incriminés, il sera modifié de telle sorte que son caractère dangereux disparaît [249].

S'il faut supprimer des « informations punissables » chez un fournisseur d'hébergement qui a été condamné en vertu de l'art. 322bis (nouveau), ch. 1, al. 1 CP, il faudrait confisquer le serveur Internet lui-même - celui qui héberge les informations en question. Mais, étant en général disproportionnée, cette mesure n'est pas appropriée. En effet, elle toucherait, chez ce fournisseur d'hébergement, tous les autres clients qui ont aussi stocké des informations sur le serveur objet de la confiscation ; la faisabilité de cette mesure est tout aussi problématique. La solution est donc d'intervenir directement sur le serveur chez le fournisseur d'hébergement et de supprimer les informations « punissables », s'il ne s'est déjà conformé à l'injonction qui lui a été faite de procéder à cette suppression.

Il semble douteux que l'art. 58 CP soit applicable par analogie à ce cas. L'objet de la confiscation serait des données ou des informations, mais celles-ci ne constituent pas des objets matériels au sens de l'art. 58 CP [250]. En outre, il ne peut pas y avoir de confiscation matérielle, il s'agit uniquement d'un effacement de données. Pour ces raisons, la commission a opté pour une solution explicite de la question.

---

[248] BAUMANN, in Niggli/Wiprächtiger, Basler Kommentar, Bâle 2003, art. 58, n. 14. Cela s'applique également aux dispositions spéciales de confiscation figurant à l'art. 135, al. 2 et 197, ch. 3, al. 2 et ch. 3bis, al. 2 : AEBERSOLD, in Niggli/Wiprächtiger, Basler Kommentar, Bâle 2003, art. 135, n. 35; ne se prononcent pas clairement : SCHWAIBOLD/MENG, in Niggli/Wiprächtiger, Basler Kommentar, Bâle 2003, art. 197, n. 61.

[249] On peut ici laisser de côté la question de savoir si une ou plusieurs autres conditions de l'art. 58 CP doivent être remplies à propos de l'art. 197, ch. 3, al. 2 et 3bis, al. 2 CP.

[250] Selon SCHMID (Bibl.), n. 22 ad art. 58, les biens incorporels tels que les « créances, avoirs et biens immatériels tels que patentes, les droits d'auteurs, etc. peuvent, conformément à la tendance, ne pas être confisqués conformément à l'art. 58 CP » ; SCHMID entend faire une exception pour les données (loc. cit. , n. 57). Mais l'exception n'est pas motivée et l'exécution de la confiscation dans ces cas n'est pas explicitée plus en détail. TRECHSEL (Bibl.), n. 5 ad art. 58, mentionne l'effacement d'un programme sur un disque dur.

9.351.2 Nature matérielle de la suppression

Comme la confiscation, dont elle constitue le pendant, la suppression de l'information est de nature matérielle. Elle est ordonnée dans le jugement du tribunal. L'al. 5 ne consacre pas une disposition de procédure analogue au séquestre qui permettrait aux autorités de poursuite pénale de bloquer provisoirement l'information. Celle-ci est réservée à la législation procédurale, qui relève aujourd'hui encore des cantons. Ceux-ci sont tenus d'exécuter le droit pénal fédéral matériel et doivent prévoir à cette fin des instruments de procédure suffisants. Il s'agit ici en premier lieu d'une ordonnance de blocage des autorités de poursuite pénale; elle doit s'appuyer - en tant que mesure de contrainte - sur les dispositions cantonales.

L'avant-projet de code de procédure pénale suisse sera l'occasion de débattre de l'intégration d'une réglementation explicite du « séquestre » des données sous forme de blocage (de l'accès), y compris l'interdiction de les modifier [251]. De même, la convention du Conseil de l'Europe sur la cybercriminalité requiert, dans ses dispositions de procédure, que la législation donne les moyens nécessaires aux autorités compétentes pour bloquer l'accès à certaines données (art. 19, ch. 3, let. d).

9.351.3 Suppression des informations en cas d'acquittement

La suppression des informations n'est ordonnée par le tribunal que lorsqu'il y a condamnation. Pour ce qui est de la procédure contre le fournisseur d'hébergement et celle contre le fournisseur de contenus, il convient d'examiner à part dans quelle mesure une suppression entre également en considération en cas d'acquittement ou en cas de liquidation procédurale d'une cause :

- Si l'on ne peut condamner un fournisseur d'hébergement par exemple parce que l'on ne peut prouver qu'il a eu une connaissance sûre de la punissabilité de l'information, mais tout au plus un dol éventuel, la question se pose de savoir si les informations « punissables » peuvent, malgré tout, être supprimées dans le cadre de cette procédure. L'art. 58 CP prévoit la confiscation « alors même qu'aucune personne déterminée n'est punissable » ; il en va de même à propos de la disposition spéciale du nouvel al. 5.

  Cela signifie deux choses : *premièrement*, d'éventuelles causes d'exclusion de la culpabilité chez le fournisseur d'hébergement - lequel a réuni, dans son action, les éléments constitutifs de l'infraction et a agi en violation du droit - ne s'opposent pas à la suppression des données en question ; *deuxièmement* - aspect plus important dans le présent contexte - , une suppression est également admissible dans le cas où non l'accusé, mais un tiers a commis l'infraction fondant la confiscation. Dans ce cas également, les informations au moyen desquelles une infraction est commise, peuvent être supprimées du serveur Internet du fournisseur d'hébergement [252].

---

[251] Selon l'art. 273 ss AP CPP, le séquestre peut porter sur des « objets et valeurs patrimoniales ».

[252] Cf. ATF 124 IV 121 : X. était le destinataire de revues et CD au contenu raciste et discriminatoire. La cour suprême cantonale a nié la réalisation de l'élément subjectif de l'infraction et prononcé un jugement libérant X de la prévention de violation de l'art 261bis CP. Elle a par contre ordonné la confiscation des revues et des CD. Le Tribunal fédéral a confirmé la confiscation en invoquant le fait

Donc si le fournisseur d'hébergement est libéré de l'accusation de réalisation prévue par l'art. 322bis (nouveau) ch. 1, al. 1 CP, cela n'implique pas obligatoirement que les informations en question ne puissent pas être éliminées de son serveur : le tribunal peut prononcer la suppression de ces informations si le jugement établit qu'il s'agit en l'espèce d'un acte (commis par un tiers, c'est-à-dire ici par le fournisseur de contenus) constitutif de l'infraction et contraire au droit. Un examen plus poussé du danger spécifique associé à ces informations - que l'art. 58 CP mentionne spécialement pour les objets - ne sera effectué que s'il s'agit d'une infraction pour laquelle une disposition spéciale sur la confiscation est prévue(à savoir aux art. 135, al. 2, 197, ch. 3, al. 2 et ch. 3bis, al. 2 CP).

- Cette solution se voit néanmoins restreinte : le Tribunal fédéral a récemment établi clairement (la question était contestée dans la doctrine [253]) qu'en vertu de l'art. 59 CP, une confiscationde valeurs patrimoniales situées en Suisse n'est possible que si l'acte dont ces valeurs sont issues relève de la juridiction suisse [254]. Si l'on s'en tient aux arguments développés dans l'arrêt cité, ces conclusions devraient être également applicables à la confiscation d'objets dangereux dont il est question ici [255]. Ainsi, si la Suisse n'a pas la compétence de juger l'acte du fournisseur de contenus, la possibilité de supprimer les informations illégales en cas d'acquittement du fournisseur d'hébergement disparaîtrait en vertu des règles générales. Il en va de même en cas de procédure autonome [256] de confiscation ou de suppression contre le fournisseur d'hébergement.

- Pour cette raison, la commission d'experts a décidé de permettre la suppression des informations « que la Suisse ait ou non une compétence juridictionnelle ». Sous l'angle politico-juridique, il ne serait pas satisfaisant que le jugement d'acquittement prononcé à l'égard du fournisseur d'hébergement constate qu'un fournisseur de contenus a chargé un fichier constitutif d'infraction et contraire au droit sur le serveur du premier, mais qu'un effacement est néanmoins impossible parce que la Suisse n'a pas de compétence pour juger l'acte du fournisseur de contenus. En effet, la réglementation spéciale de l'art. 322bis (nouveau), ch. 1 CP n'entend pas donner seulement une définition plus précise de la punissabilité du fournisseur d'hébergement, mais aussi une possibilité d'intervention pour empêcher l'utilisation de l'information.

  Cette solution est donc un moyen de dépassionner le débat autour de la notion de résultat de l'art. 7 CP ou plus exactement de la nature (délit matériel/délit

---

que l'expéditeur, demeuré inconnu (habitant aux Etats-Unis), aurait rempli les conditions subjectives et objectives de l'art. 261bis, al. 1 CP ; en outre, du fait que l'art. 58 permet la confiscation « alors même qu'aucune personne déterminée n'est punissable », le TF a estimé sans pertinence que les personnes ayant diffusé ces revues et ces disques ne puissent pas être identifiées ou poursuivies en Suisse et que X ne soit pas lui-même auteur de l'infraction ou participant à celle-ci (cf. loc. cit., p. 126).

[253] Précisions dans SCHMID (Bibl.), n. 31 ad art. 58.

[254] ATF 128 IV 145.

[255] Les art. 3 à 7 CP constituent des règles d'application du CP dont l'art. 59 doit être considéré comme une partie (p. 151). - Il n'est pas clairement défini dans quelle mesure ils contiennent une contradiction par rapport à l'ATF. Cet arrêt laisse de côté la question et ne s'exprime pas sur le fait de savoir si la discrimination raciale commise par l'expéditeur des revues et des CD doit valoir comme ayant été commise en Suisse.

[256] Voir à ce propos SCHMID (Bibl.), n. 80 ad art. 58.

formel) de l'infraction donnée. Cette question a encore un sens dans la mesure où s'agit de savoir si le fournisseur de contenus relève de la compétence juridictionnelle de la Suisse. Par contre, elle n'a (plus) lieu d'être quant aux résultats que son infraction produit car le seul point de rattachement que l'on puisse invoquer est de déterminer si ces résultats sont hébergés auprès d'un fournisseur dont le siège est en Suisse.

En résumé : que la Suisse ait ou non une compétence juridictionnelle sur l'acte du fournisseur de contenus ne tire pas à conséquence en ce qui concerne la suppression des informations. Même si cette compétence n'existe pas, les informations sont supprimées du serveur Internet du fournisseur d'hébergement. Deux *genres de procédure* sont envisageables à cet égard : soit une procédure est déjà engagée contre le fournisseur d'hébergement pour soupçon de violation du nouvel al. 1 - procédure dans le cadre de laquelle la suppression peut être ordonnée indépendamment de l'issue de la procédure. Soit, s'il n'y a pas soupçon de violation de l'al. 1 et une procédure autonome est introduite. Si le tribunal conclut qu'un contenu déterminé réunit les éléments constitutifs de l'infraction et s'avère contraire au droit, il ordonne sa suppression.

Les codes cantonaux de procédure pénale doivent provisoirement garantir une procédure de suppression (par ex. § 106a s. du code de procédure pénal zurichois) [257], le for - au cas où il n'y a pas compétence de la Confédération en vertu du nouvel art. 340ter CP – devant être attribué, de manière pertinente, au lieu de la diffusion, c'est-à-dire là où se trouve le serveur d'hébergement (cf. la réglementation similaire pour les délits de média, art. 347, al. 2 CP). Il n'est pas nécessaire de définir explicitement la compétence à raison du lieu pour cette procédure autonome [258].

9.352 Suppression dans le cas de l'al. 2

La suppression est aussi un moyen nécessaire pour éliminer des fichiers illicites lorsqu'une procédure pénale a été introduite en vertu de l'al. 2, donc lorsque le fournisseur d'hébergement a omis de répercuter un avertissement. Elle est ici expressément mentionnée en fonction des mêmes réflexions développées à propos de l'al. 1. Il convient d'éviter notamment, en cas d'acquittement du fournisseur d'hébergement, que l'on constate certes que l'annonce se réfère à une information - servant à commettre une infraction (à apprécier selon le droit suisse conformément à l'al. 4) - mais qu'elle ne relève pas de la juridiction suisse, de sorte qu'elle ne pourrait pas être éliminée du serveur Internet du fournisseur d'hébergement.

Une autre question se pose s'agissant de l'al. 2 même dans le cas où, en fin de procédure, un jugement n'établit pas avec certitude si la connexité entre l'infraction (omission de répercuter l'avertissement) et les informations (« punissables ») est suffisamment étroite : peut- on dire des informations qu'elles « auraient servi à commettre une infraction » ? Ces incertitudes disparaissent avec la réglementation

[257] Il conviendra de tenir compte de cette procédure spéciale dans la révision du code de procédure pénale fédéral (cf. art. 45 AP concernant la procédure autonome de confiscation).

[258] De même, la loi ne définit pas avec précision le for pour les procédures autonomes de confiscation (art. 58 s. CP) ; cf. SCHMID (Bibl.) art. 58, n. 81; art. 59, n. 139 « Art. 346 ff. StGB nicht anwendbar » (*art. 346 ss CP non applicables*).

explicite de l'al. 5 : les informations signalées au fournisseur d'hébergement (grief peut lui être fait ultérieurement de ne pas les avoir répercutées) peuvent être supprimées s'il ressort de la procédure qu'elles constituent une infraction.

9.4 Commentaire relatif à l'art. 340ter (nouveau) CP

9.41 Exposé de la question

Dans a plupart des cas d'infractions relevant de la cybercriminalité, il est apparu que la compétence générale des autorités cantonales n'a pas donné lieu à une poursuite pénale effective. L'opération de grande envergure lancée contre les clients de l'exploitant américain d'un site Internet de pornographie enfantine à l'automne 2002 (l'opération Genesis) a mis en évidence le fait que l'Office fédéral de la police ne disposait pas des bases légales lui permettant de procéder à ses propres investigations, sans parler de l'absence de l'obligation de coordonner les procédures d'enquêtes au niveau des cantons. Cette situation s'est traduite, entre autres conséquences, par des *retards* dans la recherche des adresses de suspects auprès des entreprises de cartes de crédit et par un manque de coordination au niveau de la *politique de l'information*. En comparaison internationale aussi, les autorités suisses ont réagi *avec lenteur*.

Eu égard à l'extrême complexité des délits transfrontaliers commis par l'intermédiaire de réseaux de communications électroniques - les cyberdélits -, on constate un manque de *criminalistes spécialisés* et de moyens au niveau des cantons.

Dans bien des cas enfin, à l'ouverture d'une enquête, *l'autorité cantonale compétente pour la poursuite n'est pas clairement définie*. Ainsi, dans l'affaire du piratage du site du Forum Economique Mondial [259], ce sont d'abord les autorités genevoises qui sont intervenues parce que le serveur en question se trouvait au siège du Forum Economique Mondial à Genève. Ensuite, au terme de longues recherches, le cas a été transmis aux autorités bernoises parce qu'un suspect domicilié dans le canton de Berne avait été trouvé. Ainsi, lorsque les résultats présentent un lien avec la Suisse, il peut y avoir pléthore de compétences lorsqu'un résultat se produit sur tout le territoire (par ex. la diffusion de propos attentatoires à l'honneur). Conformément à l'art. 346, al. 2 CP, le canton compétent devrait être celui où la première instruction a été ouverte ; une telle intervention peut toutefois tenir du hasard [260].

9.42 Requêtes de la commission d'experts

S'appuyant sur ces expériences, la commission recommande la création d'une section spéciale centrale auprès de l'Office fédéral de la police, chargée de traiter les délits importants ou transfrontaliers en qualité de *service de clearing*, et agissant conformément à une norme de compétence claire. Il s'agit ici d'infractions

[259] En résumé à propos de ce cas, cf. SCHWARZENEGGER, E-COMMERCE (Bibl.), p. 333 avec renvois.

[260] Sur le for judiciaire dans le cas des cyberdélits en vertu du droit actuel (art. 346 ss CP), cf. ci-dessus chapitre 6, ch. 6.4.

complexes, réalisées au travers d'un réseau électronique, qui nécessitent des criminalistes spécialement formés et capables d'intervenir rapidement de manière coordonnée, à l'échelle intercantonale tout comme internationale. Cette nécessité est incontestée et a été déjà concrétisée dans d'autres pays (Etats-Unis, Japon, Italie, Autriche).

Mais, en même temps, il n'est pas souhaitable d'introduire une compétence fédérale pour tous les délits possibles - ceux impliquant un message électronique par exemple - ou pour les cas dépourvus d'importance. Ceux-ci doivent être exclus de la norme de compétence par une formulation adéquate.

Au demeurant, après la clôture de l'établissement des faits et les procédures compliquées de conservation des preuves, il n'est pas nécessaire de mener le cas à terme en procédure pénale fédérale. En réalité, un *modèle mixte* semble plus efficace et plus aisé à concrétiser.

9.43 Principes du modèle proposé

9.431 En général

Ce modèle prévoit une *unité centrale* préposée à la lutte contre la cybercriminalité. La mission de cette unité pourrait être assumée par le SCOCI (Service national de coordination de la lutte contre la criminalité sur Internet), doté de personnel supplémentaire. Elle enquêterait tout d'abord sous la direction d'un procureur de la Confédération. Ce service serait aussi responsable des contacts et de l'échange d'informations avec les unités chargées de la cybercriminalité dans d'autres Etats

Au terme de l'investigation, les cas simples seraient délégués aux autorités cantonales de poursuite pénale, un juge d'instruction, un procureur de district ou un procureur soutenant ensuite l'accusation devant le tribunal cantonal compétent.

Tout comme le crime organisé est soumis à la juridiction fédérale (art. 340bis, al. 1 CP), le procureur général de la Confédération peut déléguer aux autorités cantonales le jugement d'une affaire de droit pénal fédéral après la clôture de l'instruction et soutenir lui-même l'accusation.

9.432 Compétence fédérale contraignante ou facultative ?

9.432.1 En général

La réglementation concrète de la compétence peut prendre la forme soit d'une norme impérative, avec une restriction aux cyberdélits importants ou transfrontaliers (par analogie avec l'art. 340bis, al. 1 CP), soit d'une *disposition potestative* (par analogieavec l'art. 340bis,al. 2 CP).

Par souci de mettre en place une règlementation aussi claire que possible, la commission d'experts opte pour une prescription contraignante. Ce qui signifie qu'en

présence des conditions (restreintes), la compétence de poursuivre et de juger revient aux autorités fédérales. Les expériences rassemblées jusqu'ici par la police criminelle fédérale ont montré, par exemple dans le domaine du crime organisé, que l'application de l'art. 340bis, al. 1 CP ne pose pas de problèmes. La réglementation proposée a l'avantage de créer des conditions claires pour les autorités de poursuite pénale cantonales et pour le Ministère public de la Confédération. Conjointement aux deux conditions de la compétence fédérale (déjà citées), l'effet de filtre sera assuré contre toutes sortes d'états de faits simples en relation avec Internet.

9.432.2 Art. 340ter (nouveau) CP en particulier

L'art. 340ter (nouveau), *al. 1, let. a* CP se fonde sur l'art. 340bis,al. 1, let. b CP, alors que l'art. 340ter (nouveau), *al. 1, let. b* CP renferme un complément important quant à la fonction coordinatrice en procédure d'enquête lorsqu'un grand nombre de cas identiques surviennent dans différents cantons (voir l'opération Genesis).

En revanche, la reprise de la poursuite pénale par le Ministère public de la Confédération sur demande d'un canton est conçue comme une *disposition potestative* (une possibilité) : elle figure à l'art. 340ter (nouveau), *al. 2* CP. Au cours de la suite de la procédure, il faut prévoir un filtre supplémentaire avec la délégation aux autorités cantonales.

L'*art. 18bis PPF* contient déjà un tel filtre. Selon cette disposition, le procureur général peut déléguer une affaire aux autorités cantonales après la clôture de l'enquête préliminaire (art. 18bis, al. 1 PPF) ; il peut déléguer les enquêtes simples aux autorités cantonales que ce soit pour instruction, pour accusation ou même pour jugement (art. 18bis, al. 2 PPF).

L'entrée en vigueur de la *loi fédérale sur le Tribunal pénal fédéral* (LTPF) ne modifiera en rien la délégation de compétence du procureur général de la Confédération car l'art. 26 LTPF réserve expressément la possibilité, pour celui-ci, de déléguer l'instruction et le jugement aux autorités cantonales.

9.44 Remarques spécifiques concernant l'art. 340ter (nouveau) CP

- La proposition d'art. *340ter* (nouveau), *al. 1, let. a* CP couvre à la fois les faits complexes se passant en Suisse (par ex. le cas de piratage du site du Forum Economique Mondial) - dans lesquelles le for judiciaire peut, au début, ne pas être clairement défini -, que les délits transfrontaliers qui concernent plusieurs cantons, mais sans qu'il y ait prédominance d'un canton donné. Ces faits peuvent être pris en mains par un organe central, qui pourra, au besoin, confier la poursuite à une autorité cantonale.
- L'art. *340ter* (nouveau), *al. 1, let. b* CP est un nouvel article spécialement taillé pour les cas dans lesquels un grand nombre d'auteurs doivent faire l'objet d'une enquête pour des cyberdélits similaires et où une coordination est indispensable. Là aussi, une délégation aux cantons selon l'art. 18bis PPF est possible.
- Enfin, l'art. *340ter, al. 2* CP permet de faire entrer en jeu les autorités fédérales sur demande des autorités de poursuite pénale cantonales. Le Ministère public de la Confédération peut toutefois refuser cette requête au cas où une poursuite au

niveau local ne lui semblerait pas poser de problèmes. Il doit, dans cette décision, examiner les circonstances concrètes du cas d'espèce.

L'art. *340ter, al. 3* CP établit clairement, par analogie avec l'art. 340bis, al. 3 CP que l'ouverture d'une procédure d'enquête fonde automatiquement une compétence de la Confédération.

A la lumière de ses propositions de réglementation pénale, la commission d'experts considère d'un œil critique les procédures législatives en cours dans le domaine de la cybercriminalité. Elle désire par ailleurs exprimer des recommandations concernant les autres mesures législatives à prendre dans ce domaine.

10. Procédures législatives parallèles et autres tâches législatives en matière de cybercriminalité

10.1 Avis de la commission concernant les procédures législatives parallèles

Diverses autres procédures législatives sont actuellement en cours, parallèlement aux travaux de la commission d'experts « Cybercriminalité ». Ces procédures touchent également des questions sur lesquelles la commission s'est penchée. Cette dernière estime donc opportun et urgent de se prononcer sur ces dispositions légales élaborées en parallèle et de souligner le danger de contradictions pouvant survenir entre le droit pénal fondamental et les autres textes législatifs de la Confédération.

10.11 Loi fédérale sur le commerce électronique

L'avant-projet relatif à la loi fédérale sur le commerce électronique (Révisions partielles du code des obligations et de la loi fédérale contre la concurrence déloyale) du 17 janvier 2001 [261] contient le passage suivant :

> « De même, les éventuelles adaptations du droit des biens immatériels et de la responsabilité pénale et civile du fournisseur d'accès dépendent pour l'essentiel des développements sur le plan international. Un besoin de légiférer n'existe pas dans l'immédiat. Des solutions adéquates peuvent être trouvées sur la base des règles actuelles ».

L'avis de la *commission Cybercriminalité* diverge sur ce point. Elle estime qu'il serait souhaitable de procéder à un examen approfondi des questions touchant à la responsabilité civile et à ses limitations, en relation avec la transmission et la préparation automatiques de données sur les réseaux de communications électroniques [262]. D'une part, ces questions pourraient être traitées dans le cadre des travaux législatifs en cours sur le commerce électronique. La portée fondamentale de cette question nécessiterait néanmoins qu'un complément dans ce sens fasse l'objet d'une procédure de consultation spécifique. D'autre part, on pourrait procéder à une

[261] Adresse Internet: www.ofj.admin.ch/themen/e-commerce/vn-ber-b-d.pdf
[262] Cf. plus haut chapitre 8, in fine, ainsi que chapitre 11, ch. 11.33.

limitation échelonnée de la responsabilité pour les différents groupes de prestataires, également dans le cadre des travaux de révision de la *loi sur le droit d'auteur* ou du *droit de la responsabilité civile*.

10.12 Loi fédérale sur les loteries et les paris professionnels

Le projet du 25 octobre 2002 relatif à la révision de la loi fédérale sur les loteries et les paris professionnels a fait l'objet d'une *procédure de consultation* qui a duré jusqu'au 31 mars 2003 [263].

L'art. 50, let. d du projet est ainsi libellé :

> « Art. 50 Délits
>
> *[1] Sera puni de l'emprisonnement pendant un an ou plus ou d'une amende de un million de francs au plus quiconque :*
> *...*
> *d. aura transmis en tant que fournisseur d'accès (« provider ») des jeux non autorisés par la présente loi.*
>
> [2] Dans les cas graves, la peine sera la réclusion pendant cinq ans au plus ou l'emprisonnement pendant un an au moins. Cette peine pourra être assortie d'une amende de deux millions au plus.
>
> [3] Quiconque aura agi par négligence sera puni d'une amende de 500 000 francs au plus. »

Le *rapport explicatif* s'exprime ainsi à propos de l'art. 50, al. 1, let. d du projet :

> « Le montant maximal de l'amende prévu ici est nettement supérieur aux maxima définis dans la partie générale du code pénal ce qui, aux yeux de la commission, se justifie, compte tenu de l'importance des intérêts économiques en jeu. Seules des sanctions conséquentes sont de nature à contribuer à ce que les exploitants suisses et étrangers se conforment aux dispositions de la loi et n'incluent pas d'emblée dans leur calcul financier l'amende dont ils pourraient écoper.
>
> La commission est, en outre, persuadée que l'on ne parviendra à lutter efficacement contre l'offre de loteries et de paris non autorisés sur Internet, qu'à la condition de sanctionner également les fournisseurs d'accès (providers) qui se livreraient à une telle diffusion » [264].

La *commission d'experts* « *Cybercriminalité* » est d'un autre avis sur ce point. Dans une perspective constitutionnelle et administrative, elle estime que les obligations de contrôle qui naîtraient d'une telle disposition pénale pour les fournisseurs d'accès seraient inadmissibles parce que disproportionnées. Par ailleurs, la mesure prévoyant un blocage local n'est guère efficace du point de vue technique car les possibilités de la contourner sont très nombreuses et échappent au contrôle des

---

[263] Adresse Internet: www.ofj.admin.ch/themen/lotterie/lg-rev/intro-d.htm
[264] Rapport explicatif du 25 octobre 2002, relatif au projet de loi fédérale sur les loteries et paris, p. 43.

fournisseurs d'accès. Enfin et surtout, la punissabilité des fournisseurs d'accès serait en contradiction avec le droit en vigueur dans l'espace européen [265].

Du point de vue pénal, une obligation de contrôle ou de blocage serait non seulement disproportionnée, mais établirait en outre une punissabilité pour des activités économiques absolument légales bien que le fournisseur d'accès, objet de la disposition, n'ait aucun contact avec l'exploitant des loteries ou paris illégaux responsable de l'illicéité, ne le connaisse pas, ni ne profite de ses actions - contrairement par exemple à la situation en matière de blanchiment d'argent.

L'exclusion de punissabilité proposée par la commission d'experts pour les « purs » fournisseurs d'accès (art. 27 [nouveau], ch. 4 CP) doit également valoir pour l'ensemble du droit pénal accessoire (cf. art. 333, al. 1 CP). Une disposition divergente dans la loi fédérale sur les loteries et les paris réduirait à néant l'unification recherchée au travers de la nouvelle réglementation. L'art. 50, let. d du projet de loi fédérale sur les loteries et paris professionnels doit donc être supprimé.

10.13 Loi fédérale instituant des mesures contre le racisme, le hooliganisme et la propagande incitant à la violence

La loi fédérale instituant des mesures contre le racisme, le hooliganisme et la propagande incitant à la violence a fait l'objet d'une *procédure de consultation* jusqu'au 31 mai 2003 [266].

Elle renferme une modification de la loi fédérale du 21 mars 1997 instituant des mesures visant le maintien de la sécurité intérieure (LMSI, RS 120) ainsi libellée :

« Art. 13bis (*nouveau*) Saisie, séquestre et confiscation de matériel de propagande

[1]Les autorités de police et les autorités douanières saisissent, à l'intention de l'office fédéral, indépendamment de sa quantité, de sa nature et de son type, le matériel qui peut servir à des fins de propagande et dont le contenu:
a. est à caractère raciste, ou
b. incite, d'une manière concrète et sérieuse, à faire usage de la violence contre des personnes ou des groupes de personnes, ou à endommager leurs biens ou à bafouer d'autres droits.
[2]Si des collaborateurs de l'office fédéral trouvent du matériel au sens de l'al. 1, ils peuvent le saisir directement.
[3]En cas de soupçon d'un acte punissable, l'autorité chargée de la saisie transmet le matériel à l'autorité pénale compétente.
[4]Dans les autres cas, les autorités de police et les autorités douanières transmettent le matériel à l'office fédéral. Celui-ci décide du séquestre et de la confiscation. La loi fédérale du 20 décembre 1968 sur la procédure administrative est applicable.
[5]Si du matériel de propagande défini à l'al. 1 est diffusé par le biais d'Internet, l'office fédéral peut recommander aux fournisseurs d'accès de bloquer les sites concernés. »

A propos de l'al. 5 de cette disposition, le *rapport explicatif* accompagnant le projet mis en consultation relève ce qui suit :

---

[265] Cf. art. 12 de la directive européenne sur le commerce électronique; voir plus haut, chapitre 4.
[266] Adresse Internet : www.ejpd.admin.ch/doks/mm/2003/030212c-d.htm.

« Art. 13bis, al. 5 : prenant en compte les recommandations émises lors de la consultation des offices, le nouvel art. prévoit aussi que l'office fédéral compétent puisse agir contre la diffusion de propagande sur Internet au sens de l'al. 1, let. a et b, dudit article. L'office fédéral peut recommander aux fournisseurs d'accès concernés de bloquer les sites Internet qui contiennent de la propagande visée par la loi. Ce blocage ne concerne que les sites qui sont hébergés à l'étranger. Les sites hébergés en Suisse sont dénoncés auprès du juge pénal. »

Par contre, le rapport élaboré en septembre 2000 [267] par le *groupe de travail Extrémisme de droite* (GT Extrémisme de droite), antérieur au projet et au rapport y relatif, avait souligné que la poursuite pénale relative aux contenus Internet consultables sur les serveurs européens ne se heurtait à aucun problème incontournable [268], mais que le blocage des contenus incriminés par des fournisseurs de services Internet (suisses) impliquait par contre une multitude de problèmes techniques [269].

Le groupe de travail avait en conséquence recommandé aux autorités compétentes :

- de poursuivre la collaboration avec les fournisseurs suisses afin de lutter contre la diffusion de contenus extrémistes sur Internet,
- de promouvoir la collaboration internationale en vue de créer une convention relative aux contenus illicites sur Internet,
- de maintenir ou de renforcer la pression diplomatique sur les Etats constituant une assise pour la diffusion de ces contenus [270].

A l'instar du groupe de travail, la *commission d'experts « Cybercriminalité »* estime qu'une collaboration des autorités avec les fournisseurs est extrêmement positive. Elle considère néanmoins que l'al. 5 du nouvel art.13bis LMSI est inutile. De simples recommandations des autorités compétentes qui, en cas d'inobservation, n'ont aucune suites pénales, civiles ou administratives, ne nécessitent pas de base légale explicite et sont déjà possibles sur la base de la législation actuelle.

Pour les raisons citées, une compétence des autorités fédérale visant à ordonner un blocage des contenus incriminés par des fournisseurs d'accès serait disproportionnée (cf. plus haut ch. 7.215) et ne pourrait donc s'appuyer sur l'art. 13bis, al. 5 projet-LMSI. Le commentaire relativement peu précis de la norme dans le rapport d'accompagnement devrait être corrigé dans ce sens. Afin d'éviter les malentendus, la commission d'experts se prononce en faveur d'une suppression de l'art. 13bis, al. 5 projet-LMSI.

10.2 Autres tâches législatives en matière de cybercriminalité

Dès le début de ses consultations, la commission d'experts a décidé *de procéder par étapes*. Elle a d'abord mis l'accent sur la clarification des limites posées à la punissabilité en cas de transmission et de mise à disposition automatique des données sur les réseaux de communications électroniques, étant évident qu'il

[267] Adresse Internet : www.bap.admin.ch/d/aktuell/berichte/bericht-d-ag-rex-d-01-s.pdf
[268] Rapport du GT Extrémisme de droite, p. 28.
[269] Rapport du GT Extrémisme de droite, p. 41.
[270] Rapport du GT Extrémisme de droite, p. 44.

convenait d'examiner la question à la fois sous l'angle du droit public et du droit civil. Elle s'est également penchée en priorité sur la création de nouvelles conditions-cadres permettant de *lutter efficacement contre la cybercriminalité*.

La création de compétences centralisées d'investigation et d'un service de clearing au niveau fédéral figure à cet égard au premier plan ; ces deux mesures ont pour but de garantir la rapidité de réaction et la coordination internationale dans les cas complexes sans élargir inutilement les compétences de la Confédération. Par ailleurs, il s'agit d'introduire une règle pénale permettant d'éliminer les informations incriminées dans la mesure où elles ont été préparées et mises à disposition en Suisse. Cet objectif correspond à celui de la motion Pfisterer (cf. plus haut ch. 1.21) ainsi qu'au mandat confié par le DFJP à la commission d'experts (cf. plus haut ch. 1.3).

La commission d'experts relève expressément que ses propositions *ne sont qu'un premier pas* vers des conditions-cadres pénales pertinentes et une poursuite efficace de la cybercriminalité. D'autres mesures devront suivre.

10.21 Adaptation du droit interne à la Convention sur la cybercriminalité

Il conviendra ensuite de procéder sans attendre aux adaptations législatives en vue de la ratification de la Convention du 23 novembre 2001 sur la cybercriminalité (CCC (STCE n° 185) [271], dont la Suisse est l'un des 31 Etats signataires. Cette convention du Conseil de l'Europe requiert diverses modifications du droit pénal interne et surtout de la procédure pénale.

10.211 Contenu de la Convention

La Convention sur la cybercriminalité a comme objectif premier une *harmonisation des dispositions pénales matérielles* dans le domaine de la criminalité informatique et de la cybercriminalité [272].

En second lieu, la Convention vise la création d'un *arsenal de règles uniformes de procédure pénale* permettant l'investigation et la poursuite des délits commis à l'aide d'un système ou d'un réseau informatique. Ces règles ont notamment pour but de permettre ou de faciliter la conservation rapide sous forme électronique des moyens de preuve « éphémères » et des données de liaison [273].

---

[271] Le texte de la convention est disponible sur Internet à l'adresse http://conventions.coe.int.

[272] Chapitre II Section 1 de la Convention. Outre les infractions contre la confidentialité des données et des systèmes informatiques (art. 2 à 3 CCC), la Convention définit aussi l'atteinte à l'intégrité des données (art. 4 CCC), l'atteinte à l'intégrité du système (art. 5 CCC), l'abus de dispositifs (art. 6 CCC), la falsification informatique (art. 7 CCC), la fraude informatique (art. 8 CCC), les infractions se rapportant à la pornographie enfantine (art. 9 CCC) et enfin les infractions liées à la propriété intellectuelle et les droits connexes (art. 10 CCC). Par ailleurs, ce titre contient une disposition sur la responsabilité des personnes morales (art. 12 CCC). Un *premier protocole additionnel* visant l'harmonisation des normes pénales matérielles *en matière de discrimination raciale et de xénophobie* a été ouvert à la signature le 28 janvier 2003. La Suisse n'a pas encore signé ce protocole additionnel.

[273] Le chapitre II Section 2 de la Convention. L'élargissement du champ d'application de ces normes est particulièrement important. Elles ne sont donc pas seulement applicables aux infractions conformément aux art. 2 à 11 CCC, mais à toutes les infractions pénales commises au moyen d'un

Troisièmement, la Convention entend établir un *système* plus rapide et plus efficace *concernant l'extradition et l'entraide* à propos des infractions commises dans une intention délictueuse ou en relation avec un système informatique ; elle complètera les conventions actuelles sur l'entraide et les traités bilatéraux ou comblera les lacunes en l'absence de traités ou d'arrangements [274].

La Concention prévoit également des *mesures provisoires*, telles que la conservation rapide de données informatiques stockées (art. 29 CCC) ou la divulgation rapide des données de liaison conservées (art. 30 CCC).

Le dernier chapitre de la Convention, le chapitre IV Clauses finales (clauses contractuelles standards des accords conclus dans le cadre du Conseil de l'Europe) contient à l'art. 41 une « *clause fédérale »* applicable à la Suisse. Selon cette clause, les Etats fédéraux peuvent se réserver le droit d'honorer les obligations aux termes du Chapitre II de la Convention dans la mesure où celles-ci sont compatibles avec les principes fondamentaux qui gouvernent les relations entre son gouvernement central et les États constituants. Lorsqu'il fait une réserve prévue au paragraphe 1, l'Etat fédéral doit néanmoins garantir une poursuite pénale étendue et efficace en vertu des principes statués au chapitre II. La réserve ne pouvant être étendue au chapitre III, toutes les obligations sur la coopération transfrontalière doivent également être respectées [275].

10.212 Adaptations nécessaires

Le mandat donné à la commission d'experts n'aurait pas permis, eu égard aux délais, d'examiner les adaptations nécessaires du *droit de procédure pénale* surtout, lesquelles relèvent encore de la compétence des cantons.

Il convient à cet égard de tenir compte notamment des travaux en cours relatifs au *code suisse de procédure pénale*. La mise en oeuvre des principes de la Convention sur la cybercriminalité doit être coordonnée avec ces travaux. En outre, il reste à débattre de la modification de la *loi fédérale sur la surveillance de la communication par poste et télécommunication* (LSCPT, RS 780.1) et de l'ordonnance y relative (OSCPT; RS 780.11) car la Convention sur la cybercriminalité prévoit des pouvoirs et des compétences élargies quant à l'obtention des données relatives aux communications.

Par ailleurs, il s'imposera d'adapter aussi les *normes de la Partie spéciale* du code pénal.

La Convention sur la cybercriminalité pose un cadre de réglementation flexible qui, à de nombreux égards, permet aux Etats signataires de requérir des explications (art.

---

système informatique et à la collecte des preuves électroniques de toute infraction pénale (art. 14, al. 2, let. b et c CCC).

[274] Chapitre III de la Convention.

[275] Cf. à ce propos OFFICE FEDERAL DE LA JUSTICE, Rapport national de la Suisse sur la prévention et la lutte contre la cybercriminalité, Conférence sur la Cybercriminalité, Budapest, 22 novembre 2001; CHRISTIAN SCHWARZENEGGER: Die internationale Harmonisierung des Computer- und Internetstrafrechts durch die Convention on Cybercrime vom 23. November 2001, in: Festschrift Trechsel, Zurich 2002, p. 305 ss avec d'autres renvois.

40 CCC), ou de se prévaloir de réserves (art. 42 CCC), permettant ainsi une mise en pratique limitée. C'est pourquoi il faut déterminer tout d'abord s'il convient de viser pour la Suisse une solution minimale ou une adaptation la plus complète possible.

10.213 Recommandations de la commission d'experts

La commission d'experts recommande d'examiner les problèmes découlant de la Convention sur la cybercriminalité soit dans le cadre d'un élargissement de son mandat, soit dans le cadre d'une autre commission d'experts. Le résultat de ces travaux sera intégré dans le code pénal, dans une loi distincte relative aux mesures de contrainte de la procédure pénale en matière de cybercriminalité, ainsi que dans la LSCTP et l'OSCTP.

Les travaux relatifs au code de procédure pénale suisse sont loin d'être terminés. La mise en application de la Convention sur la cybercriminalité étant particulièrement urgente dans l'optique d'une poursuite efficace de la cybercriminalité (voir ci-dessous ch. 10.22) et s'agissant en outre d'un domaine spécial, la commission d'experts est d'avis qu'il faut entamer immédiatement les travaux préparatoires en vue de la ratification de la Convention sur la cybercriminalité. Au niveau cantonal, les règles de procédure pénale nécessaires ne doivent plus être mises en œuvre de manière autonome.

10.22 Révision de la LSCPT [276] visant à définir le lieu de commission

L'adresse IP [277] transmise dans presque tous les genres de communication est le point de référence fondamental en matière de poursuite d'activités pénalement répréhensibles. Elle est la seule à permettre, notamment en cas de délits formels, d'établir rapidement la *compétence à raison du lieu* et d'introduire les éventuelles mesures pour assurer la conservation des preuves.

Si l'auteur de l'infraction est branché sur Internet par une *adresse IP statique*, les autorités de police suisses, entre autres, peuvent, en application de l'art. 14 LSCPT (en liaison avec l'art. 27, let. a OSCPT), obtenir le nom et l'adresse de la personne en question, également en dehors d'une procédure pénale formelle ; elles sont soutenues à cet égard par le Service des tâches spéciales (STS), subordonné au DETEC.

Dans la majorité des cas néanmoins, l'auteur de l'infraction n'a pas d'adresse IP statique. En fait, une adresse IP (dite *adresse IP dynamique*) lui est attribuée par le fournisseur Internet pour chaque consultation d'Internet. On ne peut donc obtenir l'adresse de son domicile que par une mesure juridictionnelle et, de ce fait, uniquement dans le cadre d'une procédure pénale formelle (cf. art. 24, let f OSCPT). En effet, les données individuelles concernant l'adresse IP dynamique sont englobées, en tant que données relatives aux communications et à la facturation, dans les données sur lesquelles il convient d'observer le secret conformément à l'art.

---

[276] Loi fédérale du 6 octobre 2000 sur la surveillance de la correspondance par poste et télécommunication (RS 780.1).

[277] Adresse protocole Internet : série de quatre nombres que reçoivent tous les ordinateurs branchés sur Internet.

43 LTC. La compétence cantonale à raison du lieu est ici déterminable uniquement jusqu'au siège du fournisseur ce qui, fréquemment (notamment en cas de gros fournisseurs présents au niveau national), mène à des résultats insatisfaisants et inefficaces.

Néanmoins, une *poursuite pénale efficace* requiert absolument que le Service de coordination de la lutte contre la criminalité sur Internet (SCOCI), géré par les cantons et la Confédération, puisse connaître le plus rapidement possible le lieu de connexion [278], même *en dehors de toute procédure pénale formelle,* pour pouvoir transmettre le cas aux autorités véritablement compétentes.

Bien que le lieu de connexion ne permette, en soi, d'obtenir de précisions ni sur la personne consultant le réseau, ni sur la portée et la durée de la liaison Internet, il y a lieu d'admettre en vertu de l'actuelle LSCPT que cette information constitue une *donnée relative à la communication,* que l'on peut obtenir uniquement dans les conditions posées par l'art. 3 en liaison avec l'art. 5 LSCPT. La Convention sur la cybercriminalité requiert une conservation rapide des *données relatives au trafic* (art. 16 CCC), pour lesquelles elle établit un niveau de protection un peu moins élevé que pour les *données relatives au contenu.* Les modifications de loi requises (cf. ci-dessus ch. 10.21) seront donc l'occasion d'aborder en priorité la différenciation, dans le cadre d'une révision de la LSCPT, entre données relatives au trafic (ou données de liaison) et données relatives au contenu.

A cet égard, il conviendra de ne pas perdre de vue le fait qu'un accès facilité aux données relatives aux communications – qui pourrait avoir lieu notamment par ordonnance à la place de l'ordre de surveillance – est aussi essentiel à la détermination du lieu de l'infraction, dont dépendent la compétence juridictionnelle et le for judiciaire. En vertu de la nouvelle réglementation de compétences ici proposée (art. 340ter ([nouveau] CP), cet accès sera dans bien des cas du ressort du SCOCI.

[278] Il s'agit ici du raccordement téléphonique ou du raccordement par câble à partir duquel une personne peut se connecter à Internet.

11. Conclusion

11.1 Généralités

Que ce soit sur le fond ou sous l'angle juridique - et bien entendu politique -, la cybercriminalité est un sujet complexe, aux *multiples facettes*.

La commission d'experts s'est attachée à en donner *la meilleure vue d'ensemble possible* et à analyser tous les points essentiels. Elle avait néanmoins fixé des *priorités* et s'est penchée avec plus d'insistance sur certains domaines (cf. ci-dessous ch. 11.2), alors que d'autres aspects ont été *abordés de manière sommaire* (cf. ci-dessous ch. 11.3).

Conformément au mandat qui lui avait été confié, la commission a mis tout particulièrement l'accent sur la thématique « *droit pénal* » (cf. ci-dessous ch. 11.2). En effet, ce mandat était essentiellement axé sur l'examen de la responsabilité pénale sur Internet, plus particulièrement sur le point si controversé de la *responsabilité pénale des fournisseurs d'Internet* qui a d'ailleurs été l'une des raisons majeures de la création de la commission. Sans oublier bien entendu, tant au niveau politique que public, la question extrêmement sensible de la *pédocriminalité* (et de quelques autres formes de criminalité) dont le réseau Internet est devenu le vecteur majeur.

11.2 Le droit pénal en point de mire (chapitres 6 et 9)

11.21 Responsabilité pénale

Exposé de la question

Le droit pénal en vigueur n'offre aucune réglementation claire et explicite de la responsabilité en rapport avec les contenus illégaux. Le débat porte ici sur le fait de savoir si, et dans quelle mesure, les prescriptions du droit pénal des médias et les règles générales du code pénal sont applicables. La loi doit donc contenir une réglementation précise de la question.

Proposition de solution de la commission d'experts

A l'instar de certaines prescriptions d'application de la directive de l'Union européenne sur le commerce électronique (cf. les considérations de droit comparé figurant au chapitre 4), la commission d'experts propose au chapitre 9 (notamment aux ch. 9.2 et 9.3) d'introduire une *nouvelle réglementation dans le code pénal* [art. 27 (nouveau) et art. 322^{bis} (nouveau)] selon laquelle :

- l'auteur et le *fournisseur de contenus* sont pleinement responsables pénalement des contenus illégaux qui émanent d'eux ;

- le *fournisseur d'hébergement* encoure d'une responsabilité limitée : il n'est responsable que lorsqu'il omet, en connaissance de cause, d'empêcher l'utilisation d'informations constituant une infraction alors qu'on peut raisonnablement et techniquement l'attendre de lui, ou s'il ne transmet pas aux autorités de poursuite pénale les avertissements reçus de tiers à propos de ces informations ;

- le *fournisseur d'accès* n'est pas pénalement responsable des contenus délictueux circulant sur Internet.

11.22 Caractère international de la cybercriminalité

Exposé du problème

La cybercriminalité ignore les frontières nationales. Elle est présente au niveau mondial. Souvent, vu de la Suisse, l'auteur de l'infraction se trouve à l'étranger, dans un pays qui parfois a de tout autres bases légales que la Suisse. Il serait impossible de le poursuivre pénalement en Suisse compte tenu des points de rattachement traditionnels de la juridiction pénale suisse.

Propositions de solutions de la commission d'experts

- Comme il est mentionné plus haut au ch. 11.21, le fournisseur d'hébergement qui se trouve en Suisse doit pouvoir, à certaines conditions, être poursuivi pénalement (cf. chapitre 9, ch. 9.3)
- La réglementation proposée permet de *compenser dans une certaine mesure* le caractère transfrontalier de la cybercriminalité. En effet, lorsque des contenus étrangers sont aussi stockés sur le serveur de l'hébergeur suisse, ces contenus peuvent être jugés en vertu du droit pénal suisse.
- Par ailleurs, la commission d'experts recommande de procéder sans attendre à *l'adaptation des dispositions du droit suisse* aux exigences de la *Convention sur la cybercriminalité* signée par la Suisse (cf. chapitre 10, ch. 10.2).

11.23 A qui incombe la poursuite pénale ?

Exposé du problème

Détecter rapidement les contenus Internet délictueux et y répondre par des contre-mesures tout aussi rapides requièrent que l'on dote la police et la justice des moyens adéquats. Eu égard au caractère transfrontalier très marqué de la cybercriminalité et au nombre incommensurable de sites Internet, bien des cantons, à qui la poursuite et le jugement de ce genre d'infractions incombent, ne disposent pas des moyens et des capacités nécessaires.

Proposition de solution de la commission d'experts

- Depuis le 1er janvier 2003, l'Office fédéral de la police dispose d'un service qui effectue des recherches sur Internet dans le but de déceler les infractions commises (activités de monitoring) et coordonne les communications émanant de particuliers. Il s'agit du SCOCI, Service national de coordination de la lutte contre la criminalité sur Internet. La Confédération doit poursuivre sur cette voie en collaboration avec les cantons.
- En outre, la Confédération devrait avoir la possibilité, dans certains cas, de mener elle-même les procédures pénales requises en référence au projet dit « d'Efficacité » [279] (Art. 340ter (nouveau) CP ; cf. chapitre 9, notamment ch. 9.4).

11.3 Autres aspects

Bien qu'elle ait examiné en priorité les problèmes de droit pénal, la commission d'experts n'a pas ignoré les autres aspects de la cybercriminalité qui existent en parallèle au droit pénal ou qui en découlent :

11.31 Contrôles techniques d'Internet (cf. chapitre 3)

Il est techniquement possible, du moins en partie, de contrôler l'accès à Internet et les contenus mis en ligne. Mais Internet ayant été conçu sur une base décentralisée et devant garantir une haute disponibilité, ces contrôles requièrent de très gros moyens. Pour la même raison, il est relativement facile de tourner les mesures de contrôle et de blocage.

11.32 Mesures de droit administratif (cf. chapitre 7)

On pourrait envisager des mesures de droit administratif qui, en complément des dispositions pénales, préviendraient les violations des biens juridiquement protégés sur les réseaux de communications électroniques. Le droit en vigueur n'offre aucune base adéquate. Toutefois, ces mesures se heurteraient pour la plupart à des limites pratiques ou constitutionnelles, surtout celles qui découlent des droits fondamentaux de la libre communication et du principe constitutionnel de la proportionnalité des interventions des autorités (cf. à ce propos également chapitre 5). La commission d'experts n'a donc pas opté, dans ses propositions, pour des mesures d'accompagnement de droit administratif.

11.33 Droit civil (cf. chapitre 8*)*

Le droit pénal et la responsabilité civile présentent certes divers points de convergence dans le contexte de la cybercriminalité. Mais des différences les séparent aussi qui proviennent essentiellement d'une conception différente de la faute (surtout eu égard aux prétentions en cessation ou suppression du trouble à raison de la faute, qui existent en droit civil, et à certains points spécifiques à la procédure civile).

---

[279] Mesures tendant à l'amélioration de l'efficacité et de la légalité dans la poursuite pénale (Message FF 1998, 1253 ss. Modification du code pénal du 22.12.1999, en vigueur depuis le 1er janvier 2002, RO 2001, 3071).

La commission estime souhaitable que certaines questions qui se posent dans le présent contexte soient résolues par le législateur. Elle est néanmoins d’avis que le cadre ad hoc doit être recherché dans les projets de loi et les projets de révision en cours (par ex. législation sur le commerce électronique ou révision et unification du droit de la responsabilité civile).

Annexe

A - Modification du code pénal proposé dans la motion Pfisterer (Développement)

6. Punissabilité des réseaux de télécommunication et des médias

Art. 27 Punissabilité des médias

[1] Lorsqu'une infraction aura été commise et consommée sous forme de publication par un média, l'auteur sera seul punissable, sous réserve de l'article 27ter et des dispositions suivantes.

Al. 2 à 4 inchangés.

Art. 27bis Protection des sources

Inchangé

Art. 27ter Punissabilité des réseaux

[1] Lorsqu'une infraction aura été commise par voie de transmission, de préparation ou de mise à disposition d'informations, notamment de contenus, par un réseau de télécommunication, le fournisseur de ces informations sera seul punissable, sous réserve des dispositions suivantes. Si le fournisseur effectue un contrôle rédactionnel de l'information au sens de l'article 27 alinéa 2 CP, il est punissable conformément aux articles 27 et 322bis. 322bis.

[2] Lorsqu'une infraction aura été commise au moyen d'informations, notamment de contenus, d'origine étrangère, celui qui met des informations à disposition sur un réseau de télécommunication n'est punissable que lorsqu'il néglige sciemment d'empêcher la transmission de ces informations, alors même qu'il est techniquement à même de le faire et qu'une telle mesure peut raisonnablement être attendue de lui.

[3] Celui qui se borne à fournir l'accès à des informations, et notamment à des contenus, d'origine étrangère, sur un réseau de télécommunication, n'est pas punissable dans la mesure où :
a. il n'a pas occasionné la transmission des informations;
b. il n'a pas sélectionné les destinataires des informations transmises;
c. il n'a pas sélectionné ou modifié les informations transmises.
Un enregistrement automatique et pour une brève durée d'informations d'origine étrangère par suite d'une transmission automatique est considéré comme une fourniture d'accès.
Art. 27^{quater} Réserve d'autres lois

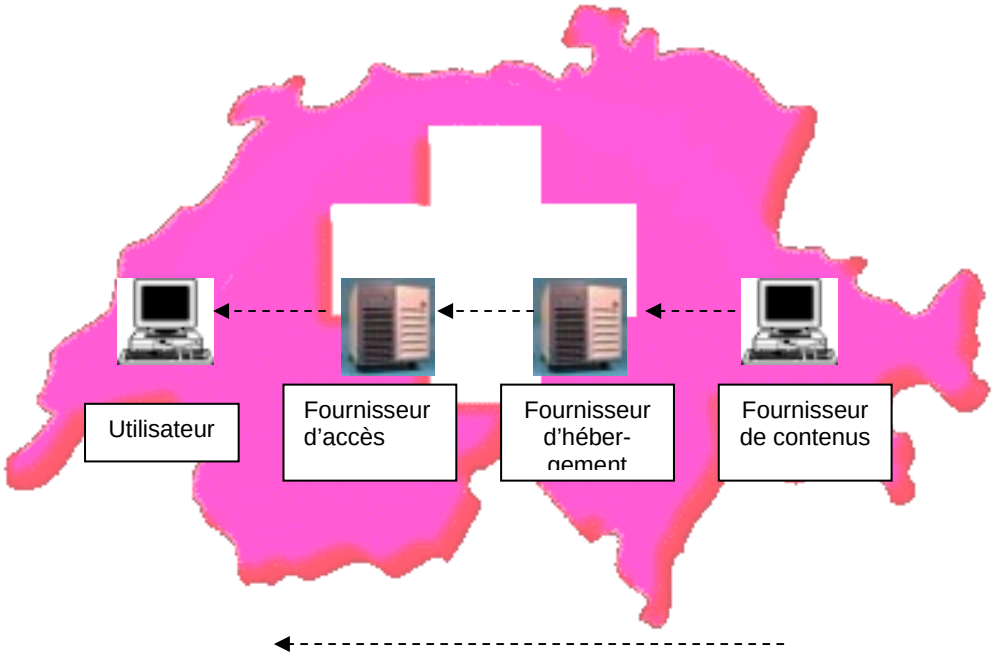
L'article 27ter règle de manière exhaustive la responsabilité pénale sur les réseaux de télécommunication. Les obligations liées à la suppression ou au blocage de l'accès à des informations, conformément à la législation générale de la Confédération et des cantons, ne sont pas touchées lorsque les personnes visées à l'article 27ter prennent licitement connaissance de ces informations, qu'une mesure de blocage est techniquement possible et qu'on peut raisonnablement attendre d'elles qu'elles prennent une telle mesure.

Art. 340ter

Sont soumis à la juridiction fédérale d'autres actes punissables sur les réseaux de télécommunication (art. 27ter et 27quater).

B - Etudes de cas en relation avec le chapitre 6, ch. 6.4

Situation 1 : tous les acteurs sont en Suisse



1 <u>Cas 1</u> : fichier-image de pornographie enfantine sur la Toile 1

• ***Applicabilité du droit pénal des médias*** : non (Tribunal fédéral), doctrine néanmoins en majorité divergente (cf. plus haut ch. 6.2).
• ***Fournisseur de contenus*** : lieu d'exécution de l'acte en Suisse, donc compétence juridictionnelle donnée en vertu du principe de la territorialité (cf. plus haut ch. 6.41); auteur principal de l'infraction pour accessibilité selon l'art. 197, ch. 3 CP.
• ***Fournisseur d'hébergement*** : auteur (médiat) pour accessibilité selon l'art. 197, ch. 3 CP ou complicité pour contribution à l'encouragement de l'acte principal (les deux variantes à clarifier, cf. plus haut ch. 6.3). Dans les deux variantes : compétence juridictionnelle donnée en vertu du principe de la territorialité (cf. plus haut ch. 6.41).
• ***Fournisseur d'accès*** : auteur (médiat) pour accessibilité selon l'art. 197, ch. 3 CP ou complicité pour contribution à l'encouragement de l'acte principal (les deux options à rejeter, néanmoins à clarifier, cf. plus haut ch. 6.3). Dans les deux variantes : compétence juridictionnelle donnée en vertu du principe de la territorialité (cf. plus haut ch. 6.41).
• ***Utilisateur*** : auteur principal si le fichier-image est stocké sur son disque dur (possession de pornographie enfantine, art. 197, ch. 3bis CP). Lieu d'exécution de l'acte en Suisse, donc compétence juridictionnelle donnée en vertu du principe de la territorialité (cf. plus haut ch. 6.41).

1 Cas 2 : provocation à l'incendie volontaire dans un forum de discussion

• ***Applicabilité du droit pénal des médias*** : oui (cf. plus haut ch. 6.1).
• ***Fournisseur de contenus*** : auteur principal de l'infraction pour provocation publique selon l'art. 259, al. 1 CP. Lieu d'exécution de l'acte en Suisse, donc compétence juridictionnelle donnée en vertu du principe de la territorialité (cf. plus haut ch. 6.41);
• ***Fournisseur d'hébergement*** : l'applicabilité du droit pénal des médias dépend de la question de savoir si le fournisseur d'hébergement tombe sous le coup de l'art. 27 CP en tant que diffuseur ; si oui, il n'est pas punissable car l'auteur peut être poursuivi; si non, la complicité pour contribution à l'encouragement de l'acte principal entre en considération (à clarifier, cf. plus haut ch. 6.3). En raison de l'accessoirité de la complicité, appréciation selon le droit du lieu d'exécution de l'acte principal (Suisse), donc compétence juridictionnelle donnée en vertu du principe de la territorialité (cf. plus haut ch. 6.41).
• ***Fournisseur d'accès*** : l'applicabilité du droit pénal des médias dépend de la question de savoir si le fournisseur d'accès tombe sous le coup de l'art. 27 CP ; si oui, il n'est pas punissable car l'auteur peut être poursuivi; si non, la complicité pour contribution à l'encouragement de l'acte principal entre en considération (à rejeter, cf. plus haut ch. 6.3). En raison de l'accessoirité de la complicité, appréciation selon le droit du lieu d'exécution de l'acte principal (Suisse), donc compétence juridictionnelle donnée en vertu du principe de la territorialité (cf. plus haut ch. 6.41).
• ***Utilisateur*** : non punissable.

1 Cas 3 : textes discriminatoires sur la Toile

• ***Applicabilité du droit pénal des médias*** : à clarifier (plutôt à rejeter) [280].
• ***Fournisseur de contenus*** : doutes sur sa qualité d'auteur principal de l'infraction pour diffusion publique selon l'art. 261bis, al. 2 CP [281]. Lieu d'exécution de l'acte en Suisse, donc compétence juridictionnelle donnée en vertu du principe de la territorialité (cf. plus haut ch. 6.41).
• ***Fournisseur d'hébergement*** : appréciation selon le droit pénal suisse dans la mesure où une variante distincte de l'acte selon art. 261bis, al. 3 CP par encouragement de l'acte principal est admise (à clarifier, cf. plus haut ch. 6.3). Si la complicité est admise, il y a accessoirité envers l'acte principal, c'est-à-dire appréciation selon le droit du lieu où l'acte principal a été exécuté (Suisse).
• ***Fournisseur d'accès*** : appréciation selon le droit pénal suisse dans la mesure où une variante distincte de l'acte selon art. 261bis, al. 3 CP par encouragement de l'acte principal est admise (à clarifier, cf. plus haut ch. 6.3). Si la complicité est admise, il y

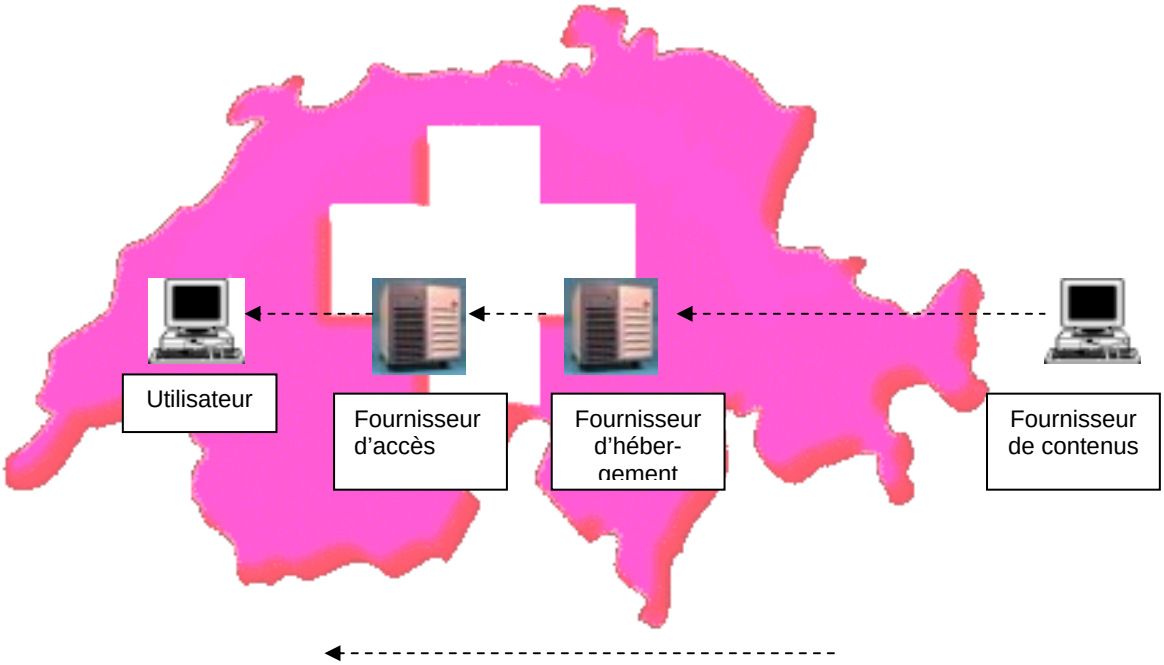
---

[280] En résumé sur les opinions contradictoires à ce propos RIKLIN/STRATENWERTH (Bibl.), p. 15 avec renvois. Dans l'ATF 125 IV 206 ss, le Tribunal fédéral ne s'est pas prononcé à propos de la classification de l'art. 261bis, al. 2 CP.

[281] En Suisse, le débat porte encore sur le fait de savoir si l'acte du diffuseur est uniquement accompli par la personne qui transmet activement des informations à un grand nombre de personnes ou si déjà la préparation sur un serveur suffit à remplir cette condition objective de l'infraction (cf. PETER VON INS/PETER-RENÉ WYDER, in : Niggli/Wiprächtiger, CP Kommentar, Bâle 2003, art. 179 n. 41 « Mitteilung, also Weitergabe an Dritte »). Aux termes d'un arrêt contesté de la BGH allemande (cour fédérale suprême), la diffusion constitue un sous-groupe de l'action de rendre accessible, à savoir l'accessibilité d'une information qui a été concrètement « appelée » au moins une fois par un utilisateur ; cf. arrêt de la BGH du 27.6.2001 - 1 StR 66/01, cons. III.3.b)bb).

a accessoirité envers l’acte principal, c’est-à-dire appréciation selon le droit du lieu où l’acte principal a été exécuté (Suisse).
• ***Utilisateur*** : non punissable.

Situation 2 **: le fournisseur de contenus agit à l'étranger, tous les autres acteurs sont en Suisse**



2 Cas 1 : fichier-image de pornographie enfantine sur la Toile 2

• ***Applicabilité du droit pénal des médias*** : non (Tribunal fédéral), doctrine néanmoins en majorité divergente (cf. plus haut ch. 6.2).
• ***Fournisseur de contenus*** : lieu d'exécution de l'acte à l'étranger; en cas de délits de mise en danger abstraite, pas de possibilité de rattachement à un résultat en Suisse, donc pas de compétence juridictionnelle en vertu du principe de la territorialité (cf. plus haut ch. 6.42), pas de compétence juridictionnelle non plus en vertu du principe de l'universalité (art. 6bis CP) [282], donc ne peut être poursuivi en Suisse ; sur requête, possibilité d'entraide judiciaire pour un autre Etat [283].
• ***Fournisseur d'hébergement*** : appréciation juridique en vertu du droit pénal suisse dans la mesure où l'hébergeur est auteur (médiat) pour accessibilité selon l'art. 197, ch. 3 CP. Dans la mesure où la complicité pour contribution à l'encouragement de l'acte principal est admise, accessoirité envers l'acte principal, donc ne peut être poursuivi en Suisse, appréciation en vertu du droit du lieu où l'acte principal a été commis (les deux variantes à rejeter; cf. plus haut ch. 6.3).
• ***Fournisseur d'accès*** : appréciation juridique en vertu du droit pénal suisse dans la mesure où le fournisseur d'accès est auteur (médiat) pour accessibilité selon l'art. 197, ch. 3 CP. Dans la mesure où il y a complicité pour contribution à l'encouragement de l'acte principal, accessoirité envers l'acte principal, donc ne peut être poursuivi en Suisse, appréciation en vertu du droit du lieu où l'acte principal a été commis (les deux options à rejeter, néanmoins à clarifier ; cf. plus haut ch. 6.3).

[282] Autrement selon l'art. 5 révisé des Dispositions générales du CP.
[283] Un rattachement au principe de la personnalité active, art. 6, ch. 1 CP, demeure encore possible, si le fournisseur de contenus est de nationalité suisse et se trouve en Suisse (après exécution de l'acte à l'étranger).

• ***Utilisateur*** : auteur principal si le fichier-image est stocké sur son disque dur (possession de pornographie enfantine, art. 197, ch. 3bis CP). Lieu d'exécution de l'acte en Suisse, donc compétence juridictionnelle donnée en vertu du principe de la territorialité (cf. plus haut ch. 6.41).

2 Cas 2 : provocation à l'incendie volontaire dans un forum de discussion

• ***Applicabilité du droit pénal des médias*** : oui (cf. plus haut ch. 6.1).
• ***Fournisseur de contenus*** : lieu d'exécution de l'acte à l'étranger; en cas de délits de mise en danger abstraite, pas de possibilité de rattachement à un résultat en Suisse, donc pas la compétence juridictionnelle en vertu du principe de la territorialité (cf. plus haut ch. 6.42), par conséquent n'est pas punissable en Suisse.
• ***Fournisseur d'hébergement*** : lieu d'exécution de l'acte en Suisse (art. 3 en liaison avec art. 7 CP), donc compétence juridictionnelle donnée en vertu du principe de la territorialité (cf. plus haut ch. 6.41); selon une opinion, punissabilité en vertu de l'art. 27, al. 2 en liaison avec l'art. 322bis CP, car on ne peut poursuivre l'auteur et que le fournisseur d'hébergement est considéré comme une personne responsable de la publication ; selon une autre opinion, le droit pénal des médias n'est pas applicable. La complicité entrant éventuellement en considération ne peut être poursuivie en Suisse; sur requête, possibilité d'entraide judiciaire pour un autre Etat. Selon un troisième avis, il n'y a pas de punissabilité en vertu de l'art. 27 CP eu égard au traitement privilégié du diffuseur (à clarifier, cf. plus haut ch. 6.43).
• ***Fournisseur d'accès*** : lieu d'exécution de l'acte en Suisse (art. 3 en liaison avec art. 7 CP), donc compétence juridictionnelle donnée en vertu du principe de la territorialité (cf. plus haut ch. 6.41); selon une opinion, pas de punissabilité en vertu de l'art. 27, al. 2 CP car le fournisseur d'hébergement peut être poursuivi ; selon une autre opinion, le droit pénal des médias n'est pas applicable. La complicité entrant éventuellement en considération ne peut être poursuivie en Suisse ; sur requête, possibilité d'entraide judiciaire pour un autre Etat. Selon un troisième avis, il n'y a pas de punissabilité en vertu de l'art. 27 CP eu égard au traitement privilégié du diffuseur (à clarifier, cf. plus haut ch. 6.43).
• ***Utilisateur*** : non punissable.

2 Cas 3 : textes discriminatoires sur la Toile

• ***Applicabilité du droit pénal des médias*** : à clarifier (plutôt à rejeter).
• ***Fournisseur de contenus*** : lieu d'exécution de l'acte à l'étranger; en cas de pur délit formel, pas de possibilité de rattachement à un résultat en Suisse, donc pas de compétence juridictionnelle en vertu du principe de la territorialité (cf. plus haut ch. 6.42) ; de ce fait, ne peut être poursuivi en Suisse ; sur requête, possibilité d'entraide judiciaire pour un autre Etat [284].
• ***Fournisseur d'hébergement*** : appréciation selon le droit pénal suisse dans la mesure où est admise une variante distincte de l'acte selon l'art. 261bis, al. 3 CP par

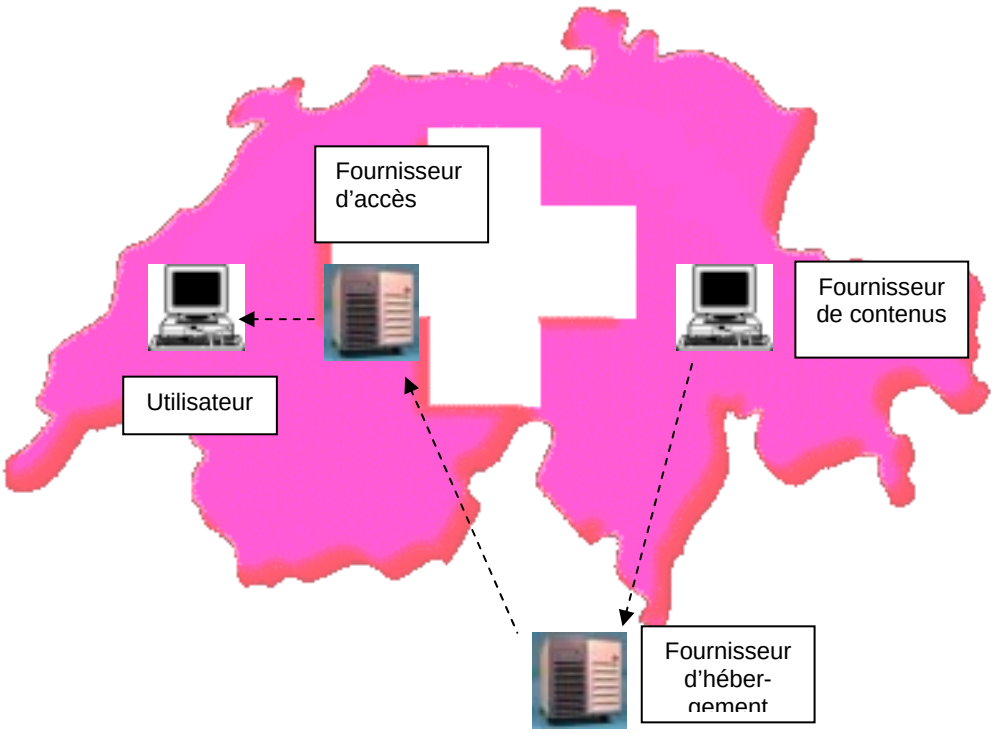
[284] A.M. SCHWARZENEGGER, ABSTRAKTE GEFAHR (Bibl.), p. 252. Cf. à propos de la doctrine allemande selon laquelle les délits d'expression ont tous valeur de délit matériel, raison pour laquelle un rattachement au résultat au sens du § 9, al. 1 3. Alt. du code pénal allemand est possible, THOMAS FUHR: Die Äusserung im Strafgesetzbuch, Berlin 2001, 175 ss et 188 ss avec renvois; THEODOR LENCKNER – in: Schönke/Schröder, Strafgesetzbuch, Kommentar, 26^{e} édition, Munich 2001, § 185 n. 12 et § 186 n. 8 in fine à l'exemple de l'outrage et de la diffamation.

encouragement de l'acte principal (à clarifier, cf. plus haut ch. 6.3). Si la complicité est admise, il y a accessoirité envers l'acte principal, c'est-à-dire appréciation selon le droit du lieu où l'acte principal a été exécuté, pas de compétence juridictionnelle de la Suisse.

• ***Fournisseur d'accès*** : appréciation selon le droit pénal suisse dans la mesure où est admise une variante distincte de l'acte selon l'art. 261bis, al. 3 CP par encouragement de l'acte principal. Si la complicité est admise, il y a accessoirité envers l'acte principal, c'est-à-dire appréciation selon le droit du lieu où l'acte principal a été exécuté, pas de compétence juridictionnelle de la Suisse (les deux options à rejeter, à clarifier, cf. plus haut ch. 6.3).

• ***Utilisateur*** : non punissable.

<u>Situation 3</u> : le fournisseur d'hébergement agit à l'étranger, les autres acteurs en Suisse



Chemin parcouru par les contenus/données

3 <u>Cas 1</u> : fichier-image de pornographie enfantine sur la Toile 3

• ***Applicabilité du droit pénal des médias*** : non (Tribunal fédéral), doctrine néanmoins en majorité divergente (cf. plus haut ch. 6.2).
• ***Fournisseur de contenus*** : lieu d'exécution de l'acte en Suisse, donc compétence juridictionnelle donnée en vertu du principe de la territorialité (cf. plus haut ch. 6.41); auteur principal de l'infraction pour accessibilité selon l'art. 197, ch. 3 CP.
• ***Fournisseur d'hébergement*** : appréciation juridique en vertu du droit où l'acte a été commis, c'est-à-dire l'étranger, dans la mesure où le fournisseur d'accès est auteur (médiat) pour accessibilité selon l'art. 197, ch. 3 CP, pas de compétence juridictionnelle de la Suisse. Dans la mesure où il y a complicité pour contribution à l'encouragement de l'acte principal, accessoirité envers l'acte principal, c'est-à-dire appréciation en vertu du droit pénal suisse (à clarifier dans les deux cas; cf. plus haut ch. 6.3) [285].
• ***Fournisseur d'accès*** : appréciation juridique en vertu du droit pénal suisse dans la mesure où le fournisseur d'accès est auteur (médiat) pour accessibilité selon l'art. 197, ch. 3 CP. Dans la mesure où il y a complicité pour contribution à l'encouragement de l'acte principal, accessoirité envers l'acte principal, c'est-à-dire

[285] Une autre possibilité est offerte par le rattachement au principe de la personnalité active, art. 6, ch. 1 CP au cas où le ressortissant suisse responsable du serveur web est et séjourne en Suisse.

appréciation également en vertu du droit suisse (les deux options à rejeter, néanmoins à clarifier ; cf. plus haut ch. 6.3)
• ***Utilisateur*** : auteur principal si le fichier-image est stocké sur son disque dur (possession de pornographie enfantine, art. 197, ch. 3bis CP). Lieu d'exécution de l'acte en Suisse, donc compétence juridictionnelle donnée en vertu du principe de la territorialité (cf. plus haut ch. 6.41).

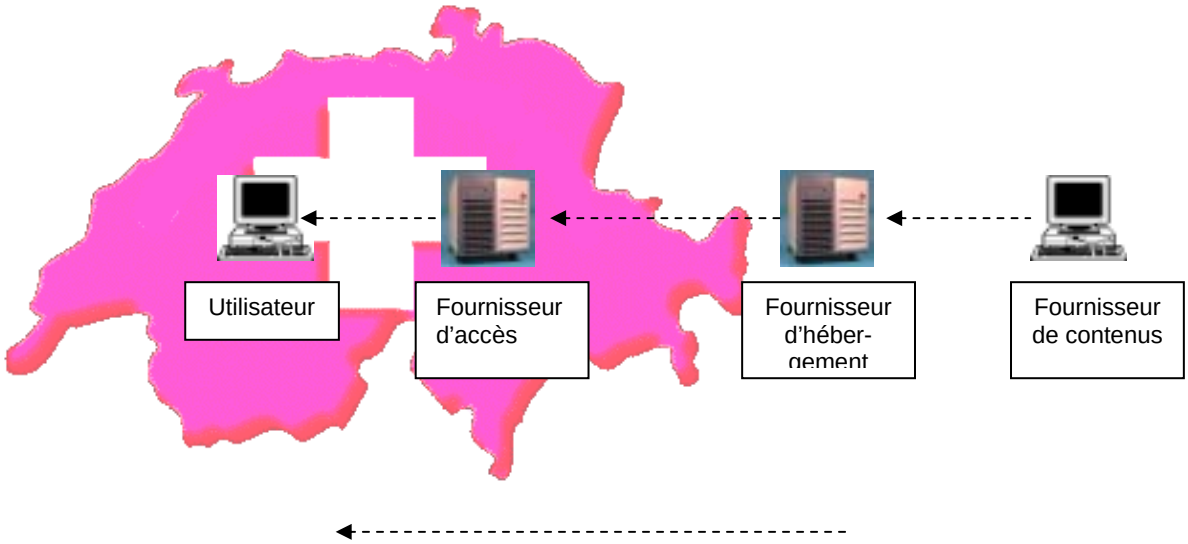
3 Cas 2 : provocation à l'incendie volontaire dans un forum de discussion

• ***Applicabilité du droit pénal des médias*** : oui (cf. plus haut ch. 6.1).
• ***Fournisseur de contenus*** : lieu d'exécution de l'acte en Suisse, donc compétence juridictionnelle donnée en vertu du principe de la territorialité (cf. plus haut ch. 6.41); auteur principal de l'infraction pour provocation publique en vertu de l'art. 259, al. 1 CP.
• ***Fournisseur d'hébergement*** : dans la mesure où il y a complicité pour contribution à l'encouragement de l'acte principal, accessoirité envers l'acte principal, c'est-à-dire appréciation selon le droit suisse. Selon un autre avis, pas de punissabilité en vertu de l'art. 27 (diffuseur).
• ***Fournisseur d'accès*** : selon un avis, libération de la punissabilité en vertu de l'art. 27, al. 1 CP puisque l'auteur peut être poursuivi ; selon un autre avis, le droit pénal des médias n'est pas applicable et il n'y a pas lieu d'admettre non plus la complicité (cf. plus haut ch. 6.3).
• ***Utilisateur*** : non punissable.

3 Cas 3 : textes discriminatoires sur la Toile

• ***Applicabilité du droit pénal des médias*** : à clarifier (plutôt à rejeter).
• ***Fournisseur de contenus*** : auteur principal de l'infraction pour diffusion publique selon l'art. 261bis, al. 2 CP. Lieu d'exécution de l'acte en Suisse, donc compétence juridictionnelle donnée en vertu du principe de la territorialité (cf. plus haut ch. 6.41);
• ***Fournisseur d'hébergement*** : dans la mesure où une variante distincte de l'acte selon l'art. 261bis, al. 3 CP par encouragement de l'acte principal est admise, appréciation selon le droit du lieu d'exécution, pas de compétence juridictionnelle de la Suisse. Si la complicité est admise, accessoirité envers l'acte principal, c'est-à-dire appréciation selon le droit suisse.
• ***Fournisseur d'accès*** : dans la mesure où une variante distincte de l'acte selon l'art. 261bis, al. 3 CP par encouragement de l'acte principal est admise, appréciation selon le droit pénal suisse. Dans la mesure où il y a complicité pour contribution à l'encouragement de l'acte principal, accessoirité à l'égard de l'acte principal, c'est-à-dire appréciation également en vertu du droit suisse (les deux options à rejeter).
• ***Utilisateur*** : non punissable.

<u>Situation 4</u> : le fournisseur de contenus et le fournisseur d'hébergement agissent à l'étranger, le fournisseur d'accès et l'utilisateur agissent en Suisse



4 <u>Cas 1</u> : fichier-image de pornographie enfantine sur la Toile

• ***Applicabilité du droit pénal des médias*** : non (Tribunal fédéral), doctrine néanmoins en majorité divergente (cf. plus haut ch. 6.2).
• ***Fournisseur de contenus*** : lieu d'exécution de l'acte à l'étranger; en cas de délits de mise en danger abstraite, pas de possibilité de rattachement à un résultat en Suisse, donc pas de compétence juridictionnelle en vertu du principe de la territorialité (cf. plus haut ch. 6.42), pas de compétence juridictionnelle non plus en vertu du principe de l'universalité (art. 6bis CP) [286], donc ne peut être poursuivi en Suisse ; sur requête, possibilité d'entraide judiciaire pour un autre Etat [287].
• ***Fournisseur d'hébergement*** : lieu d'exécution de l'acte à l'étranger; en cas de délits de mise en danger abstraite, pas de possibilité de rattachement à un résultat en Suisse, donc pas de compétence juridictionnelle en vertu du principe de la territorialité (cf. plus haut ch. 6.42) ; par conséquent, en Suisse, seule l'entraide judiciaire est possible.
• ***Fournisseur d'accès*** : dans la mesure où le fournisseur d'accès est auteur médiat pour accessibilité selon l'art. 197, ch. 3 CP (à rejeter, mais reste à clarifier, cf. plus haut ch. 6.3), applicabilité du code pénal suisse. Dans la mesure où la complicité pour contribution à l'encouragement de l'acte principal est admise, accessoirité envers l'acte principal, appréciation en vertu du droit du lieu où l'acte principal a été exécuté, pas de compétence juridictionnelle de la Suisse. Seule l'entraide judiciaire est possible.
• ***Utilisateur*** : auteur principal si le fichier-image est stocké sur son disque dur (possession de pornographie enfantine, art. 197, ch. 3bis CP). Lieu d'exécution de l'acte en Suisse, donc compétence juridictionnelle donnée en vertu du principe de la territorialité (cf. plus haut ch. 6.41).

---

[286] Une autre possibilité est le rattachement au principe de la personnalité active, art. 6, ch. 1 CP au cas où le ressortissant suisse responsable du serveur web est et séjourne en Suisse.
[287] Autrement selon l'art. 5 des Dispositions générales révisées du code pénal.

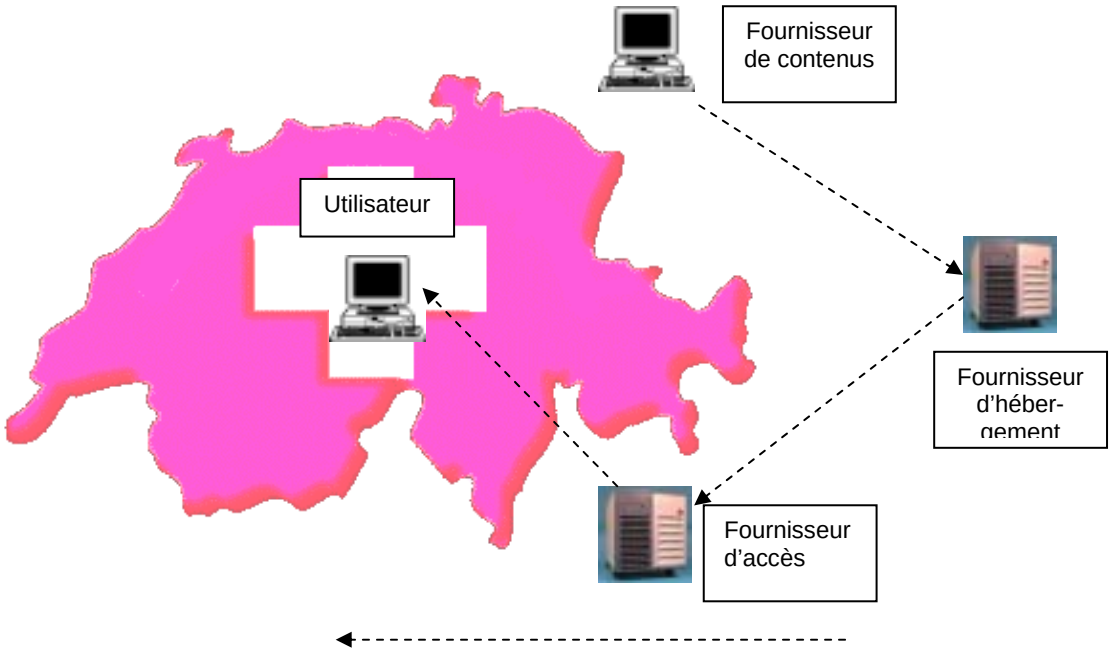
4 Cas 2 : provocation à l'incendie volontaire dans un forum de discussion

• ***Applicabilité du droit pénal des médias*** : oui (cf. plus haut ch. 6.1).
• ***Fournisseur de contenus*** : lieu d'exécution de l'acte à l'étranger; donc pas compétence juridictionnelle en vertu du principe de la territorialité (cf. plus haut ch. 6.42), donc ne peut être poursuivi en Suisse ; sur requête, possibilité d'entraide judiciaire pour un autre Etat.
• ***Fournisseur d'hébergement*** : lieu d'exécution de l'acte à l'étranger; en cas de délits de mise en danger abstraite, pas de possibilité de rattachement à un résultat en Suisse, donc pas de compétence juridictionnelle donnée en vertu du principe de la territorialité (cf. plus haut ch. 6.42) ; de ce fait, en Suisse, seule l'entraide judiciaire est possible.
• ***Fournisseur d'accès*** : lieu d'exécution de l'acte en Suisse, donc compétence juridictionnelle donnée en vertu du principe de la territorialité (cf. plus haut ch. 6.41); selon un avis, punissabilité selon l'art. 27, al. 2 en liaison avec l'art. 322bis CP, étant donné que l'auteur et le fournisseur d'hébergement ne peuvent être poursuivis et que le fournisseur d'accès est considéré comme une personne responsable de la publication ; selon un autre avis, le droit pénal des médias n'est pas applicable, même la complicité entrant éventuellement en considération ne pourrait pas être poursuivie ; sur requête, possibilité d'entraide judiciaire pour un autre Etat. Selon encore un autre avis, le fournisseur d'accès est exclu de la punissabilité d'une manière générale en vertu de l'art. 27 CP (en tant que diffuseur) (à clarifier, cf. plus haut ch. 6.43).
• ***Utilisateur*** : non punissable.

4 Cas 3 : textes discriminatoires sur la Toile

• ***Applicabilité du droit pénal des médias*** : à clarifier (plutôt à rejeter).
• ***Fournisseur de contenus*** : lieu d'exécution de l'acte à l'étranger; en cas de purs délits formels, pas de possibilité de rattachement à un résultat en Suisse, donc pas de compétence juridictionnelle en vertu du principe de la territorialité (cf. plus haut ch. 6.42), par conséquent ne peut être poursuivi en Suisse ; sur requête, possibilité d'entraide judiciaire pour un autre Etat.
• ***Fournisseur d'hébergement*** : lieu d'exécution de l'acte à l'étranger; en cas de pur délit formel, pas de possibilité de rattachement à un résultat en Suisse, donc pas de compétence juridictionnelle en vertu du principe de la territorialité (cf. plus haut ch. 6.42), par conséquent ne peut être poursuivi en Suisse ; sur requête, possibilité d'entraide judiciaire pour un autre Etat.
• ***Fournisseur d'accès*** : dans la mesure où une variante distincte de l'acte selon art. 261bis, al. 3 CP par encouragement de l'acte principal est admise (à clarifier, cf. plus haut ch. 6.3), lieu d'exécution de l'acte en Suisse, donc compétence juridictionnelle donnée en vertu du principe de la territorialité (cf. plus haut ch. 6.41). Dans la mesure où la complicité pour contribution à l'encouragement de l'acte principal est admise, accessoirité envers l'acte principal, c'est-à-dire appréciation selon le droit du lieu où l'acte principal a été exécuté, pas de compétence juridictionnelle de la Suisse. Possibilité d'entraide judiciaire.
• ***Utilisateur*** : non punissable.

Situation 5 : seul l'utilisateur agit en Suisse, tous les autres acteurs agissent à l'étranger



5 Cas 1 : fichier-image de pornographie enfantine sur la Toile

• ***Applicabilité du droit pénal des médias*** : non (Tribunal fédéral), doctrine néanmoins en majorité divergente (cf. plus haut ch. 6.2).
• ***Fournisseur de contenus*** : lieu d'exécution de l'acte à l'étranger; en cas de délits de mise en danger abstraite, pas de possibilité de rattachement à un résultat en Suisse, donc pas de compétence juridictionnelle en vertu du principe de la territorialité (cf. plus haut ch. 6.42), pas de compétence juridictionnelle non plus en vertu du principe de l'universalité (art. 6bis CP) [288], donc ne peut être poursuivi en Suisse ; sur requête, possibilité d'entraide judiciaire pour un autre Etat [289].
• ***Fournisseur d'hébergement*** : situation identique à celle du fournisseur de contenus.
• ***Fournisseur d'accès*** : situation identique à celle du fournisseur de contenus.
• ***Utilisateur*** : auteur principal si le fichier-image est stocké sur son disque dur (possession de pornographie enfantine, art. 197, ch. 3bis CP). Lieu d'exécution de l'acte en Suisse, donc compétence juridictionnelle donnée en vertu du principe de la territorialité (cf. plus haut ch. 6.41).

5 Cas 2 : provocation à l'incendie volontaire dans un forum de discussion

• ***Applicabilité du droit pénal des médias*** : oui (cf. plus haut ch. 6.1).
• ***Fournisseur de contenus*** : lieu d'exécution de l'acte à l'étranger; en cas de délits de mise en danger abstraite, pas de possibilité de rattachement à un résultat en

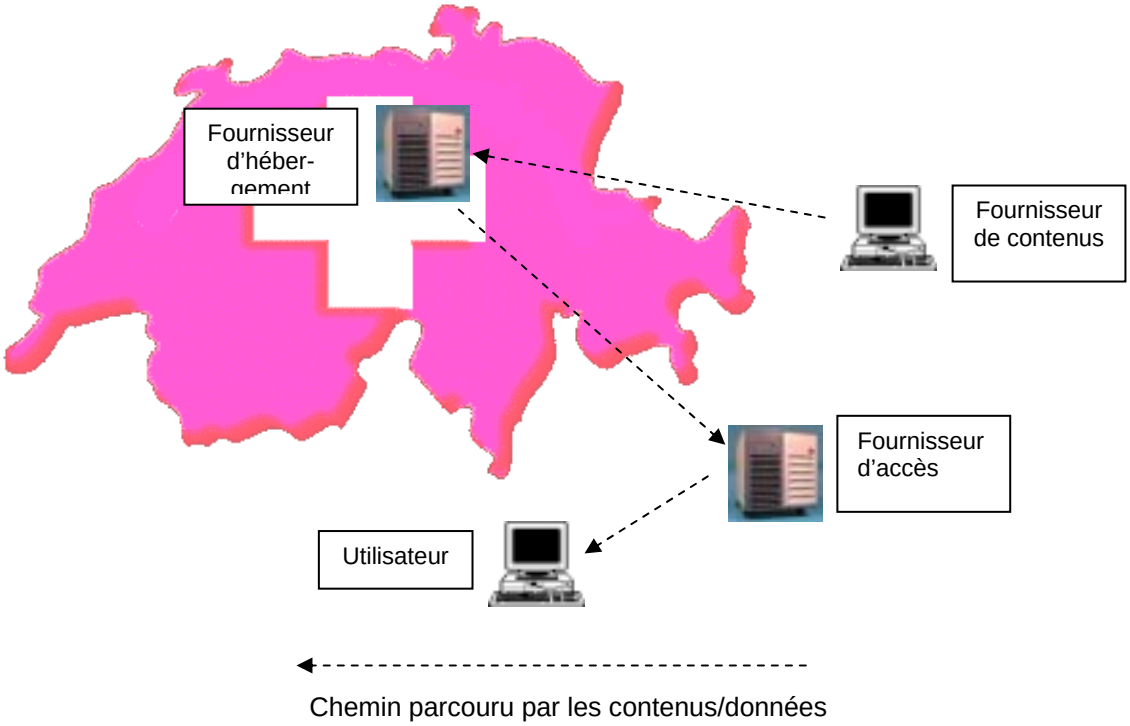
[288] Une autre possibilité est le rattachement au principe de la personnalité active, art. 6, ch. 1 CP au cas où le ressortissant suisse responsable du serveur web est et séjourne en Suisse.
[289] Autrement selon l'art. 5 des Dispositions générales révisées du code pénal.

Suisse, donc pas de compétence juridictionnelle en vertu du principe de la territorialité (cf. plus haut ch. 6.42), par conséquent ne peut être poursuivi en Suisse ; sur requête, possibilité d'entraide judiciaire pour un autre Etat.
• ***Fournisseur d'hébergement*** : situation identique à celle du fournisseur de contenus.
• ***Fournisseur d'accès*** : situation identique à celle du fournisseur de contenus.
• ***Utilisateur*** : non punissable.

5 <u>Cas 3</u> : textes discriminatoires sur la Toile

• ***Applicabilité du droit pénal des médias*** : à clarifier (plutôt à rejeter).
• ***Fournisseur de contenus*** : lieu d'exécution de l'acte à l'étranger; en cas de purs délits formels, pas de possibilité de rattachement à un résultat en Suisse, donc pas de compétence juridictionnelle en vertu du principe de la territorialité (cf. plus haut ch. 6.42), par conséquent ne peut être poursuivi en Suisse ; sur requête, possibilité d'entraide judiciaire pour un autre Etat.
• ***Fournisseur d'hébergement*** : situation identique à celle du fournisseur de contenus.
• ***Fournisseur d'accès*** : situation identique à celle du fournisseur de contenus.
• ***Utilisateur*** : non punissable.

Situation 6 : seul le fournisseur d'hébergement agit en Suisse, tous les autres acteurs agissent à l'étranger



6 Cas 1 : fichier-image de pornographie enfantine sur la Toile

• ***Applicabilité du droit pénal des médias*** : non (Tribunal fédéral), doctrine néanmoins en majorité divergente (cf. plus haut ch. 6.2).
• ***Fournisseur de contenus*** : lieu d'exécution de l'acte à l'étranger; en cas de délits de mise en danger abstraite, pas de possibilité de rattachement à un résultat en Suisse, donc pas de compétence juridictionnelle en vertu du principe de la territorialité (cf. plus haut ch. 6.42), pas de compétence juridictionnelle non plus en vertu du principe de l'universalité (art. 6bis CP), donc ne peut être poursuivi en Suisse ; sur requête, possibilité d'entraide judiciaire pour un autre Etat.
• ***Fournisseur d'hébergement*** : appréciation juridique en vertu du droit pénal suisse dans la mesure où il est admis que le fournisseur d'hébergement est auteur (médiat) pour accessibilité selon l'art. 197, ch. 3 CP. Dans la mesure où la complicité pour contribution à l'encouragement de l'acte principal est admise, accessoirité envers l'acte principal, c'est-à-dire ne peut être poursuivi en Suisse, appréciation en vertu du droit du lieu où l'acte principal a été commis (les deux options à clarifier ; cf. plus haut ch. 6.3).
• ***Fournisseur d'accès*** : situation identique à celle du fournisseur de contenus.
• ***Utilisateur*** : lieu d'exécution de l'acte à l'étranger (possession), donc pas decompétence juridictionnelle en vertu du principe de la territorialité; ne peut être poursuivi en Suisse.

6 Cas 2 : provocation à l'incendie volontaire dans un forum de discussion

• ***Applicabilité du droit pénal des médias*** : oui (cf. plus haut ch. 6.1).

• ***Fournisseur de contenus*** : lieu d'exécution de l'acte à l'étranger; en cas de délits de mise en danger abstraite, pas de possibilité de rattachement à un résultat en Suisse, donc pas de compétence juridictionnelle en vertu du principe de la territorialité (cf. plus haut ch. 6.42), par conséquent ne peut être poursuivi en Suisse ; sur requête, possibilité d'entraide judiciaire pour un autre Etat.
• ***Fournisseur d'hébergement*** : selon un avis, punissabilité en vertu de l'art. 27, al. 2 en liaison avec l'art. 322bis CP, puisqu'on ne peut poursuivre l'auteur et que le fournisseur d'hébergement est considéré comme une personne responsable de la publication ; selon un autre avis, le droit pénal des médias n'est pas applicable, même la complicité entrant éventuellement en considération ne peut être poursuivie en Suisse ; selon encore un autre avis, le fournisseur d'hébergement est toujours impuni en tant que diffuseur en cas de délits de média (à clarifier, cf. plus haut ch. 6.43).
• ***Fournisseur d'accès*** : situation identique à celle du fournisseur de contenus.
• ***Utilisateur*** : non punissable.

6 <u>Cas 3</u> : textes discriminatoires sur la Toile

• ***Applicabilité du droit pénal des médias*** : à clarifier (plutôt à rejeter).
• ***Fournisseur de contenus*** : lieu d'exécution de l'acte à l'étranger; en cas de purs délits formels, pas de possibilité de rattachement à un résultat en Suisse, donc pas de compétence juridictionnelle en vertu du principe de la territorialité (cf. plus haut ch. 6.42), par conséquent ne peut être poursuivi en Suisse ; sur requête, possibilité d'entraide judiciaire pour un autre Etat.
• ***Fournisseur d'hébergement*** : appréciation selon le droit pénal suisse dans la mesure où est admise une variante distincte de l'acte selon art. 261bis, al. 3 CP par encouragement de l'acte principal (à clarifier, cf. plus haut ch. 6.3). Si la complicité est admise, il y a accessoirité envers l'acte principal, c'est-à-dire appréciation selon le droit du lieu où l'acte principal a été exécuté, pas de compétence juridictionnelle de la Suisse
• ***Fournisseur d'accès*** : situation identique à celle du fournisseur de contenus
• ***Utilisateur*** : non punissable.