Die strafrechtliche Verantwortung von Internet Service Providern

Positionspapier der Bundespolizei, April 2000

1. Vorbemerkung

Am 23. Juli 1998 versandte die Bundespolizei ein Rundschreiben an Internet Service Provider (ISP) in der Schweiz mit dem Ersuchen, die Sperrung bestimmter Sites, welche rassendiskriminierende Inhalte im Sinne von Art. 261bis des schweizerischen Strafgesetzbuches[1] (StGB) aufweisen, zu prüfen. Begründet wurde das Ersuchen mit dem Hinweis, dass die Ermöglichung des Zugangs für Nutzer auf solche Sites als Gehilfenschaft (Art. 25 StGB) zur Haupttat qualifiziert werden kann. Das Rundschreiben löste relativ starke Reaktionen von Seiten der ISP aus, was dazu führte, dass eine Kontaktgruppe gegründet wurde, welche versuchen sollte, die verschiedenen Interessen der ISP einerseits und der Polizeibehörden des Bundes andererseits auf einen gemeinsamen Nenner zu bringen. **Die Kontaktgruppe besteht zurzeit einerseits aus einer repräsentativen Vertretung der Schweizer ISP sowie aus Vertretern der Bundesämter für Informatik, für Kommunikation, für Justiz, und für Polizei.**

Bestrebungen, welche darauf abzielen, dass rechtswidrige Inhalte im Internet weder veröffentlicht, noch abgerufen werden können, haben gleichzeitig zu berücksichtigen, dass **legitime Kommunikationsbedürfnisse** im Internet ohne Behinderung befriedigt werden können[2]. Weiter gilt es, das **Interesse der Wirtschaft** am Standort Schweiz, und damit an international vergleichbaren Rahmenbedingungen zu fördern[3], unter Berücksichtigung des **gesetzlichen Auftrags von Polizei- und Justizbehörden**, im Internet begangene Delikte zu verfolgen oder solche zu verhindern[4]. Dabei ist zu beachten, dass viele Delikte von Amtes wegen zu verfolgen sind und dass die Verfolgungs- und Beurteilungskompetenz bezüglich eines grossen Teils der Straftatbestände **den Kantonen zugewiesen** ist.

Das vorliegende Positionspapier soll dazu dienen, **grundsätzliche Fragen zur strafrechtlichen Haftung der ISP zu beantworten und mögliche Wege zur Zusammenarbeit mit Strafverfolgungsbehörden aufzuzeigen.** Es ist als Ergänzung zu verstehen zum Bericht einer interdepartementalen Arbeitsgruppe vom Mai 1996.[5]

Nachdem ein erster Entwurf des Positionspapiers den Kontaktgruppenmitgliedern zur Vernehmlassung zugestellt wurde, drängte sich die **gutachtliche Prüfung der**

---

[1] SR 311.0

[2] vgl. die Meinungs- und Informationsfreiheit gemäss Art. 16 der Bundesverfassung vom 18.4.1999 (BV), in Kraft seit dem 1.1.2000

[3] vgl. etwa den federführend vom Staatssekretariat für Wirtschaft (seco) verfassten Aktionsplan zur Förderung des elektronischen Geschäftsverkehrs

[4] Die verfassungsmässig garantierte Wirtschaftsfreiheit (Art. 27 und 94 BV) darf nur in dem von Art. 36 BV vorgezeichneten Rahmen eingeschränkt werden; vorliegend in erster Linie durch die formellgesetzlichen Bestimmungen des StGB

[5] Internet, Neues Medium, neue Fragen ans Recht; Bericht einer interdepartementalen Arbeitsgruppe zu strafrechtlichen, datenschutzrechtlichen und urheberrechtlichen Fragen rund um Internet. (http://www.bj.admin.ch/themen/ri-ir/internet/rf-internet-d.pdf).

Frage der strafrechtlichen Verantwortlichkeit von Internet-Access-Providern gemäss Art. 27 und 322bis StGB auf. Das Gutachten ist in der Zwischenzeit vom Bundesamt für Justiz (BJ) erstellt und in der Kontaktgruppe verteilt worden[6]. Nachfolgend wird an geeigneter Stelle darauf eingegangen.

2. Straftaten im Internet

Das Internet spiegelt zumindest teilweise die reale Welt mit ihren faszinierenden, aber auch weniger ansprechenden Seiten. So wird das Internet mit seinen verschiedenen Diensten inzwischen für nahezu jede Art krimineller Betätigung genutzt. Im Zusammenhang mit dem vorliegenden Papier erscheint bezüglich der verschiedenen strafbaren Handlungen eine Unterscheidung in zwei Hauptgruppen sinnvoll:

- **Delikte, bei deren Begehung das Internet dem (häufig zeitlich kurzfristigen) Datentransfer dient**. Darunter fallen zunächst die eigentlichen Computerdelikte, wie unbefugte Datenbeschaffung (Art. 143 StGB), das unbefugte Eindringen in ein Datenverarbeitungssystem (Art. 143bis StGB), die Datenbeschädigung (Art. 144bis StGB), der betrügerische Missbrauch einer Datenverarbeitungsanlage (Art. 147 StGB) sowie das Erschleichen einer Leistung (Art. 150 Abs. 3 StGB). Hinzu kommen alle weiteren Delikte, bei welchen Informationen via Internet übermittelt werden, wie Urheberrechtsverletzungen, Verstösse gegen das Lotteriegesetz, Verletzung des Fabrikations- oder Geschäftsgeheimnisses (Art. 162 StGB), Verbotener Nachrichtendienst (Art. 272 ff. StGB), Geldwäscherei (Art. 305bis StGB), usw. Dieser Kategorie zugeordnet werden können auch die Beteiligungshandlungen (Mittäterschaft, Gehilfenschaft, Anstiftung) zu allen möglichen Straftatbeständen, wenn sie in der Kommunikation zwischen den Tatbeteiligten bestehen.
- **Delikte, bei deren Begehung das Internet über eine gewisse zeitliche Dauer benützt wird, indem Inhalte abrufbar gehalten werden.** Dazu gehören beispielsweise Gewaltdarstellungen (Art. 135 StGB), Betrug (Art. 146 StGB; z.B. durch arglistige Irreführung mittels einer entsprechend gestalteten Website), Pornografie (Art. 197 StGB), die als Antragsdelikte ausgebildeten Ehrverletzungen (Art. 173 ff StGB), Rassendiskriminierung (Art. 261bis StGB) sowie wiederum Urheberrechtsverletzungen[7].

Bei den Straftaten der ersten Kategorie ist diejenige Phase des Handlungsablaufs, die über das Internet erfolgt, nur im Falle einer gleichzeitigen Überwachung des Datentransfers feststellbar, d.h. eine Verhinderung oder Einschränkung des Erfolgseintritts mittels Internet-spezifischer Massnahmen ist nicht vorstellbar, sodass einzig die traditionellen Interventionsarten Erfolg versprechen.

Die zweite Kategorie ist vorliegend insofern von besonderem Interesse, als die diesbezüglichen strafbaren Handlungen häufig während einer gewissen Dauer stattfinden, sodass bei ihrer Entdeckung und anschliessender Vornahme entsprechender Gegenmassnahmen zumindest der Umfang des Taterfolgs eingeschränkt werden kann. **Bezüglich der in der Öffentlichkeit in Bezug auf das Internet am meisten diskutierten Delikte, Pornografie und Rassendiskriminierung, lässt sich fest-**

[6] Das Gutachten ist auch im Internet greifbar: http://www.bj.admin.ch/themen/ri-ir/access/intro-d.htm.
[7] vgl. Anhang 2 des Berichts einer interdepartementalen Arbeitsgruppe vom Mai 1996

halten, dass entsprechende Inhalte zum grössten Teil auf ausländischen Servern abrufbar gehalten werden[8].

Die Bekämpfung der vielfältigen Internetkriminalität kann sich nicht mit der Bereitstellung von Cyberpolizisten begnügen, sondern bedingt (zusätzlich) den konsequenten Aufbau eines spezifischen Fachwissens bei den jeweils zuständigen Strafverfolgungsbehörden.

3. Funktionsträger im Internet[9]

Die verschiedenen am Internet beteiligten Personen oder Organisationen können in folgende Gruppen unterteilt werden (wobei allerdings teilweise Abgrenzungsschwierigkeiten bestehen und einzelne Personen mehrere Funktionen wahrnehmen können):

- **Nutzer/User**: Personen, die im Internet angebotene Dienste nachfragen.
- **Carrier**: Sie betreiben die Basisinfrastruktur zur Verbindung der Teilnetze (Übertragungssysteme und Leitungen). Hierher gehören etwa Swisscom, Sunrise oder diAx[10].
- **Network-Provider**: Personen oder Organisationen, die die Basis-Übertragungsinfrastruktur (Mietleitungen) von Carriers mieten und mit Routern komplexe Netze betreiben, welche den ISP den Anschluss ans Internet ermöglichen (so z.B. ip-plus, Eunet, usw.)[11].
- **ISP**: Sie ermöglichen den Nutzern den Zugang zum Internet (im Sinne der Access-Provider-Funktion) und stellen in der Regel auch selber Dienste (z. B. über eigenen Web-, Mail- oder News-Server) zur Verfügung (z.B. Swiss Online, Bluewin, Datacomm, usw.). Vorliegend interessieren in erster Linie die Zugangsvermittlung (**Access-Provider**) und das Zurverfügungstellen von Speicherplatz auf Web-Servern (**Hosting-Provider**).
- **Online-Service-Provider** oder Online-Dienste: Sie bieten im Unterschied zu ISP vor allem ”proprietäre” Dienste (insbesondere Datenangebote) an, die sie i.d.R. auf eigenen Rechnern abspeichern und überwiegend nur von den Mitgliedern des Online-Dienstes abgerufen werden können. Daneben nehmen sie die Funktion von ISP wahr. Online-Service-Provider gelten nachfolgend bei der Nennung der ISP als mitumfasst. Bekannte Beispiele sind AOL und Compuserve.
- **Content-Provider**: Personen, die auf Servern von ISP oder Online-Diensten (oder auf eigenen Rechnern) eigene Informationen zur Verfügung stellen, wie z.B. der Autor eines Beitrages für eine Newsgroup oder ein Unternehmen, das im WWW auftritt.

---

[8] gilt namentlich für das WWW, während entsprechende Inhalte in Newsgroups häufig auch auf News-Server in der Schweiz gespiegelt werden

[9] vgl. die Ausführungen von Ulrich Sieber im Aufsatz ”Kontrollmöglichkeiten zur Verhinderung rechtswidriger Inhalte in Computernetzen”, in Computer und Recht 10/97, S. 597 sowie die Ausführungen von Andreas Ochsenbein und Peter L. Heinzmann im Aufsatz ”Strafrechtliche Aspekte im Internet”, in Kriminalistik 7/98, S. 516 f.

[10] Sowohl bezüglich der Carriers als auch der Network-Provider ist festzuhalten, dass vor allem aus Gründen des schichtenspezifischen Aufbaus der Netzwerkarchitektur strafrechtlich motivierte Kontrollmassnahmen oder Einflussnahmen bei diesen Arten von Dienstleistern nicht zur Diskussion stehen (vgl. Ulrich Sieber, ”Verantwortlichkeit im Internet”, Beck’sche Verlagsbuchhandlung, München 1999, S. 27)

[11] vgl. FN 9

4. Internet-Anwendungen (Dienste)

Je nachdem, ob eine Internet-Anwendung öffentlich ist oder der Autor einer Information nur einen von ihm bestimmten Adressatenkreis erreichen will, können die häufigsten Anwendungen wie folgt unterteilt werden:

- **Öffentlich**: WWW, allgemein zugängliche Newsgroups, FTP-Server (sofern Zugang nicht beschränkt), öffentlich zugängliche chat-Foren.
- **Nicht öffentlich** und damit dem Fernmeldegeheimnis[12] unterstehend: E-Mail[13], private-chat, Internet-Telefonie[14].

5. Arten strafrechtlicher Haftung

Das eingangs erwähnte **Gutachten des BJ** führt eingehend aus, auf Grundlage welcher Bestimmungen des StGB ein *Access*-Provider strafrechtlich verantwortlich werden kann. Die dort gemachten Erwägungen können auch dazu dienen, die strafrechtliche Verantwortlichkeit in Bezug auf die übrigen Funktionen eines ISP respektive der weiteren Funktionsträger im Internet herzuleiten.

Im Sinne einer kurzen Zusammenfassung des Gutachtens ist **auf folgende Aussagen hinzuweisen:**

- **Nicht alle Medieninhaltsdelikte führen zu einer Anwendung des Medienstrafrechts**. Insbesondere die Tatbestände der Artikel 135 (Gewaltdarstellungen), 197 (Pornografie) und 261bis StGB (Rassendiskriminierung) fallen nicht darunter[15] (Pkt. 4.3 des Gutachtens).
- Bei Medieninhaltsdelikten, die zur Anwendung des Medienstrafrechts führen, ist **grundsätzlich der Autor[16] allein strafbar**, was auch im Internet gilt (Pkt. 5.2.1 und 5.3.1).
- Nach dem System des Medienstrafrechts (Art. 27 i.V.m. Art. 322bis StGB) steht grundsätzlich **auch bei Fehlen des Autors immer eine für die Veröffentlichung verantwortliche Person** zur Verfügung. Dem möglicherweise geringeren Verschulden der in der Verantwortlichkeitsordnung weiter entfernten Person kann und muss bei der Anwendung von Art. 322bis StGB Rechnung getragen werden (Pkt. 5.2.2 a.E.).
- Der **Hosting-Provider** dürfte in Bezug auf die Funktionsträger im Internet und auf das Medienstrafrecht als allfälliger **subsidiär Verantwortlicher** im Vordergrund stehen (Pkt. 5.3.3.2).

---

[12] Art. 13 Abs. 1 BV; Art 43 Fernmeldegesetz (FMG/SR 784.10)

[13] Auf staatsrechtliche Klage der Fa. Swiss Online AG hin kam das Bundesgericht mit Entscheid vom 5.4.2000 (Aktenzeichen 1A.104/1999) zum Schluss, dass der E-Mail-Verkehr unter das Fernmeldegeheimnis fällt, weshalb er nur unter den Bedingungen nach Art. 179octies StGB überwacht werden darf (vgl. NZZ vom 6.4.2000)

[14] Die in der Regel auf Intra- oder Extranet eingerichteten Closed User Groups können ebenso als nichtöffentlich gelten. Je nach Grösse und Struktur ist innerhalb dieser Groups dennoch eine strafrechtlich relevante Öffentlichkeit, etwa im Sinne von Art. 261bis StGB, möglich

[15] der im Gutachten diesbezüglich unter dem Aktenzeichen 6S. 810-813/1998 zitierte Entscheid des Bundesgerichts ist in der Zwischenzeit unter 125 IV 206 veröffentlicht worden

[16] Im Sinne der unter Pkt. 3 aufgelisteten Funktionsträger ist dies der Content-Provider

- ”Fehlt” diese im Vordergrund stehende, subsidiär verantwortliche Person, erscheint es richtig, den **Access-Provider** als **subsidiär verantwortlich** anzusehen (Pkt. 5.3.3.3 und 5.3.4), wobei diesfalls bestimmte, allenfalls sehr enge Grenzen zu setzen sind (Pkt 5.3.3.4).
- In Bezug auf das für die **vorsätzliche Begehung** von Art. 322bis StGB notwendige Wissen um einen spezifischen Internet-Inhalt, ist es dem Access-Provider weder möglich noch zumutbar, (selber) im grossen Stil Kontrollen durchzuführen**. Hinweise Dritter** über solche Inhalte **müssen konkret sein und aus zuverlässiger Quelle stammen** (Pkt. 6.1.2).
- Das rechtlich relevante Wissen des Access-Providers bezüglich eines deliktischen Inhalts kann in der Regel erst dann angenommen werden, wenn die betreffende Information von einer **Instanz der Strafrechtspflege** ausgegangen ist, etwa von einem Untersuchungsrichter oder einem Staatsanwalt. Blosse Äusserungen von Privaten oder allgemeine Pressemeldungen dürften dagegen für die Bejahung eines vorsatzrelevanten Wissens häufig nicht genügen (Pkt. 6.1.2).
- Die vorsätzliche Erfüllung von Art. 322bis StGB durch einen Access-Provider ist zwar möglich, dürfte in der Praxis jedoch nicht häufig auftreten. **Häufiger** können Fälle sein, in welchen mit **Eventualvorsatz** gehandelt wird (Pkt. 6.1.4).
- In Bezug auf die **fahrlässige Begehung** von Art. 322bis StGB gründet die geforderte Sorgfaltspflicht namentlich auf dem allgemeinen Gefahrensatz, wonach derjenige, der einen Gefahrenzustand schafft, alles Zumutbare vorzukehren hat, damit die Gefahr zu keiner Verletzung fremder Rechtsgüter führt. **Der Access-Provider hat alles Zumutbare vorzukehren, damit deliktische Inhalte nicht zum Endbenutzer gelangen** (Pkt. 6.2.2).
- **Das Mass der Zumutbarkeit richtet sich nach objektiven Umständen und nach den persönlichen Verhältnissen** (Pkt. 6.2.3). Letztere sind für jeden Täter einzeln zu untersuchen (Pkt. 6.2.3.2).
- Bezüglich der objektiven Umstände wird die Sorgfaltspflicht des (Access-) Providers in der Regel erst dann aktuell, wenn ihm ein **konkreter und verlässlicher Hinweis auf einen deliktischen Inhalt** zukommt, was vor allem dann der Fall ist, wenn der Hinweis, allenfalls mit Aufforderungscharakter, von einer schweizerischen Strafverfolgungsbehörde ausgeht (Pkt. 6.2.3.1).
- Auf Grund des qualifizierten Charakters des vorausgesetzten Wissens dürfte eine **fahrlässige Erfüllung von Art. 322bis StGB nur in seltenen Ausnahmefällen** vorkommen (Pkt. 6.2.4).
- **Zusammenfassend lässt sich zum Ausmass der Verantwortlichkeit des Access-Providers festhalten, dass seine Stellung als subsidiär Verantwortlicher bloss ”zweiter Ordnung” auf den tatsächlichen Umfang seiner strafrechtlichen Verantwortlichkeit einen stark begrenzenden Einfluss hat, indem ein Wissen bei ihm über deliktische Inhalte nicht leichthin angenommen oder vermutet werden kann, sondern hierfür in der Praxis in erster Linie konkrete Hinweise von schweizerischen Strafverfolgungsbehörden gegeben sein müssen** (Pkt. 6.3).
- Die Strafbarkeit der Access-Provider hinsichtlich Medieninhaltsdelikten, die nicht unter die medienstrafrechtlichen Sonderregeln fallen, richtet sich nach den allgemeinen **Regeln der Teilnahme**, gemäss welchen sich die Access-Provider na-

mentlich als Gehilfe zur Haupttat strafbar machen, wenn sie trotz Kenntnis des deliktischen Internet-Inhalts nicht die erforderlichen Massnahmen treffen (Pkt. 7).

- Die Kenntnis des Providers vom deliktischen Inhalt ist zentral für die Annahme einer strafbaren Gehilfenschaft, da diese **nur vorsätzlich** geleistet werden kann (Pkt. 7).
- Vom Access-Provider als möglicher Gehilfe kann keine Übersicht über die durch seine Installation transitierenden Inhalte verlangt werden, weshalb ihm die **Kenntnis vom Bestehen bestimmter strafbarer Inhalte** insbesondere durch Hinweise Dritter zukommen muss (Pkt. 7).
- Der **Hinweis einer Strafverfolgungsbehörde** an den Access-Provider auf konkrete Netzinhalte ist als ausreichend zu beurteilen, wogegen Mitteilungen Privater wohl nur ausnahmsweise die Voraussetzungen erfüllen dürften (Pkt. 7).

In Bezug auf die eben dargelegte mögliche Teilnahme des Access-Providers als Gehilfe des Haupttäters ist zudem auf Pkt. 1.5 des Gutachtens hinzuweisen, wonach die massgebliche Lehre eine - nicht unbeschränkte - Anwendung des **Ubiquitätsprinzips** (Art. 7 StGB) postuliert auf die häufig als Erfolgsdelikte konzipierten Internet-relevanten Straftaten. Damit ist **schweizerisches Strafrecht anwendbar, auch wenn - was häufig der Fall ist - die Haupttat im Ausland begangen wird**[17].

Hinsichtlich des Argumentes, eine mögliche Gehilfenschaft falle ausser Betracht, weil die vom Access-Provider erbrachte Leistung eine neutrale Alltagshandlung darstelle, ist auf Pkt. 5.3.3.4 des Gutachtens zu verweisen, wonach das Bundesgericht dieser Betrachtungsweise betreffend Kommunikationsnetzen eine Absage erteilte.

Vor dem Hintergrund dieser hier zitierten Erwägungen des BJ, welche in erster Linie auf den Access-Provider zugeschnitten sind, sind hinsichtlich des **Hosting-Providers** folgende Ergänzungen anzubringen:

Der Hosting-Provider steht mit dem Content-Provider in einer vertraglichen Bindung hinsichtlich der zur Verfügung gestellten Speicherkapazität auf dem Web-Server. In Bezug auf das Medienstrafrecht steht er auch deshalb als **subsidiär Verantwortlicher** im Vordergrund[18] (Pkt. 5.3.3.2 des BJ-Gutachtens).

Wie beim Access-Provider ist **auch beim Hosting-Provider das Wissens-Element von zentraler Bedeutung**, um den Vorsatz einer Widerhandlung im Sinne von Art. 322bis StGB zu verwirklichen. Dieses Wissen ist auch notwendig, um die bei der fahrlässigen Begehung relevante Sorgfaltspflicht aktuell werden zu lassen (vgl. BJ Gutachten, Pkt. 6.2.4).

Neben konkreten und aus zuverlässiger Quelle stammenden Hinweisen, welche ein strafrelevantes Wissen des Hosting-Providers begründen, stellt sich die Frage, ob auch weniger qualifizierte Hinweise hierfür genügen, oder ob dem Hosting-Provider zugemutet werden kann, den Inhalt seines Web-Servers selber zu kontrollieren. Diese Fragen stellen sich namentlich auch hinsichtlich Providern, die Speicherkapazitäten ihres Web-Servers unentgeltlich zur Verfügung stellen oder dem Content-Provider einen nicht verifizierten Zugang ermöglichen.

---

[17] In Bezug auf eine Widerhandlung im Sinne von Art. 322bis StGB stellt sich die Frage einer vorgängigen Haupttat nicht, da Art. 322bis StGB eine selbständige Handlung darstellt (BJ-Gutachten; Pkt. 5.3.3.4)

[18] Der Grundsatz der primären und ausschliesslichen Verantwortlichkeit des Content-Providers/Autors gilt natürlich auch hier

Da der **Inhalt des Web-Servers** eines Hosting-Providers in der Regel ohne dessen Zutun durch den Content-Provider bestimmt und auch geändert wird, könnte sich dieser sein Wissen um den eingespeisten Inhalt nur durch regelmässig wiederholte Kontrollen verschaffen. Angesichts der möglichen grossen Datenmengen auf einem Web-Server erscheinen solche Kontrollen nicht Erfolg versprechend, weshalb sie nicht erwartet werden können[19]. Es kann jedoch möglich sein, dass der Hosting-Provider in seltenen Einzelfällen auf Grund eigener Wahrnehmung - z.B. durch die im Rahmen der Vertragsschliessung mit dem Content-Provider erhältlich gemachten Informationen - an der rechtmässigen Verwendung des dem Content-Provider zur Verfügung gestellten Speicherraumes berechtigte Zweifel hegen muss. Diesfalls ist von ihm zu fordern, die Inhalte dieses Content-Providers **mindestens stichprobenweise zu kontrollieren**, um sich nicht einem allfälligen Vorwurf einer (eventual-) vorsätzlichen Gehilfenschaft auszusetzen.

Da die auf dem Web-Server gespeicherten Datenmengen im Verhältnis zu denjenigen, welche die Access-Infrastruktur transitieren, wesentlich geringer sind und zudem der Hosting-Provider in der Kette der Intermediäre zwischen Content-Provider und Nutzer dem Ersteren am nächsten steht, ist vom Hosting-Provider zu fordern, dass er - im Unterschied zum Access-Provider - detaillierten und konkreten Hinweisen nachzugehen hat, auch wenn sie nicht aus einer Quelle stammen, die mit einer Instanz der Strafrechtspflege gleichgesetzt werden kann. Die **im Vergleich zum Access-Provider erhöhte Pflicht des Hosting-Providers, Hinweisen nachzugehen**, ergibt sich weniger aus der technischen Nähe zum Content-Provider, als vielmehr daraus, dass beide in einem Vertragsverhältnis zueinander stehen. Im Einzelfall können solche Hinweise dazu führen, dass der Hosting-Provider, gegebenenfalls unter Beizug einer Strafverfolgungsbehörde oder von fachlich qualifizierten Dritten, Nachforschungen treffen muss[20,21]. Regelmässig aber sollte zur Beantwortung der Frage, ob ein bestimmter Inhalt strafrelevant ist, die Parallelwertung in der Laiensphäre genügen. Dabei hat der Hosting-Provider unter Berücksichtigung seiner Auffassungen, seiner Umgebung und der gesetzlichen Bewertung einzuschätzen, ob ein Inhalt als unzulässig zu betrachten ist[22].

Anzufügen bleibt bezüglich dieser Ausführungen, dass sie in strafrechtlicher Hinsicht für den Hosting-Provider nur dann greifen, wenn der Content-Provider nicht ermittelt oder in der Schweiz nicht vor ein Gericht gestellt werden kann.

In Bezug auf die Teilnahme an Delikten, welche nicht unter die medienstrafrechtlichen Sonderregeln fallen, können hinsichtlich der Hosting-Provider folgende Ergänzungen zu den Ausführungen des BJ-Gutachtens angebracht werden:

Als mögliche Teilnahmeform steht typischerweise **nur die Gehilfenschaft** im Sinne von Art. 25 StGB in Frage[23]. Die funktionelle und rechtliche Nähe des Hosting-Providers zum Content-Provider sowie die kleinere Datenmenge auf seinem Web-Server - im Verhältnis zur Datenmenge, die beim Access-Provider transitiert - führt

[19] vgl. auch Ochsenbein/Heinzmann, a.a.O., S. 602 ff.
[20] vgl. Internet, Neues Medium, neue Fragen ans Recht, a.a.O., S. 10 f. (die dort gemachten Ausführungen beziehen sich zwar auf die Gehilfenschaft und nicht auf das Medienstrafrecht; in Bezug auf das Wissenselement einer Handlung i.S. Art. 322bis StGB können sie dennoch herangezogen werden)
[21] Die im Gutachten des BJ angesprochene Gefahr einer "Privatzensur" (Pkt. 6.1.2), welche durch die Verminderung der Qualitätsanforderung der Hinweise befürchtet werden könnte, ist im Verhältnis zwischen Content- und Hosting-Provider insofern nicht virulent, als es jedem Hosting-Provider im Rahmen der Vertragsfreiheit offen steht, wem und für was er seine Server zur Verfügung stellt.
[22] Schultz, AT I StGB, 4. Auflage, Bern 1982, S. 190 f.
[23] vgl. Internet, Neues Medium, neue Fragen ans Recht, a.a.O., S. 8

bezüglich des Wissens-Elementes des Gehilfenschafts-Vorsatzes dazu, dass von ihm dasselbe Verhalten zu fordern ist, wie eben hinsichtlich Art. 322bis StGB ausgeführt: Neben qualifizierten Hinweisen von Strafverfolgungsbehörden ist auch detaillierten und konkreten Hinweisen aus anderen Quellen nachzugehen.

Bei den bis hier aufgeführten Erwägungen sind in erster Linie Inhalte des WWW zu Grunde gelegt worden. **In strafrechtlicher Hinsicht gilt das Gesagte aber prinzipiell auch für Inhalte auf news- oder FTP-Servern**.

Bezüglich der Inhalte auf **news-Servern** ist eine aktive Kontrolle auf Grund der grossen Datenvolumen und der sich ständig veränderten Inhalte nicht vorstellbar[24]. Sofern ein news-Server nicht nur (nahezu) ausschliesslich einschlägige groups enthält, scheidet auf Grund der zu beachtenden Informationsfreiheit auch die Frage der Sperrung des Zugangs auf einen solchen Server aus der Diskussion. Von Betreibern von news-Servern aber ist zu fordern, dass sie konkreten und detaillierten Hinweisen auf groups mit strafrelevantem Inhalt nachgehen. Da die einzelnen Inhalte innerhalb einer group häufig grosse qualitative Unterschiede aufweisen, vermag ein Hinweis auf einzelne Nachrichten einer Gruppe die zu fordernde Bestimmtheit des Wissens in der Regel kaum zu begründen, zumal die einzelnen Nachrichten nach relativ kurzer Zeit automatisch gelöscht werden. Ist aber auf Grund des Hinweises davon auszugehen, dass überwiegend und regelmässig Nachrichten mit strafrelevanten Inhalten in eine group gesendet werden, ist der Hinweis zu prüfen und diese group gegebenenfalls zu löschen (sowie das erneute automatische Spiegeln zu verhindern).

In Bezug auf **FTP-Server** ergeben sich strafrechtliche Verantwortlichkeitsfragen in erster Linie für den Betreiber eines solchen Servers, während die Möglichkeit einer gezielten Zugangssperre (auf einzelne Verzeichnisse oder Dateien) durch den Access-Provider von vornherein auf Grund der technischen Gegebenheiten ausscheiden dürfte.[25] Der Betreiber eines FTP-Servers, der die freie Datenablage ermöglicht, hat Hinweisen nachzugehen. Diesbezüglich kann von ihm jedoch nicht verlangt werden, dass er zum Lesen der Dateien Software einsetzt, die nicht als branchenüblich bezeichnet werden kann.

Klarerweise steht die Frage einer Zugangssperre oder inhaltlichen Kontrolle **auf Internet Relay Chat-Server** nicht zur Diskussion. Die Flüchtigkeit der Daten lassen ein strafrechtlich relevantes Wissen gar nie entstehen[26].

6. Technische Aspekte einer Zugriffssperrung[27]

Komplexe technische Fragen stellen sich beim Zugriff auf illegale Inhalte auf WWW-Servern, die wegen ihrer grossen Verbreitung und des relativ langen zeitlichen Verbleibens der Inhalte auf den Servern im Vordergrund stehen. Wie schon erwähnt, muss davon ausgegangen werden, dass der eigentliche Autor oder der Hosting-Provider in vielen Fällen rechtlich nicht belangt werden kann (z.B. Server in den USA und Kanada unter dem Schutz der Meinungsäusserungsfreiheit). Deshalb drängt

[24] vgl. Ulrich Sieber, Verantwortlichkeit im Internet, S. 51
[25] Die Sperrung des Zugangs auf den ganzen FTP-Server steht kaum je in Frage, da diese i.d.R. auch strafrechtlich nicht relevante Dateien enthalten
[26] vgl. hierzu v.a. Ulrich Sieber, Verantwortlichkeit im Internet, S. 40 f. und 57 f.
[27] Zu den technischen Aspekten siehe Rosenthal, David: Current Problems and Possible Strategies for Combating Racism on the Internet (http://www.rvo.ch/docs/unracism.pdf), sowie Sieber Ulrich: Verantwortlichkeit im Internet - Technische Kontrollmöglichkeiten und multimediarechtliche Regelungen (Beck: München 1999).

sich sozusagen als "zweitbestes" Mittel eine Sperrung des Zugriffs auf solche Inhalte durch Schweizer Internet Access oder Network-Provider auf.

Welche Möglichkeiten stehen einem ISP grundsätzlich zur Verfügung, um einen bestimmten Inhalt auf einem WWW-Server zu sperren?

1. Der Provider **sperrt die IP-Adresse** des betroffenen Webservers auf Router-Ebene. Dies führt zur Sperrung *aller* Angebote auf dem Server und nicht nur des monierten Inhalts. Dieses Vorgehen ist damit bei grossen Anbietern wie AOL, Geocities usw. mit Tausenden von verschiedenen Inhalten keine praktikable Lösung. Sie bietet sich hingegen bei illegalen Angeboten mit eigenem Server / Namen an, bei denen unter einem bestimmten Domain Name respektive einer bestimmten IP-Adresse meist nur Angebote ähnlichen Inhalts (z.B. rassistisch oder gewaltextremistisch) vorliegen. Dieser Fall ist im Bereich rassistische/extremistische Inhalte relativ häufig, da diese Content-Provider den Vorteil von einfach zu merkenden Domain Names nutzen wollen (Beispiele: stormfront.org, aryanbooks.com). Die von der Bundespolizei momentan zur Sperrung empfohlenen Websites entsprechen dieser Kategorie.
   Eine Variante dieser Lösung ist, auf DNS-Ebene (Domain Name Server) gewisse Domain Names (wie eben z.B. stormfront.org) auszuschliessen.
2. Der Provider betreibt einen so genannten **Proxy-Server**. Alle WWW-Anfragen (z.B. Port 80) gehen in der Grundkonfiguration des Webbrowsers über diesen Proxy. Dieser ermöglicht dann das Aufzeichnen der Anfragen, Zwischenspeichern der angeforderten Daten, aber auch deren Sperrung. Der Kunde hat seinen Webbrowser entsprechend zu konfigurieren. Wenn er dies jedoch nicht tut, dann wird der Proxy-Server umgangen und die Verbindung wird direkt zu der gewünschten Site aufgebaut. Die meisten Provider betreiben bereits solche Proxy-Server, allerdings mit der Absicht der Performance-Steigerung. Es existieren auch Proxies für andere Protokolle als HTTP, zum Beispiel für FTP.
3. Der Provider verwendet einen sog. **"Transparent Proxy"**, sodass die Kunden automatisch den Proxy-Server benützen, egal ob sie es wollen oder nicht. Im Proxy kann dann bis auf die Ebene einer einzelnen Seite gesperrt werden. Im Prinzip handelt es sich hier um einen offenen Firewall, der aber gewisse Dienste umleiten und ggf. filtern kann[28].

Eine Abwandlung der Variante 1 wird heute zur Sperrung der von der Bundespolizei zur Sperrung empfohlen Websites bereits eingesetzt.

Allen Varianten sind allerdings **gewisse Nachteile** gemeinsam:

a) Sämtliche Arten von Filterung führen zu **Performanceproblemen**, die Methoden sind schlecht skalierbar. Was jetzt bei einem Dutzend Adressen gut funktioniert, führt bei einigen Tausend unter Umständen zu einem Zusammenbruch der Provider-Infrastruktur.

b) Alle genannten Methoden können durch die Benutzung eines so genannten **Anonymizers**, der die IP-Nummer des gesuchten Inhalts verschleiert, umgangen werden.

c) Gesperrte Websites werden von der Internet-Community erfahrungsgemäss auf diversen Servern in voller Kopie abgelegt (**mirroring**), da solche Vorgänge von

[28] Allerdings stellt sich hier ein ähnliches Problem wie beim normalen Proxy-Server. Je nach Einstellung verhindert er den Zugriff auf Dienste mit speziellen Protokollen oder Ports (z.B. Telebanking).

vielen Benutzern beinahe reflexartig als Zensur interpretiert werden. Alle diese Websites müssten wieder gesperrt werden.

d) Der **Aufwand** für die Aktualisierung und Administrierung der Sperrlisten ist für den einzelnen Provider u.U. hoch, je nach Sperrmethode ist dies auch mit recht hohen Investitionen verbunden. Je nach Zählung sind in der Schweiz momentan über 300 Provider aktiv, Grossfirmen und die öffentliche Verwaltung / Schulen nicht mitgezählt. Auch für jene polizeilichen / richterlichen Stellen, die Sperrungen verlangen, ist damit der administrative Aufwand nicht zu unterschätzen. Abhilfe könnte bis zu einem gewissen Grad die Sperrung auf der Ebene der Network-Provider bringen, auf denen die einzelnen ISPs basieren.

e) Ein **nationaler Lösungsansatz** ist in der Internet-Welt grundsätzlich problematisch. Bei den heutigen tiefen Telefonpreisen ist eine Einwahl eines Schweizer Kunden bei einem ausländischen Provider (ohne Sperrungen) durchaus im Rahmen der finanziellen Möglichkeiten. Einige Online-Service-Provider (z.B. AOL) bieten ausserdem laut eigenen Angaben den Internet-Zugang europaweit über die gleichen Netze an; somit wäre eine Sperrung nur für die Schweiz bei ihrer jetzigen Netztopologie gar nicht machbar.

Fazit aus technischer Sicht:

Die Sperrung ganzer Websites (Domain Name oder IP-Nummer) ist für Internet Service Provider oder für Network machbar, aber nicht in allen Fällen adäquat (illegaler Inhalt nur als Teil eines Angebots z.B. bei Web-Hosting-Firmen) und je nach Methode sehr aufwändig.

Nachteile aller technischen Lösungen auf nationaler Ebene sind der relativ hohe administrative und finanzielle Aufwand sowie die Umgehbarkeit durch Nutzer, die einen gewissen Aufwand nicht scheuen. Der notwendige Administrierungsaufwand bei den einzelnen Providern könnte allerdings verkleinert werden, wenn in der Schweiz eine **einzige Stelle** für die Sperrungen bezeichnet würde und diese Stelle die notwendigen Daten (IP-Nummer, Domain Name) in einem **maschinenlesbaren Format** regelmässig zur Verfügung stellen würde. Wenn die grossen schweizerischen **Network-Provider** (wie ip-plus, Eunet usw.) die Sperrungen als Dienstleistung für ihre Kunden durchführen würden, wäre die grosse Mehrheit der kleineren Provider, die ihre Leitungskapazität von den Network-Providern beziehen, automatisch mitbeteiligt. Bei dieser Lösung müsste allerdings die Skalierbarkeit noch genauer studiert werden.

Bei einer allfälligen zukünftigen internationalen Lösung (siehe dazu Kapitel 11) ergäben sich schliesslich **neue technische Sperrmöglichkeiten an der Quelle** (z.B. wären dann in den USA nicht verfolgbare rassistische oder rechtsextreme Inhalte durch technische Vorkehrungen beim Hosting Provider für Europäer nicht mehr sichtbar).[29]

[29] Diese Methode wurde z.B. bis vor kurzem eingesetzt, um auf amerikanischen Websites Nichtbürgern der USA den Download von Internet-Browsern mit starker Kryptographie zu verwehren

7. Zumutbarkeit und Verhältnismässigkeit von Zugangssperrungen und Inhaltslöschungen

Die Frage der Zumutbarkeit respektive Unzumutbarkeit einer Handlung wird zum einen beim Notstand (Art. 34 StGB) gestellt. Sie ergibt sich weiter bei der Bestimmung des pflichtgemässen Verhaltens in Bezug auf das fahrlässige Begehungsdelikt[30], das vorliegend nicht weiter interessiert, da ein ISP (sowohl als Access-, als auch als Hosting-Provider), der Kenntnis von strafrelevanten Inhalten hat und darauf nicht reagiert, sich in der Regel (eventual-)vorsätzlich verhält[31].

Ein solches Verhalten wäre im Sinne einer Notstandshandlung dann straflos, wenn dem ISP nicht zugemutet werden könnte, sein Gut[32] preiszugeben. Das zumutbare Verhalten muss folglich verhältnismässig im Sinne einer Rechtsgüterabwägung sein. Auf Grund der endgültig nur durch die Gerichte einzelfallweise vornehmbaren Abwägung der betroffenen Rechtsgüter, kann eine allgemein gültige Bestimmung, welche Rechtsgüter gegenüber anderen als höherwertig einzustufen sind, im vorliegenden Papier nicht vorgenommen werden, zumal diese[33] in der Regel schwer zu quantifizieren sind.

Bei der Zumutbarkeit in einem bestimmten Mass zu berücksichtigen ist sicherlich auch der Umstand der gegenüber einer Zugangssperre möglichen Umgehungsmöglichkeiten. Es gilt diesbezüglich jedoch darauf hinzuweisen, dass der kausale Tatbeitrag, den ein ISP gegebenenfalls leistet, zur Begründung der Gehilfenschaft ausreicht[34]. Selbst wenn die Sperrung des Zugriffs für schweizerische Kunden durch ihre Provider zurzeit nicht lückenlos sein kann oder ein zu löschender Inhalt vom Content-Provider auf dem Server eines anderen Hosting-Providers platziert werden kann, rechtfertigt sich - ähnlich wie die präventiven Aufgaben von Polizei oder Zoll - ein solches Vorgehen grundsätzlich auch bei nicht hundertprozentigen Erfolgsquoten.

Diese bezüglich der Gehilfenschaft geltenden Ausführungen gelten sinngemäss auch bezüglich der subsidiären Verantwortlichkeit der ISP nach Medienstrafrecht, zumal sich die Frage der Kausalität auf Grund des Umstandes, dass Art. 322bis StGB ein selbstständiges Delikt darstellt, nicht stellt.

Vor dem Hintergrund der rechtlichen und technischen Situation sind folgende Vorkehren als zumutbar zu erachten[35]:

[30] vgl. Trechsel/Noll, StGB AT I, 4. Auflage, Zürich 1994, S. 243
[31] vgl. diesbezüglich die Zusammenfassung des BJ-Gutachtens unter Pkt. 8
[32] wohl in erster Linie sein Vermögen, das einerseits in einem Wettbewerbsvorteil durch unbeschränkten Zugang bestehen und andererseits durch den notwendigen Einsatz technischer und menschlicher Ressourcen vermindert werden kann.
[33] neben dem Vermögen auf der einen Seite kommen auf der anderen Seite etwa in Frage: Jugendschutz und Schutz der sexuellen Integrität bei Art. 197 StGB; öffentlicher Friede, respektive Menschenwürde oder Schutz des Gefühls, von anderen als anderer geachtet zu werden bei Art. 261bis StGB; Vermögen und Selbstbestimmungsrecht beim Urheberrecht.
[34] vgl. BGE 120 IV 272, wonach der "Gehilfe die Erfolgschancen der tatbestandserfüllenden Handlung erhöhen" muss; BGE 119 IV 292: "Nach der Rechtsprechung gilt als Hilfeleistung jeder kausale Beitrag, der die Tat fördert, so dass sich diese ohne Mitwirkung des Gehilfen anders abgespielt hätte. Nicht erforderlich ist, dass es ohne die Hilfeleistung nicht zur Tat gekommen wäre."
[35] Die gerichtliche Beurteilung der Zumutbarkeit (im Einzelfall) und damit letztlich der Frage, ob ein strafbares Verhalten des Providers vorliegt, bleiben selbstverständlich vorbehalten.

- **Erhält ein Access-Provider durch Strafverfolgungsbehörden konkrete und detaillierte Hinweise auf strafrelevante Inhalte, so sorgt er für die Sperrung des Zugangs zu diesen Sites** im Sinne der unter Punkt 6 hiervor aufgezählten Massnahmen. Dazu zählen in erster Linie die Sperrung der IP-Adresse, wenn der strafbare Inhalt auf einer **Site mit eigener IP-Adresse** abgelegt ist, sowie allenfalls die Sperrung untergeordneter URL im Proxy-Server.

- **Erhält ein Hosting-Provider konkrete und detaillierte Hinweise** (nicht nur von Strafverfolgungsbehörden) **auf strafrelevante Inhalte, die sich auf einem seiner Server befinden, so sorgt er dafür, dass diese Inhalte nicht mehr zugänglich sind oder gelöscht werden.** Stammen diese Hinweise nicht von einer Strafverfolgungsbehörde, hat er selber - gegebenenfalls unter Beizug einer Strafverfolgungsbehörde oder von fachlich qualifizierten Dritten, entsprechende Nachforschungen zu treffen. Gleiches gilt, wenn er auf Grund seines Vertragsverhältnisses mit dem Content-Provider über Informationen verfügt, die ihn an der rechtmässigen Verwendung des zur Verfügung gestellten Speicherraumes zweifeln lassen.

8. Strafrechtlich gebotenes Verhalten der Provider

Im Sinne einer Folgerung ist von den Providern folgendes Verhalten zu erwarten:

8.1. Access-Provider:

- Liegen dem Access-Provider konkrete Hinweise einer Strafverfolgungsbehörde auf vermutlich illegale Netzinhalte vor, sind **Sperrungen** - soweit zumutbar - zu erwarten.
- **Eigenes, aktives Suchen** nach strafrelevanten Inhalten im Internet ist allein schon auf Grund der sich täglich ändernden und zunehmenden Datenmenge weder sinnvoll noch Erfolg versprechend und kann deshalb nicht erwartet werden.

8.2. Hosting-Provider:

- Detaillierten und konkreten Hinweisen auf illegale **Web-Inhalte und newsgroups** hat der Hosting-Provider nachzugehen. Findet er solche Inhalte, sind diese zu **löschen** oder zumindest deren Abrufbarkeit zu **sperren**.
- Angesichts der im Vergleich zu den reinen Access-Providern deutlich näheren Anbindung an den Content-Provider, ist mindestens die **stichprobeweise Kontrolle verdächtigter Content-Provider** zu erwarten.
- Bezüglich Dateien auf **FTP-Servern**, auf welchen die freie Datenablage ermöglicht ist, ist Hinweisen nachzugehen, sofern die Dateien mit branchenüblicher Software gelesen werden können.

8.3. Online-Service-Provider

- **Je nach Ausgestaltung ihrer Dienste** stellen Online-Service-Provider **Content-, Hosting- oder Access-Provider** dar, weshalb die Frage ihrer strafrechtlichen Verantwortung nach diesen Funktionen zu beantworten ist.

Für alle Internet Service Provider gilt:

- **Die unter Ziffer 8.1. bis 8.3. genannten Vorkehren beschränken sich auf öffentliche Dienste. Bei nicht öffentlichen Diensten hingegen greift das Fernmeldegeheimnis, weshalb dort keine Inhaltskenntnis des ISP und demnach auch keine Vorkehren erwartet werden dürfen und können.** Eine strafrechtliche Verantwortlichkeit des ISP kann im nicht öffentlichen Bereich des Internet deshalb in aller Regel ausgeschlossen werden.

- Der ISP hat bezüglich strafbaren Verhaltens oder Inhalte **keine Anzeigepflicht** an Polizeibehörden. Es gilt jedoch das allgemein gültige **Anzeigerecht**. Bei Erfüllung der Tatbestände eines Antragsdeliktes (z.B. Ehrverletzungsdelikte, bestimmte Urheberrechtsdelikte) kann entweder der Content-Provider auf die Strafrelevanz seines Verhaltens oder der Betroffene auf die Gefährdung seiner Rechte aufmerksam gemacht werden.

- **Im Rahmen von Strafverfahren, die sich nicht gegen den Provider richten, bestehen die allgemeinen Pflichten des angewendeten Strafprozessrechts** (des Kantons oder Bundes): Pflicht, als Zeuge auszusagen, Pflicht auf Herausgabe von Akten oder von Informationen ab elektronischem Speicher. Bezüglich Dienste, die dem Fernmeldegeheimnis unterstehen (E-Mail, private-chat, Internet-Telefonie) sind die Anordnungen der zuständigen Behörde nach anwendbarem Strafprozessrecht[36] auszuführen. Als solche können aufgeführt werden:
  - **Auskunft über den Internet-Verkehr von Usern, die Kunden des ISP sind**[37]. Diese Auskünfte sind soweit möglich in Echtzeit zu erteilen, d.h. soweit technisch möglich ist eine direkte Überwachungsschaltung vorzunehmen[38]. Die anordnende Behörde (welche die Massnahme über den Dienst für besondere Aufgaben des UVEK vollziehen lässt[39]) hat hierfür eine angemessene Entschädigung auszurichten[40].
  - in den Logfiles abgelegte persönliche **Verkehrs- und Rechnungsdaten** der einzelnen User. Diese müssen den zuständigen Behörden während mindestens **sechs Monaten** zur Verfügung gestellt werden können[41].

- Aufwände, die durch die vorzunehmenden **Sperrungs- oder Löschungsmassnahmen** entstehen, ergeben sich auf Grund der bestehenden strafrechtlichen Verantwortlichkeit nach Medienstrafrecht, respektive durch die mögliche Gehilfenschaft zu einer Haupttat. Die Massnahmen stellen strafrechtlich gebotenes Verhalten dar, dass **nicht zu entschädigen** ist.

9. Von der Bundesverwaltung zu erwartendes Verhalten

- Bei **Kenntnis strafbarer Inhalte** werden primär entsprechende Anzeigen (gegen Content-Provider) an kantonal zuständige Behörden gerichtet oder ausländische Behörden auf diese Inhalte hingewiesen, damit **in erster Linie Haupttat und -täter verfolgt** werden.

[36] in Verbindung mit Art. 44 FMG
[37] Art. 44 Abs. 1 FMG
[38] Art. 44 Abs. 2 FMG
[39] vgl. Verordnung vom 1. Dezember 1997 über den Dienst für die Überwachung des Post- und Fernmeldeverkehrs (SR 780.11)
[40] vgl. Verordnung vom 12. Dezember 1997 über die Gebühren und Entschädigungen bei der Überwachung des Post- und Fernmeldeverkehrs (SR 780.115.1)
[41] (Im Rahmen der Überwachung des Fermeldeverkehrs gemäss Art. 44 FMG) Art. 50 Verordnung über Fernmeldedienste (FDV; SR 784.101.1)

- Die Bundesverwaltung **unterstützt**, soweit sie über entsprechendes Fachwissen verfügt, die Provider bei der Beurteilung möglicherweise strafbarer Inhalte und der Implementierung von technischen Sperrmassnahmen.

10. Ergänzende Vorgehensweisen

Vermehrte internationale Zusammenarbeit
Neben der Sperrung bieten sich einige andere - allerdings **eher mittelfristig wirksame** - Möglichkeiten zur Bekämpfung illegaler Inhalte auf dem Internet an. So haben die Bundespolizei und andere Amtsstellen die Zusammenarbeit mit ausländischen Partnerdienststellen intensiviert, um zu einer einheitlichen Sichtweise und Strafverfolgung illegaler Inhalte auf dem Internet zu gelangen.

Rechtsvereinheitlichung
Eine internationale Angleichung der rechtlichen Tatbestände, also sozusagen "internetkompatible(re)s" Recht, wäre zwar wünschenswert, ist **aber in naher Zukunft nicht zu erwarten**. Ein möglicher, wichtiger Ansprechpartner sind hier die USA, die - ungewollt - durch das Hosten extremistischer und rassistischer Websites, dem internationalen Antisemitismus und Rassismus Vorschub leisten.

Internationale Abkommen über illegale Inhalte
Eine realistischere Lösung wären internationale Abkommen über illegale Inhalte im Internet. Hier gibt es bereits **einige Ansätze**:

- Europarat: Empfehlungen des Ministerkomitees des Europarats betreffend Informatikkriminalität (R (89) 9) und Probleme des Strafprozessrechts im Zusammenhang mit Informationstechnologie (R (95) 13).[42] 1997 ist ein Expertenkomitee zum Thema "Crime in Cyberspace" einberufen worden, das bis Ende 2000 einen Entwurf für einen internationalen Vertrag zur Bekämpfung der Internetkriminalität vorlegen will.[43]
- OECD: Vorschlag Frankreichs für eine Charta zur internationalen Kooperation im Zusammenhang mit dem Internet, inkl. Kooperation im Bereich der Strafverfolgung.[44]
- EU: Vierjähriges Aktionsprogramm (1999-2002) gegen "illegale und schädliche Inhalte in globalen Netzen" vom 25.1.1999.[45] Der EU-Ansatz beschränkt sich primär auf die Selbstkontrolle der Anbieter (Verhaltensregeln) und damit kombinierbare technische Massnahmen (Kennzeichnungs- und Filterungssysteme). Es soll eine europaweite Hotline zur Anzeige solcher Inhalte geschaffen werden.
- Die Uno führte im November 1997 in Genf ein Seminar zu diesem Thema durch und forderte die Mitgliedländer auf, ihre nationale Rechtsprechung anzupassen und zu harmonisieren.
- Die Kommission der Europäischen Gemeinschaften hat am 18. November 1998 den Vorschlag für eine Richtlinie des Europ. Parlamentes und des Rates über bestimmte rechtliche Aspekte des elektronischen Geschäftsverkehrs im Binnen-

[42] www.privacy.org/pi/agreements.html
[43] Die "Terms of Reference", die mittlerweile von Ende 1999 auf Ende 2000 verlängert wurden, sind auf der Website des Europarats abrufbar: http://www.coe.fr/cm/dec/1997/583/583.a13.html
[44] www.telecom.gouv.fr/francais/activ/techno/charteint.htm
[45] http://www.europa.eu.int/eur-lex/de/lif/dat/1999/de_399D0276.html

markt angenommen[46]. Vorliegend von Interesse ist an diesem Vorschlag Artikel 12, wonach für die ”reine Durchleitung” (im Sinne des hier verwendeten Begriffs ”Access”) keine Verantwortlichkeit bestehen soll. Nach Art. 13 soll dies auch für das Caching gelten. Bezüglich des Hostings sieht Art. 14 vor, dass der Hosting-Provider nicht verantwortlich wird, ausser er habe tatsächliche Kenntnis von der illegalen Tätigkeit des Nutzers. Art. 15 sieht für die Diensteanbieter nach Art. 12 - 14 vor, dass keine Überwachungspflicht besteht, ausser sie seien durch Justizbehörden angeordnet[47]. In einem gemeinsamen Standpunkt des Rates vom 28.2.2000 zu diesen Richtlinienvorschlag wird ausgeführt, dass es nicht Ziel der Richtlinie ist, den Bereich des Strafrechts zu harmonisieren. In Bezug auf die Art. 12 - 14 des Richtlinienvorschlages wurden neue Absätze 3 eingefügt, wonach gerichtliche und verwaltungsbehördliche Verfügungen möglich sein sollen. Auch sollen die Mitgliedstaaten in Bezug auf Art. 15 nicht beschränkt werden, ISP zur Zusammenarbeit zu verpflichten[48].

- Schliesslich hat das Eidgenössische Departement für auswärtige Angelegenheiten im Rahmen der Washingtoner Holocaust-Konferenz vom November 1997 einen Vorstoss für eine internationale Konferenz über rassistische Inhalte im Internet lanciert. Sie hat diese Thematik im Rahmen der Uno-Menschenrechtskommission im März 1999 wieder aufgebracht und will zusammen mit anderen Staaten eine internationale Konferenz zur Bekämpfung rassistischer und antisemitischer Websites im Internet einberufen. Die dort erarbeiteten Vorschläge für Gegenmassnahmen sollen dann an der für 2001 geplanten internationalen Anti-Rassismus-Konferenz verabschiedet werden[49].

Engere Zusammenarbeit der Provider, Selbstkontrolle

Eine weitere, Erfolg versprechende Möglichkeit, gegen extremistische und rassistische Inhalte vorzugehen, ist eine engere Zusammenarbeit der Provider in der Schweiz und international. Diese können gemeinsam Druck auf Provider in anderen Ländern ausüben, solche Inhalte nicht auf ihren Servern zu dulden, auch wenn sie dort rechtlich theoretisch erlaubt sein sollten. **Basis dieser Zusammenarbeit wären die verschiedenen Geschäftsbedingungen und "Codes of Conduct" der Provider, die zumindest rassistische Inhalte in praktisch allen Fällen ausschliessen.** Erfahrungsgemäss sind Provider auch bereit, auf Hinweise anderer Provider zu reagieren und solche Inhalte zu entfernen. Viele Provider haben auch bereits eine Hotline eingerichtet, wo ihnen solche Inhalte gemeldet werden. Bis anhin beschränken sie sich aber meistens auf ihre eigenen Server. **Im Sinne der kooperativen Kultur des Internets könnte aber eine solche übergreifende Lösung sinnvoll sein und vor allem im Sinne der Selbsthilfe zu einem "cleaner Internet" führen**. An dieser Stelle sei auch auf das Beispiel der Freiwilligen Selbstkontrolle (FSK) der Unterhaltungsindustrie verwiesen. Unabdingbare Voraussetzung dafür wäre die Akzeptanz einer gemeinsamen Beurteilungsstelle.

[46] vgl. vgl. Ulrich Sieber, Verantwortlichkeit im Internet, S. 317 ff.
[47] vgl. Ulrich Sieber, Verantwortlichkeit im Internet, S. 232 f.
[48] vgl. Mitteilung der Kommission vom 29.2.2000 in SEK(2000) 386 endgültig
[49] Siehe dazu einen Beitrag, der für ein Vorbereitungstreffen zur Konferenz von 2001 in Genf verfasst wurde: Rosenthal, David: Current Problems and Possible Strategies for Combating Racism on the Internet, January 2000 (http://www.rvo.ch/docs/unracism.pdf),

11. Wie weiter?

Die ad hoc gebildete Kontaktgruppe hat **die vertiefte Diskussion der mit der Sperr-empfehlung der Bundespolizei verbundenen rechtlichen und technischen Fragen gefordert**. Diesem Postulat dient das vorliegende Positionspapier, wenn auch angesichts der rasanten technologischen Weiterentwicklung und der grundsätzlichen Unabhängigkeit der Justiz gewisse Unschärfen verbleiben müssen.

Die Kontaktgruppe hat zudem einerseits innerhalb der Bundesverwaltung, andererseits aber auch zwischen den ISP und den Bundesbehörden zu einer erhöhten Sensibilisierung für die unterschiedlichen Anliegen geführt.

Mit der vorliegenden juristischen und technischen Standortbestimmung hat die Kontaktgruppe nun ihren ursprünglichen Zweck erfüllt.

Das **Bedürfnis nach einer gemeinsamen, koordinierenden Ansprechplattform** Bund/ISP könnte allerdings auch in Zukunft - und unabhängig von Sperrempfehlungen der Bundespolizei - vorhanden sein. Als **mögliche Koordinationsbedürfnisse** seien hier erwähnt:

- **Koordination der konkreten Hinweise** von Strafverfolgungsbehörden auf strafrelevante Inhalte
- Harmonisierung der nationalen und internationalen **Bestrebungen zur Eindämmung der Internetkriminalität**
- Verfolgung der **technischen und juristischen Entwicklung**
- Beratung und Koordination der kantonalen Strafverfolgungsbehörden bei **der Behandlung von Strafanzeigen** gegen im Ausland abgelegte illegale Inhalte
- Möglichst **koordiniertes Auftreten der Bundesbehörden** gegenüber den ISP
- **Einheitlicher Ansprechpartner** auf Seiten der ISP
- Förderung des **gegenseitigen Wissenstransfers und des wechselseitigen Verständnisses**

Diesen Anforderungen kann auf verschiedene Weise begegnet werden:

1. Verzicht auf Koordination

z.B. weil Koordinationsbedürfnisse als nicht so gravierend eingestuft werden, dass ein Einsatz von Ressourcen gerechtfertigt erscheint.

2. Jeder koordiniert für sich

z.B. weil die Interessen der einzelnen Gruppen (ISP, kantonale Strafverfolgungsbehörden, Bundesverwaltung) zu unterschiedlich sind, als dass eine gemeinsame Plattform Sinn machen würde.

3. Einrichtung einer gemeinsamen Koordinations- und Infostelle

z.B. bei einer ausserhalb von Bund und ISP stehenden privaten Stelle (Antirassismus-organisation), oder beim Bund (BAP, Antirassismuskommission, UVEK, BJ) oder bei den Providern (Standesorganisation). Eine Zusammenarbeit von Bund, Kantonen und Privatwirtschaft müsste unter grösstmöglicher Transparenz erfolgen, damit Vorwürfen der Zensur entgegengewirkt werden kann.

La responsabilité pénale des fournisseurs de services Internet

Avis de la Police fédérale, avril 2000

1. Remarque préalable

Le 23 juillet 1998, la Police fédérale a envoyé une circulaire aux fournisseurs de services Internet (*Internet Service Providers, ISP*) de Suisse leur demandant de tester le blocage de certains sites ayant un contenu de discrimination raciale au sens de l'art. 261bis du code pénal suisse[1] (CP). Cette demande était motivée par le fait que faciliter l'accès à de tels sites pouvait être qualifié de complicité (art. 25 CP) à une infraction principale. Cette circulaire a déclenché un tollé général de la part des ISP, ce qui a entraîné la création d'un groupe de contact qui devait tenter de concilier les intérêts des fournisseurs d'accès à Internet, d'une part, et ceux des autorités policières de la Confédération, d'autre part. **Ce groupe de contact se compose actuellement d'une représentation des ISP suisses et de représentants des offices fédéraux de l'informatique, de la communication, de la justice et de la police.**

Les efforts visant à empêcher la diffusion et la consultation de contenus illicites sur Internet doivent aussi tenir compte du fait que les **besoins de communication légitimes** doivent pouvoir être satisfaits sans entrave[2] sur Internet. Il faut également susciter **l'intérêt de l'économie** pour la place suisse et, par conséquent, pour des conditions générales comparables au niveau international[3] en ne négligeant pas la **mission légale des autorités policières et judiciaires** consistant à poursuivre ou à empêcher les délits perpétrés sur Internet[4]. Il ne faut pas oublier que beaucoup de délits doivent être poursuivis d'office et que, pour une grande partie des délits, la compétence de poursuite et de jugement **relève des cantons**.

Le présent avis doit également servir à **répondre aux questions fondamentales relatives à la responsabilité pénale des ISP et à indiquer les voies possibles pour la collaboration avec les autorités de poursuite pénale**. Ce document doit être considéré comme un complément au rapport établi par un groupe de travail interdépartemental en mai 1996.[5]

Après qu'une première ébauche du présent document a été mise en consultation auprès des membres du groupe de contact, il a fallu obtenir **l'avis d'un expert sur la question de la responsabilité pénale des fournisseurs d'accès Internet,**

[1] RS 311.0

[2] Cf. les libertés d'opinion et d'information prévues par l'art. 16 de la Constitution fédérale (Cst.) du 18.4.1999, entrée en vigueur le 1.1.2000.

[3] Voir p. ex. le plan d'action élaboré par le Secrétariat d'Etat à l'économie (SECO) pour la promotion du commerce électronique en Suisse.

[4] La liberté économique garantie par la Constitution (art. 27 et 94 Cst.) ne peut être restreinte que dans les cas et conditions prévus par l'art. 36 Cst.; en l'occurrence et en premier lieu par les dispositions légales du CP.

[5] Internet, Le Nouveau Média Interroge Le Droit; rapport d'un groupe de travail interdépartemental sur des questions relevant du droit pénal, du droit de la protection des données et du droit d'auteur suscitées par Internet. (http://www.ofj.admin.ch/themen/ri-ir/internet/rf-internet-f.pdf).

conformément aux art. 27 et 322bis CP. Dans l'intervalle, l'avis a été rédigé par l'Office fédéral de la justice (OFJ) et distribué dans le groupe de travail[6]. Il y sera fait allusion par la suite aux endroits appropriés.

2. Délits sur Internet

Internet reflète au moins en partie le monde réel avec ses aspects fascinants et ses aspects moins sympathiques. C'est ainsi qu'Internet et ses nombreux services sont désormais utilisés pour presque tous les types d'actes criminels. Les actes punissables peuvent être répartis en deux groupes principaux:

- **Les délits perpétrés par le transfert de données (souvent à court terme) via Internet**. Tombent dans cette catégorie les délits informatiques à proprement parler, tels que la soustraction de données (art. 143 CP), l'accès indu à un système informatique (art. 143bis CP), la détérioration de données (art. 144bis CP), l'utilisation frauduleuse d'un ordinateur (art. 147 CP) ainsi que l'obtention frauduleuse d'une prestation (art. 150, al. 3, CP). Viennent encore s'ajouter tous les autres délits au cours desquels des informations sont transmises via Internet, tels que la violation des droits d'auteur, l'infraction à la loi sur les loteries, la violation du secret de fabrication ou du secret commercial (art. 162 CP), l'espionnage (art. 272 ss. CP), le blanchiment d'argent (art. 305bis CP), etc. Cette catégorie peut également accueillir les autres délits de participation (complicité, assistance, instigation) à tous les délits possibles lorsqu'ils existent dans la communication entre les complices.
- **Les délits perpétrés par l'intermédiaire d'Internet durant un certain temps, en donnant à consulter des contenus punissables.** Entrent dans cette catégorie, par exemple, la représentation de la violence (art. 135 CP), l'escroquerie (art. 146 CP; p. ex. par la tromperie au moyen d'un site Web), la pornographie (art. 197 CP), les délits qui sont poursuivis sur plainte, comme les délits contre l'honneur (art. 173 ss. CP), la discrimination raciale (art. 261bis CP) et les violations des droits d'auteur[7].

Pour les infractions de la première catégorie, la phase de l'acte passant via Internet n'est constatable que par une surveillance simultanée du transfert des données. En d'autres termes, il n'est pas envisageable d'empêcher ou de limiter l'entrée de données par des mesures spécifiques à Internet, de sorte que seuls des types d'intervention traditionnels peuvent laisser escompter des résultats.

La deuxième catégorie revêt un intérêt particulier car les actes punissables qui y sont répertoriés se produisent souvent pendant une certaine durée, si bien que leur découverte et la prise de mesures adéquates permettent au moins de limiter la portée du délit. **En ce qui concerne les délits relatifs à Internet souvent débattus dans l'opinion publique, soit la pornographie et la discrimination raciale, on constate que les contenus punissables se trouvent généralement sur des serveurs étrangers**[8].

[6] L'avis peut être consulté sur Internet: http://www.bj.admin.ch/themen/ri-ir/access/intro-d.htm.
[7] Cf. annexe 2 du rapport du groupe de travail interdépartemental de mai 1996.
[8] Cette remarque vaut surtout pour le WWW tandis que les contenus des groupes d'information se retrouvent aussi fréquemment sur des serveurs d'information (*New-Server*) en Suisse.

La lutte contre la criminalité multiple sur Internet ne peut se contenter de la création de cyberpoliciers mais nécessite (en plus) la constitution d'un savoir spécialisé pour les autorités de poursuite pénale compétentes.

3. Les acteurs d'Internet[9]

Les différentes personnes et organisations actives sur Internet peuvent être classées dans les groupes suivants (toutefois, les limites sont parfois floues et certaines personnes peuvent remplir plusieurs fonctions) :

- **Utilisateurs / Users**: les personnes qui demandent les services proposés sur Internet.
- **Opérateurs / Carriers**: ils exploitent l'infrastructure de base pour relier les segments de réseau (systèmes de transmission et lignes). Il s'agit par exemple de Swisscom, Sunrise ou diAx[10].
- **Network-Providers**: les personnes ou organisations qui louent l'infrastructure de transmission de base (lignes louées) aux opérateurs et qui, à l'aide de routeurs, exploitent des réseaux complexes qui permettent aux ISP de se connecter à Internet (ex.: ip-plus, Eunet, etc.)[11].
- **Fournisseurs de services Internet (ISP)**: ils permettent à l'utilisateur d'accéder à Internet (au sens de la fonction de **fournisseur d'accès** / ***Access-Provider***) et proposent aussi généralement des services, par exemple via des serveurs Web, de messagerie ou d'informations (p. ex.: Swiss Online, Bluewin, Datacomm, etc.). En l'occurrence, l'intérêt porte particulièrement sur la fourniture d'accès (**fournisseurs d'accès**) et la mise à disposition de capacité de stockage sur les serveurs Web (**fournisseurs d'hébergement / *Hosting-Providers***).
- **Fournisseurs de services en ligne** ou **Online-Service-Providers**: à la différence des ISP, ils offrent principalement des services "propriétaires" (en particulier offres de données) qu'ils enregistrent sur des ordinateurs personnels et qui ne peuvent être consultés que par les abonnés du service en ligne. Ils assument en plus la fonction d'ISP. Les fournisseurs de services en ligne seront confondus par la suite avec l'appellation "fournisseurs d'accès Internet" ou ISP. Les exemples les plus connus sont AOL et Compuserve.
- **Fournisseurs de contenu** ou **Content-Providers**: les personnes qui rendent accessibles des informations personnelles sur les serveurs d'ISP ou des services en ligne (ou sur leur propre ordinateur). Il peut s'agir, par exemple, de l'auteur d'un article pour un groupe de discussion (newsgroup) ou une entreprise présente sur le Web.

---

[9] Cf. les commentaires d'Ulrich Sieber dans l'article "Kontrollmöglichkeiten zur Verhinderung rechtswidriger Inhalte in Computernetzen", dans Computer und Recht 10/97, p. 597, ainsi que les explications d'Andreas Ochsenbein et de Peter L. Heinzmann dans l'étude "Strafrechtliche Aspekte im Internet", dans Kriminalistik 7/98, p. 516 s.

[10] Tant pour les opérateurs que pour les fournisseurs de réseau, il faut retenir que, principalement pour des raisons d'organisation par couche de l'architecture de réseau, il n'existe pas de mesures de contrôle ou d'ingérence fondées pénalement (voir Ulrich Sieber, "Verantwortlichkeit im Internet", Beck'sche Verlagsbuchhandlung, Munich 1999, p. 27).

[11] Cf. note 9

4. Applications Internet (services)

Selon qu'une application Internet est publique ou que l'auteur d'une information ne veut atteindre que les destinataires désignés par lui, les applications les plus fréquentes peuvent être réparties comme suit :

- **Publiques** : WWW, groupes d'informations accessibles librement, serveurs FTP (autant que l'accès n'est pas limité), forums de discussion accessibles librement.
- **Non publiques** et donc protégées par le secret des télécommunications[12] dont: E-mails[13], groupes de discussion privés, téléphonie via Internet[14].

5. Types de responsabilité pénale

L'avis de droit de l'OFJ mentionné dans l'introduction indique de manière précise sur la base de quelles dispositions du CP la responsabilité pénale d'un fournisseur d'accès peut être engagée. Les considérations de cet avis peuvent aussi servir à déduire la responsabilité pénale pour les autres fonctions d'un ISP et des autres fonctions sur Internet.

Pour résumer, l'avis stipule les **points suivants :**

- **Tous les délits relatifs au contenu des médias n'entraînent pas une application du droit pénal des médias.** En sont exclus notamment les délits visés par les art. 135 (représentation de la violence), 197 (pornographie) et 261bis du CP (discrimination raciale)[15] (pt 4.3 de l'avis).
- En ce qui concerne les délits relatifs au contenu des médias menant à l'application du droit pénal des médias, **seul l'auteur[16] est en principe punissable**. Cela vaut également pour Internet (pts 5.2.1 et 5.3.1).
- En vertu du système du droit pénal des médias (art. 27 en relation avec l'art. 322bis CP), il est obligatoire **d'indiquer une personne responsable de la publication, même en l'absence de l'auteur**. Il peut et doit être tenu compte de l'éventuelle relative responsabilité de la personne plus éloignée dans l'ordre des responsabilités lors de l'application de l'art. 322bis CP (pt 5.2.2 *in fine*).
- Le **fournisseur d'hébergement** peut être considéré comme le **responsable secondaire** éventuel pour ce qui est des personnes actives sur Internet et du droit pénal des médias (pt 5.3.3.2).
- ”S'il "est absent" comme personne secondairement responsable, il semble légitime de considérer le **fournisseur d'accès** comme **responsable secondaire** (pts 5.3.3.3. et 5.3.4). Dans ce cas, il faut fixer certaines limites, au besoin très étroites (pt 5.3.3.4).

---

[12] Art. 13, al. 1, Cst.; art. 43 de la loi sur les télécommunications (LTC/RS 784.10)
[13] Sur plainte de droit public de la société Swiss Online SA, le Tribunal fédéral est parvenu à la conclusion le 5.4.2000 (numéro de dossier 1A.104/1999) que le trafic des e-mails était protégé par le secret des télécommunications et qu'il ne peut être surveillé que dans les conditions prévues à l'art. 179^{octies} CP (cf. NZZ du 6.4.2000).
[14] Les groupes d'utilisateurs privés généralement créés sur un Intranet ou Extranet peuvent aussi être considérés comme non publics. Selon la taille et la structure, il est possible néanmoins de considérer dans ce groupe un caractère public, au sens de l'art.261bis CP par exemple.
[15] L'arrêt du Tribunal fédéral cité dans le rapport sous le numéro de dossier 6S. 810-813/1998 a depuis été publié sous la référence 125 IV 206.
[16] Au sens des fonctions répertoriées sous le point 3, il s'agit des fournisseurs de contenu.

- En ce qui concerne la connaissance relative à un contenu spécifique sur Internet nécessaire pour qualifier les **actes** visés par l'art. 322bis CP **d'intentionnels**, il n'est ni possible ni raisonnable pour le fournisseur d'accès d'effectuer lui-même les contrôles. **Les informations de tiers** sur de tels contenus **doivent être concrètes et émaner d'une source fiable** (pt 6.1.2).
- La connaissance, pertinente sur le plan juridique, du fournisseur d'accès relativement à un contenu délictueux ne peut être reconnue que si l'information correspondante émane d'une **instance de procédure pénale**, par exemple d'un juge d'instruction ou d'un procureur. Les simples affirmations de particuliers ou les communiqués de presse généraux ne peuvent généralement pas suffire pour prouver une connaissance pertinente quant à l'intention (pt 6.1.2).
- La réalisation intentionnelle de l'état de fait visé par l'art. 322bis CP par un fournisseur d'accès est certes possible mais cela ne se produit pas fréquemment dans la pratique. **Il est plus probable** que l'on soit confronté à des cas où il faut traiter avec **une intention éventuelle** (pt 6.1.4).
- En ce qui concerne l'**acte de négligence** de l'art. 322bis CP, le devoir d'agir en toute diligence se fonde notamment sur le degré de risque général où toute personne qui crée une situation de risque doit tout mettre en œuvre pour que ce danger n'entraîne pas la violation de biens juridiques de tiers. **Le fournisseur d'accès doit mettre en œuvre tout ce qui est raisonnablement possible pour que l'utilisateur final n'ait pas accès aux contenus délictueux** (pt 6.2.2).
- **L'acceptabilité se mesure par des critères objectifs et les rapports personnels** (pt 6.2.3). Ces derniers doivent être déterminés au cas par cas pour chaque malfaiteur (point 6.2.3.2).
- Pour ce qui est des circonstances objectives, le devoir de diligence du fournisseur (d'accès) ne s'applique généralement que si ce dernier détient une **information concrète et fiable sur un contenu délictueux**, ce qui est le cas lorsque le renseignement émane d'une autorité suisse de poursuite pénale (pt 6.2.3.1).
- En raison du caractère qualifié de la connaissance préalable, **une réalisation par négligence de l'état de fait visé par l'art. 322bis CP ne se produit que dans de rares cas exceptionnels** (pt 6.2.4).
- **Pour résumer, on peut retenir à propos de l'étendue de la responsabilité du fournisseur d'accès que sa position de responsable à titre subsidiaire ou de "second rang" a une influence très limitée sur la portée réelle de sa responsabilité pénale: il ne peut être admis ou supposé à la légère qu'il connaisse le contenu délictueux, mais des informations concrètes doivent être fournies par les autorités suisses de poursuite pénale** (pt 6.3).
- La punissabilité du fournisseur d'accès en matière de délits créés par le contenu des médias qui ne tombent pas sous le coup des dispositions spéciales du droit pénal des médias suit les **règles générales de participation** selon lesquelles les fournisseurs d'accès peuvent être punis de complicité pour une infraction principale s'ils ne prennent pas les mesures requises malgré la connaissance du contenu délictueux sur Internet (pt 7).
- La connaissance du contenu délictueux par le fournisseur est déterminante pour la reconnaissance d'une complicité répréhensible car celle-ci ne peut être réalisée qu'intentionnellement (pt 7).

- Il ne peut être demandé au fournisseur d'accès, comme complice possible, de surveiller les contenus transitant par son installation. **La connaissance de l'existence de certains contenus punissables** doit lui être apportée par la remarque de tiers (pt 7).
- L'information donnée par une autorité de poursuite pénale au fournisseur d'accès relativement à des contenus concrets du réseau doit être jugée comme suffisante. Les communications faites par des personnes privées ne devraient remplir qu'exceptionnellement les conditions requises (pt 7).

En ce qui concerne la participation possible évoquée du fournisseur d'accès comme complice de l'auteur d'une infraction principale, il faut par ailleurs se référer au point 1.5 de l'avis de droit selon lequel la doctrine déterminante postule une application - souvent illimitée - du principe d'ubiquité (art. 7 CP) aux délits suscités par Internet, lesquels sont fréquemment conçus comme des délits matériels (*Erfolgsdelikte*). En l'occurrence, **le droit pénal suisse est applicable, quand bien même - comme c'est souvent le cas - l'infraction principale a été commise à l'étranger**[17].

Pour ce qui est de l'argument voulant qu'une complicité possible n'entre pas en ligne de compte parce que le service fourni par le fournisseur d'accès représente un acte neutre de tous les jours, il faut se référer au point 5.3.3.4 de l'avis précisant que le Tribunal fédéral a rejeté ce type de considération appliquée aux réseaux de communication.

Face à ces considérations de l'OFJ s'appliquant en premier lieu aux fournisseurs d'accès, les compléments suivants doivent être apportés pour ce qui a trait aux **fournisseurs d'hébergement**:

Le fournisseur d'hébergement est lié par un contrat avec le fournisseur de contenu pour ce qui est de la capacité de stockage mise à disposition sur le serveur Web. En ce qui concerne le droit pénal des médias, il est donc aussi considéré comme responsable secondaire[18] (pts 5.3.3.2 de l'avis de droit de l'OFJ).

Comme pour le fournisseur d'accès, **la connaissance revêt aussi une importance prépondérante pour le fournisseur d'hébergement** pour concrétiser l'intention d'un acte au sens de l'art. 322bis CP. Cette connaissance est également nécessaire pour faire appliquer le devoir de diligence dans le cas de la commission par négligence (voir avis du BJ, pt 6.2.4).

Outre les informations provenant de sources concrètes et fiables fondant la responsabilité pénale d'un fournisseur d'hébergement, une autre question se pose pour savoir si des informations moins qualifiées suffisent ou s'il faut présumer qu'il appartient au fournisseur d'hébergement de contrôler lui-même le contenu de son serveur Web. Ces questions s'appliquent principalement aussi aux fournisseurs qui mettent à disposition gratuitement des capacités de stockage de leur serveur Web ou qui permettent au fournisseur de contenu un accès non vérifié.

Etant donné que le **contenu du serveur Web** d'un fournisseur d'hébergement est déterminé et modifié en général par le fournisseur de contenu sans l'aide du fournisseur d'hébergement, la connaissance des contenus par ce dernier ne pourrait s'acquérir que par des contrôles régulièrement répétés. Vu les énormes quantités de

[17] En ce qui concerne l'infraction au sens de l'art. 322bis CP, la question de l'infraction principale préalable ne se pose pas car l'art. 322bis CP concerne une infraction autonome (avis de l'OFJ ; pt 5.3.3.4).
[18] Le principe de la responsabilité primaire et exclusive du fournisseur de contenu / auteur s'applique naturellement ici aussi.

données contenues sur un serveur Web, de tels contrôles relèveraient de la gageure et ne peuvent donc pas être imposés[19]. Il se peut néanmoins que le fournisseur d'hébergement, à de rares occasions, doive émettre des doutes fondés quant à la légalité de l'utilisation faite de la capacité de stockage mise à la disposition du fournisseur de contenu, et ce sur la base d'informations obtenues, par exemple, lors de la conclusion du contrat avec le fournisseur de contenu. Dans ce cas, il peut lui être imposé de **contrôler** les contenus de ce fournisseur **au moins par sondage**, pour ne pas se voir accusé de complicité intentionnelle (éventuelle).

Comme le volume de données stockées sur le serveur Web est moins grand que celui transitant par l'infrastructure d'accès et que le fournisseur d'hébergement est le suivant dans la chaîne des intermédiaires entre le fournisseur de contenu et l'utilisateur, il doit être exigé du fournisseur d'hébergement qu'il recherche - contrairement au fournisseur d'accès - des informations détaillées et concrètes même si elles ne proviennent pas d'une source pouvant être assimilée à une instance de procédure pénale. Ce **devoir supplémentaire - rechercher des informations - du fournisseur d'hébergement par rapport au fournisseur d'accès** se justifie moins par des raisons de proximité technique avec le fournisseur de contenu que par le fait que les deux parties se trouvent liés contractuellement. Dans certains cas, ces informations peuvent conduire à ce que le fournisseur d'hébergement doivent faire des recherches supplémentaires avec l'aide d'une autorité répressive ou de tiers professionnellement qualifiés[20,21]. Mais régulièrement, l'estimation parallèle dans la sphère non professionnelle devrait suffire pour répondre à la question de savoir si un contenu déterminé est punissable. Pour cela, le fournisseur d'hébergement doit évaluer, en tenant compte de ses vues, de son environnement et de l'interprétation des dispositions légales, si un contenu doit être considéré comme non autorisé[22].

Il reste à ajouter au sujet de ces explications qu'elles ne concernent - d'un point de vue pénal - le fournisseur d'hébergement que si le fournisseur de contenu ne peut pas être trouvé ou qu'il ne peut pas être poursuivi en justice dans notre pays.

Pour ce qui est de la participation à des délits ne tombant pas sous le coup des dispositions spéciales du droit pénal des médias, on peut ajouter aux développements de l'avis de droit de l'OFJ les éléments suivants pour le fournisseur d'hébergement:

On ne parle généralement **que de la complicité** au sens de l'art. 25 CP[23] comme forme de participation possible. La proximité fonctionnelle et juridique du fournisseur d'hébergement et du fournisseur de contenu ainsi que la quantité de données plus réduite sur son serveur Web – par rapport au volume de données transitant par le fournisseur d'accès – a pour conséquence, au niveau de l'élément de connaissance de la complicité intentionnelle, qu'il faut exiger de lui la même attitude que celle prévue à l'art. 322bis CP: il faut rechercher, en plus des informations qualifiées provenant des autorités de poursuite pénale, des renseignements détaillés et concrets émanant d'autres sources.

---

[19] Voir aussi Ochsenbein / Heinzmann, loc. cit., p. 602 ss.
[20] Cf. Internet, Le Nouveau Média Interroge le Droit, loc. cit., p. 10 ss. (les commentaires qui y sont faits se rapportent, il est vrai, à la complicité et non au droit pénal des médias; ils peuvent néanmoins être utilisés pour l'élément de connaissance d'un acte au sens de l'art. 322bis CP)
[21] Le risque de "censure privée" dont il est question dans l'avis de l'OFJ (pt 6.1.2) et qui peut être craint en raison de la diminution de la demande de qualité des informations n'est pas aussi présent dans les rapports entre les fournisseurs de contenu et d'hébergement car, en vertu de la liberté de contrat, le fournisseur d'hébergement est libre de mettre son serveur à la disposition de qui il veut et pour quoi.
[22] Schultz, AT I CP, 4e édition, Berne 1982, p. 190 s.
[23] Voir Internet, Le Nouveau Média Interroge Le Droit, loc. cit., p. 8

Dans les développements exposés jusqu'ici, il a surtout été question des contenus du World Wide Web. **Mais, d'un point de vue pénal, la même chose vaut en principe aussi pour les contenus des serveurs d'informations ou FTP**.

S'agissant des contenus diffusés sur des serveurs d'informations, une surveillance active n'est pas envisageable à cause des énormes volumes de données et des contenus sans cesse variables[24]. Pour autant qu'un serveur d'informations ne contienne pas exclusivement des groupes de la branche, la liberté d'information interdit le blocage de l'accès à un tel serveur. Il faut cependant exiger de l'exploitant de serveurs d'informations qu'il recherche des renseignements détaillés et concrets sur les groupes dont les sites ont un contenu punissable. Comme les contenus d'un groupe présentent souvent de grandes différences qualitatives, un renseignement sur des messages isolés d'un groupe ne permet pas de fonder l'exactitude de la connaissance, d'autant que les différents messages sont automatiquement effacés au bout d'une période relativement courte. Mais si on peut déduire de cette information que des messages au contenu punissable sont régulièrement et principalement envoyés dans un groupe, il faut vérifier l'information et au besoin supprimer ce groupe (ainsi qu'empêcher sa réapparition automatique).

En ce qui concerne les **serveurs FTP**, les questions de responsabilité pénale se posent en premier lieu à l'exploitant d'un tel serveur, alors que la possibilité d'un blocage ciblé de l'accès (à certains répertoires ou fichiers) peut être exclu par le fournisseur d'accès en raison des particularités techniques[25]. L'exploitant d'un serveur FTP qui autorise le stockage libre de données doit faire son enquête. On ne peut cependant attendre de lui à ce niveau qu'il utilise, pour lire les fichiers, des logiciels qui ne peuvent être considérés comme habituels pour sa branche.

Il est clair que la question d'un blocage d'accès ou d'un contrôle de contenu n'entre pas en ligne de compte pour les **serveurs de discussion Internet** (Internet Relay Chat-Server). La rapidité du passage des données ne permet pas d'établir une connaissance pénalement pertinente[26].

6. Aspects techniques d'un blocage d'accès[27]

Des questions techniques complexes se posent au sujet de l'accès à des contenus illicites de serveurs WWW en raison de leur large diffusion et de la présence relativement longue des contenus sur les serveurs. Comme déjà mentionné, il faut partir du principe que l'auteur réel ou le fournisseur d'hébergement ne peut légalement pas être poursuivi dans de nombreux cas (ex.: les serveurs localisés aux USA et au Canada sont protégés par la liberté d'expression). C'est pourquoi la "deuxième meilleure" solution consiste en un blocage de l'accès à de tels contenus par les fournisseurs suisses d'accès à Internet ou de réseau.

De quelles possibilités un fournisseur de services Internet dispose-t-il pour bloquer un contenu déterminé sur un serveur WWW?

---

[24] Cf. Ulrich Sieber, Verantwortlichkeit im Internet, p. 51

[25] Le blocage de l'accès à tout un serveur FTP est à peine imaginable car celui-ci contient généralement aussi des fichiers non punissables pénalement.

[26] Voir à ce sujet Ulrich Sieber, Verantwortlichkeit im Internet, p. 40 ss. et 57 ss.

[27] Pour les aspects techniques, voir Rosenthal, David: Current Problems and Possible Strategies for Combating Racism on the Internet (http://www.rvo.ch/docs/unracism.pdf), ainsi que Sieber Ulrich: Verantwortlichkeit im Internet – Technische Kontrollmöglichkeiten und multimediarechtliche Regelungen (Beck: Munich 1999).

1. Le fournisseur **bloque l'adresse IP** du serveur Web concerné au niveau du routeur. Cette mesure entraîne le blocage de *toutes* les offres présentes sur le serveur et non pas seulement le contenu incriminé. Cette procédure n'est donc pas une solution praticable pour les gros fournisseurs tels que AOL ou Geocities qui contiennent des milliers de contenus différents. Elle convient davantage aux offres illicites ayant leur propre serveur / nom pour lesquelles un nom de domaine déterminé ou une adresse IP précise ne présente que des contenus similaires (p. ex. racistes ou extrémistes violents). Dans le cas des contenus racistes et extrémistes, cette situation est relativement fréquente car ces fournisseurs de contenu veulent tirer avantage de noms de domaine faciles à retenir (p. ex.: stormfront.org, aryanbooks.com). Les sites Web que la Police fédérale recommande actuellement de bloquer correspondent à cette catégorie.
   Une variante de cette solution consiste à exclure certains noms de domaine (tels que stormfront.org) au niveau du DNS (Domain Name Server ou serveur de nom de domaine).
2. Le fournisseur exploite un **serveur proxy**. Toutes les consultations du WWW (p. ex.: Port 80) entrent dans la configuration de base du navigateur Web via ce proxy. Ce dernier permet alors l'enregistrement des consultations, le stockage temporaire des données demandées mais aussi leur blocage. Le client doit configurer son navigateur Web en conséquence. S'il ne le fait pas, le serveur proxy est contourné et la communication est établie directement avec le site souhaité. La plupart des fournisseurs exploitent de tels serveurs proxy, mais dans le but d'accroître les performances. Il existe également des proxies pour d'autres protocoles que le http, comme par exemple le FTP.
3. Le fournisseur utilise un "**proxy transparent**", de sorte que les clients se servent automatiquement du serveur proxy, qu'ils le veuillent ou non. Dans le proxy, il est possible d'instaurer un blocage jusqu'au niveau d'une page précise. En principe, il s'agit ici d'un firewall ouvert qui peut dévier et éventuellement filtrer certains services[28].

Une modification de la variante 1 est aujourd'hui utilisée pour interdire l'accès à des sites Web dont le blocage est recommandé par la Police fédérale.

Toutes les variantes ont néanmoins en commun **certains inconvénients**:

a) Tous les types de filtrage entraînent des **problèmes de performance**, les méthodes pouvant difficilement évoluer. Ce qui fonctionne correctement pour une douzaine d'adresses mène à une interruption de l'infrastructure du fournisseur pour quelques millier d'autres.

b) Toutes les méthodes citées peuvent être contournées par l'utilisation d'un **anonymizer** qui masque l'adresse IP du contenu recherché.

c) L'expérience montre que les sites Web bloqués sont stockés par la communauté Internet sur plusieurs serveurs en copie intégrale (**mirroring** ou mise en miroir) car de tels procédés sont interprétés – presque par réflexe - par beaucoup d'utilisateurs comme une censure. Tous ces sites Web ont dû à nouveau être bloqués.

d) Le **coût** de mise à jour et de gestion de listes de blocage est élevé pour les fournisseurs. La méthode de blocage entraîne également des investissements élevés

[28] Un problème identique se pose néanmoins ici comme pour les serveurs proxy normaux. Selon les paramètres, il bloque l'accès à des services utilisant des protocoles ou des ports spéciaux (p. ex.: le télébanking).

variant selon le procédé choisi. Plus de 300 fournisseurs actifs sont actuellement recensés en Suisse, les grandes entreprises et les administrations publiques / écoles n'étant pas prises en compte. Même pour les services policiers / juridiques demandant les blocages, les frais administratifs ne doivent pas être sous-estimés. Une aide pourrait être apportée jusqu'à un certain degré par le blocage au niveau des fournisseurs de réseau sur lesquels s'appuie tout ISP.

e) Une solution nationale est en principe problématique dans le monde d'Internet. Grâce aux tarifs téléphoniques relativement bas actuellement, un client suisse peut choisir un fournisseur étranger (sans blocages). Certains fournisseurs de services en ligne (p. ex.: AOL) proposent en plus, d'après leurs propres indications, l'accès à Internet dans toute l'Europe via le même réseau; dans ce cas, un blocage uniquement valable pour la Suisse ne serait pas réalisable avec cette topologie de réseau.

Bilan de l'aspect technique:

Le blocage de sites Web complets (nom de domaine ou adresse IP) est réalisable pour les fournisseurs de services Internet ou pour les réseaux mais ne convient pas dans tous les cas (si le contenu illicite ne représente qu'une partie de l'offre, p. ex. pour les sociétés d'hébergement sur le Web) et est très onéreux selon la méthode choisie.

Les inconvénients de toutes les solutions techniques au niveau national sont les efforts administratifs et financiers relativement élevés ainsi que la possibilité de contournement par l'utilisateur qui ne recule pas devant une dépense certaine. L'effort administratif nécessaire de la part des fournisseurs pourrait cependant être réduit si **une seule instance** était désignée en Suisse pour les blocages et si cette instance mettait régulièrement à disposition les données nécessaires (adresses IP, noms de domaine) dans un **format lisible par les machines**. Si les grands **fournisseurs suisses de réseau** (comme ip-plus, Eunet, etc.) effectuaient les blocages à titre de service pour leurs clients, la grande majorité des plus petits fournisseurs qui tirent leur capacité de ligne des fournisseurs de réseau en bénéficieraient automatiquement. Cette solution n'éliminerait toutefois pas l'obligation d'étudier de plus près la possibilité d'évolution.

En cas de solution future éventuelle au niveau international (voir à ce sujet le chapitre 11), il existerait de **nouvelles possibilités de blocage technique à la source** (p. ex.: les contenus racistes et extrémistes non punissables aux USA ne seraient plus visibles pour les Européens grâce à des dispositions techniques mises en œuvre par les fournisseurs d'hébergement).[29]

7. Acceptabilité et proportionnalité des blocages d'accès et des suppressions de contenus

Le caractère raisonnable ou déraisonnable d'une mesure est déterminé en partie par l'état de nécessité (art. 34 CP). Il est établi aussi par l'attitude de devoir vis-à-vis d'un

[29] Cette méthode a ainsi été utilisée jusqu'il y a peu pour empêcher les personnes qui ne sont pas citoyennes des USA de télécharger des navigateurs Internet sur les sites Web américains à l'aide d'un solide verrouillage.

délit commis par négligence[30], qui n'est plus pertinent en l'occurrence car un fournisseur de services Internet (que ce soit le fournisseur d'accès ou le fournisseur d'hébergement) qui a connaissance de contenus punissables et n'y réagit pas se comporte généralement de façon (éventuellement) intentionnelle[31].

Au sens d'un acte exécuté en état de nécessité, un tel comportement serait alors punissable si l'on ne pouvait exiger raisonnablement de l'ISP le sacrifice de son bien[32]. Le comportement raisonnable doit par conséquent être adapté aux circonstances, au sens de la pesée des biens juridiques opposés. Du fait que cette pondération des intérêts en conflit est exclusivement réservée aux tribunaux, il est impossible de fixer, dans le présent document, une règle générale permettant de déterminer à quel bien juridique il convient de donner la primauté, ce d'autant que ces biens [33] sont généralement difficiles à quantifier.

Pour ce qui est de l'acceptabilité dans une certaine mesure, il faut certainement tenir compte aussi des possibilités de contournement d'un blocage d'accès. Il convient néanmoins d'attirer l'attention sur le fait que la participation causale à un délit éventuellement réalisée par un fournisseur de services Internet suffit pour invoquer la complicité[34]. Quand bien même le blocage de l'accès ne peut pas être intégral pour les clients suisses par leur fournisseur ou si un contenu du fournisseur de contenu à effacer peut être placé sur le serveur d'un autre fournisseur d'hébergement, une telle procédure se justifie en principe même pour des quotas de réussite inférieurs à 100 % - à l'instar des missions de prévention de la police ou de la douane.

Ces développements valables pour ce qui concerne la complicité s'appliquent également par analogie à la responsabilité subsidiaire du fournisseur de services Internet conformément au droit pénal des médias, d'autant que la question de causalité ne se pose pas en raison du fait que l'art. 322bis CP vise un délit autonome.

---

[30] Voir Trechsel/Noll, CP AT I, 4e édition, Zurich 1994, p. 243
[31] Voir à ce sujet le résumé de l'avis de droit de l'OFJ sous le pt 8
[32] En premier lieu, son bien qui, d'une part, peut consister en un avantage de concurrence par un accès illimité et qui, d'autre part, peut être diminué par le recours nécessaire à des ressources techniques et humaines.
[33] Outre son bien, d'un côté, entrent en considération, de l'autre: la protection de la jeunesse et la protection de l'intégrité sexuelle conformément à l'art. 197 CP; le respect de la paix publique, de la dignité humaine ou de la protection du sentiment d'être respecté par les autres comme un autre en vertu de l'art. 261bis CP; le bien et le droit de disposer de soi-même pour les droits de propriété intellectuelle.
[34] Cf. ATF 120 IV 272 selon lequel "la complicité doit augmenter les chances de réussite d'un acte réunissant les éléments constitutifs d'une infraction"; ATF 119 IV 292: "Selon la jurisprudence, est réputée complicité toute contribution causale à l'acte, dans la mesure où cet acte se serait déroulé autrement sans l'aide du complice. Il n'est pas indispensable que l'acte n'aurait pas pu être réalisé sans la complicité."

Face à la situation légale et technique, les mesures suivantes doivent être considérées comme raisonnables [35] :

- **Si un fournisseur d'accès reçoit des autorités répressives des informations détaillées et concrètes sur des contenus qui présentent un caractère pénal, il veille au blocage de l'accès à ces sites** au sens des mesures répertoriées sous le point 6. Font partie de ces mesures: le blocage de l'adresse IP si le contenu punissable est stocké sur un **site ayant sa propre adresse IP,** ainsi que le blocage de l'URL incriminé dans le serveur proxy.

- **Si un fournisseur d'hébergement dispose d'informations concrètes et détaillées (ne provenant pas exclusivement d'autorités répressives) sur des contenus punissables se trouvant sur un de ses serveurs, il veille à ce que ces contenus ne soient plus accessibles ou soient effacés. Si ces renseignements n'émanent pas d'une autorité répressive, il doit lui même procéder aux recherches complémentaire nécessaires, au besoin en faisant appel à une autorité de poursuite pénale ou à des tiers professionnellement qualifiés. Le même principe s'applique s'il dispose d'informations obtenues grâce à ses relations contractuelles avec le fournisseur de contenu le faisant douter de la légalité de l'utilisation de la capacité mise à disposition**.

[35] Demeurent naturellement réservés le jugement par les tribunaux du caractère raisonnable (dans chaque cas d'espèce) et la question de savoir si un comportement punissable du fournisseur est donné .

8. Attitude exigée des fournisseurs sous l'angle de la responsabilité pénale

En guise de conclusion, l'attitude suivante est attendu des fournisseurs de services:

8.1. Fournisseurs d'accès:

- Si le fournisseur d'accès est en possession d'indices concrets émanant d'une autorité de poursuite pénale et liés à de présumés contenus illicites circulant sur le réseau, il est invité à procéder à des **blocages**, pour autant que ceux-ci soient raisonnables.
- **Il n'est pas concevable ni rationnel de rechercher activement et individuellement** des contenus répréhensibles sur Internet en raison du changement et de l'augmentation que subissent quotidiennement les données; une telle mesure ne peut donc être exigée.

8.2. Fournisseurs d'hébergement:

- Le fournisseur d'hébergement est tenu de rechercher des informations détaillées et concrètes liées à des **contenus du Web et à des groupes de discussion (newsgroups) illégaux.** S'il en trouve, ils doivent être **effacés** ou leur accès doit être **bloqué**.
- Etant donné que le fournisseur d'hébergement a des relations nettement plus étroites avec le fournisseur de contenu que le fournisseur d'accès, le fournisseur d'hébergement est tenu de **surveiller, du moins par sondage, les fournisseurs de contenus suspects**.
- En ce qui concerne les fichiers se trouvant sur des **serveurs FTP,** qui permettent le libre stockage des données, la surveillance est de mise pour autant que les fichiers puissent être lus par des logiciels de type classique.

8.3. Fournisseurs de services en ligne

- **Suivant l'organisation de leurs services,** les fournisseurs de services en ligne sont des **fournisseurs de contenu, d'hébergement ou d'accès.** La question de leur responsabilité pénale doit donc être envisagée selon leurs fonctions.

Pour tous les fournisseurs de services Internet, les points suivants s'appliquent:

- **Les dispositions mentionnées sous les points 8.1 à 8.3 se limitent aux services publics. Les services non publics, par contre, tombent sous le coup**

du secret des télécommunications. Aussi, ne peut-on attendre du fournisseur de services Internet qu'il ait connaissance du contenu ni qu'il prenne des dispositions à cet égard. Dès lors, une responsabilité pénale du fournisseur de services Internet peut par principe être exclue pour le domaine non public d'Internet.

- Le fournisseur de services Internet n'a **aucune obligation de dénoncer** des attitudes ou des contenus punissables vis-à-vis des autorités policières. Le **droit de dénonciation,** valable généralement, s'applique néanmoins. En cas de délit poursuivi sur plainte (p.ex. délits contre l'honneur, certaines infractions contre les droits d'auteur), soit le fournisseur de contenu peut être rendu attentif à la peine à laquelle il s'expose par son comportement, soit la personne concernée peut être informée de l'atteinte à ses droits.

- **En ce qui concerne les enquêtes pénales qui ne visent pas les fournisseurs, sont valables les devoirs généraux découlant du droit de procédure pénale appliqué (cantonal ou de la Confédération)**: devoir de déposer à titre de témoin, devoir de remettre des documents ou des informations prélevés dans des mémoires électroniques. En ce qui concerne les services protégés par le secret des télécommunications (e-mail, private-chat, téléphonie via Internet), les décisions des autorités compétentes selon la procédure pénale applicable[36] doivent être exécutées. Citons notamment:
  - **les renseignements sur le trafic Internet des utilisateurs clients du fournisseur de services Internet**[37]. Ces renseignements doivent autant que possible être fournis en temps réel, c'est-à-dire que, pour autant que la technique le permette, il s'agit de procéder à une surveillance directe[38]. L'autorité qui ordonne la surveillance (elle confie le soin d'exécuter la mesure au Service des tâches spéciales du DETEC[39]) doit dédommager le fournisseur de manière appropriée[40].
  - les données personnelles de chaque utilisateur relatives au trafic et à la facturation qui sont stockées dans les fichiers log. Ces données doivent pouvoir être mises à la disposition des autorités compétentes pendant au moins six mois[41].

- Les frais qui découlent des **mesures de blocage ou de suppression** se justifient en raison de la responsabilité pénale prévue dans le droit pénal des médias ou par la complicité possible avec l'infraction principale. Ces mesures représentent un comportement normal sous l'angle du droit pénal, lequel ne doit pas être dédommagé.

---

[36] en relation avec l'art. 44 LTC
[37] art. 44, al. 1, LTC
[38] art. 44, al. 2, LTC
[39] cf. ordonnance du 1er décembre 1997 sur le service de surveillance de la correspondance postale et des télécommunications (RS 780.11)
[40] cf. ordonnance du 12 décembre 1997 sur les émoluments et les indemnités en matière de surveillance la correspondance postale et des télécommunications (RS 780.115.1)
[41] (dans le cadre de la surveillance des télécommunications selon l'art. 44 LTC) art. 50 de l'ordonnance sur les services de télécommunications (OST; RS 784.101.1)

9. Attitude à attendre de la Confédération

- En cas de connaissance de contenus illicites, des dénonciations (contre les fournisseurs de contenu) seront d'abord déposées auprès des autorités compétentes au niveau cantonal, ou la présence de ces contenus sera communiquée aux autorités étrangères, pour que **l'infraction principale et les auteurs principaux** soient **poursuivis** en premier lieu.
- L'administration fédérale **apporte son soutien** - pour autant qu'elle dispose des connaissances spécialisées nécessaires - aux fournisseurs, qui doivent juger du caractère éventuellement répréhensible des contenus et mettre en œuvre de mesures de blocage de nature technique.

10. Autres angles d'action

Collaboration internationale renforcée
Outre le blocage, il existe d'autres possibilités - mais **plutôt efficaces à moyen terme** - de lutter contre les contenus illégaux sur Internet. C'est ainsi que la Police fédérale et d'autres offices ont intensifié leur collaboration avec des partenaires étrangers pour tendre à une convergence des points de vue et de la poursuite pénale en matière de contenus illicites sur Internet.

Unification du droit
Une harmonisation internationale des états de fait juridiques - un droit "(plus) compatible avec Internet" - serait certes souhaitable mais n'est pas prévue dans un avenir proche. Les Etats-Unis pourraient être un partenaire important quoiqu'ils favorisent ,involontairement, l'antisémitisme et le racisme à l'échelon international en hébergeant des sites Web extrémistes et racistes.

Accords internationaux sur les contenus illicites
Une solution réaliste consisterait à ratifier les accords internationaux concernant les contenus illicites diffusés sur Internet. Voici les **quelques ébauches** existant déjà:

- Conseil de l'Europe: Recommandation du Comité des Ministres du Conseil de l'Europe sur la criminalité en relation avec l'ordinateur (R (89) 9) et Recommandation relative aux problèmes de procédure pénale liée à la technologie de l'information (R (95) 13).[42] En 1997, un comité d'experts a été appelé à se pencher sur le thème du "crime in cyber-space" et devrait présenter fin 2000 un projet de convention internationale pour la lutte contre la criminalité sur Internet.[43]
- OCDE: Proposition française présentée à l'OCDE pour une Charte de coopération internationale sur Internet, qui pose également les principes d'une coopération en matière de poursuite pénale.[44]
- UE: plan d'action pluriannuel (1999-2002) de lutte contre les "messages à contenu illicite et préjudiciable diffusés sur les réseaux mondiaux" du 25.1.1999.[45] Le

[42] www.privacy.org/pi/agreements.html
[43] Les "terms of reference" qui ont depuis été prolongés de fin 1999 à fin 2000 peuvent être consultés sur le site Web du Conseil de l'Europe: http://www.coe.fr/cm/dec/1997/583/583.a13.html
[44] www.telecom.gouv.fr/francais/activ/techno/charteint.htm
[45] http://www.europa.eu.int/eur-lex/fr/lif/dat/1999/fr_399D0276.html

projet de l'UE se limite de prime abord à l'autoréglementation des fournisseurs (règles déontologiques) et aux mesures techniques combinables (outils de classement et de filtrage). Des mécanismes de "signalement" par ligne téléphonique directe devraient être prévus à l'échelon européen pour permettre aux utilisateurs de signaler des contenus qu'ils jugent illégaux.

- En novembre 1997, l'ONU a tenu à Genève un séminaire sur ce thème et a demandé à ses Etats membres d'adapter et d'harmoniser leurs législations nationales.
- La Commission des Communautés européennes a adopté le 18 novembre 1998 la proposition de directive du Parlement européen et du Conseil relative à certains aspects juridiques du commerce électronique dans le marché intérieur[46]. L'article 12, disposition particulièrement intéressante, dispose que la responsabilité du prestataire ne peut être engagée pour le "simple transport" (au sens du terme "accès" employé dans le présent avis). Aux termes de l'art. 13, ce principe vaut aussi pour la forme de stockage dit "caching". En ce qui concerne l'hébergement, l'art. 14 stipule que la responsabilité du fournisseur d'hébergement ne peut être engagée sauf s'il a effectivement connaissance de l'activité illégale de l'utilisateur. L'art. 15 ne prévoit, pour les fournisseurs de services visés aux art. 12 à 14, aucune obligation de surveillance sauf s'ils y sont invités par les autorités judiciaires[47]. Dans la position commune du Conseil du 28.2.2000 concernant cette proposition de directive, il a été précisé que la directive n'était pas destinée à harmoniser le domaine du droit pénal. En ce qui concerne les art. 12 à 14 de la proposition de directive, de nouveaux paragraphes 3 prévoient la possibilité de dispositions juridiques et administratives. Enfin, l'art. 15 de la directive n'empêche pas les Etats membres d'instaurer, pour les fournisseurs de services Internet[48], l'obligation de coopérer avec les autorités.
- Pour terminer, le Département fédéral des affaires étrangères a lancé l'idée d'une conférence internationale sur les contenus à caractère raciste diffusés sur Internet, lors de la conférence de Washington de novembre 1998 concernant les avoirs l'Holocauste. Il a reparlé de cette problématique dans le cadre de la Commission de l'ONU sur les droits de l'homme en mars 1999 et souhaite mettre sur pied, en collaboration avec d'autres Etats, une conférence internationale pour la lutte contre les sites Web à caractère raciste et antisémite. Les mesures de lutte élaborées à cette occasion devraient être approuvées lors de la conférence internationale contre le racisme prévue en 2001[49].

Collaboration plus étroite des fournisseurs, auto-contrôle

Une autre possibilité gage de succès en la matière consiste en une collaboration plus étroite des fournisseurs de services aux niveaux national et international. Ensemble, ceux-ci peuvent exercer une pression plus grande sur les fournisseurs d'autres pays pour les inciter à ne pas tolérer de tels contenus sur leurs serveurs même si la loi le permet théoriquement. **La base de cette collaboration serait constituée des différentes conditions générales et des codes de conduite des fournisseurs qui, à quelques exceptions près, refusent pour le moins les contenus à**

[46] Voir Ulrich Sieber, Verantwortlichkeit im Internet, p. 317 ss.
[47] Voir Ulrich Sieber, Verantwortlichkeit im Internet, p. 232 s.
[48] Voir la communication de la Commission du 29.2.2000 in PCE (2000) 386 définitif
[49] Voir à ce sujet un document rédigé pour une réunion de préparation à la conférence de 2001 à Genève: Rosenthal, David: Current Problems and Possible Strategies for Combating Racism on the Internet, janvier 2000 (http://www.rvo.ch/docs/unracism.pdf).

caractère raciste. L'expérience montre que les fournisseurs sont également disposés à réagir aux informations d'autres fournisseurs et de supprimer pareils contenus. De nombreux fournisseurs ont aussi installé une ligne téléphonique directe pour signaler l'existence de tels contenus; jusqu'à présent, ces lignes se limitent généralement à leurs propres serveurs. **Compte tenu de l'esprit de coopération qui caractérise les acteurs d'Internet, cette solution d'ordre général pourrait être intéressante et mener à un "Internet plus propre" grâce à un effort personnel**. On pourrait également s'inspirer de l'exemple de l'auto-contrôle introduit dans l'industrie des loisirs. La condition indispensable à cela serait l'acceptation d'une instance de jugement commune.

11. Et ensuite ?

Le groupe de contact ad hoc a demandé **une discussion approfondie au sujet des questions légales et techniques liées à la recommandation de blocage de la Police fédérale.** Le présent avis répond à cette exigence, même s'il subsiste certaines incertitudes imputables au développement sans précédent des technologies et au principe de l'indépendance fondamentale de la justice.

De plus, le groupe de contact a fait naître une meilleure prise de conscience en la matière tant au sein de l'administration fédérale que parmi les fournisseurs de services Internet.

En déterminant les conditions juridiques et techniques dans ce dossier, le groupe de contact a rempli son objectif initial.

La **nécessité d'une plate-forme de discussion commune et coordonnée** entre la Confédération et les fournisseurs de services Internet pourrait subsister à l'avenir et ce, indépendamment des recommandations de blocage de la Police fédérale. Voici ce que pourraient être les **besoins futurs** en matière **de coordination**:

- **coordination des indices concrets** émanant des autorités de poursuite pénale sur les contenus répréhensibles;
- harmonisation des **efforts** nationaux et internationaux **pour endiguer la criminalité sur Internet;**
- poursuite du **développement technique et juridique;**
- conseil et coordination des autorités cantonales de poursuite pénale dans **le traitement des dénonciations** sur des contenus illicites stockés à l'étranger;
- **unité de doctrine des autorités fédérales** face aux fournisseurs de services Internet;
- **interlocuteur unique** du côté des fournisseurs de services Internet;
- encouragement **à l'échange des connaissances et à la compréhension mutuelle.**

Il est possible de répondre diversement à ces besoins :

1. Abandon de la coordination

ex. parce que les besoins en matière de coordination ne sont pas considérés comme suffisamment patents pour justifier l'utilisation de ressources.

2. Chacun s'occupe de sa propre coordination

ex. parce que les intérêts de chaque groupe (fournisseurs de services Internet, autorités cantonales de poursuite pénale, administration fédérale) sont trop éloignés pour pouvoir mettre raisonnablement sur pied une plate-forme commune.

3. Création d'un organisme commun de coordination et d'information

ex. auprès d'un service privé indépendant de la Confédération et des fournisseurs de services Internet (organisation contre le racisme), ou à la Confédération (OFP, commission contre le racisme, DETEC, OFJ) ou auprès des fournisseurs (organisation centrale). Cette collaboration de la Confédération, des cantons et de l'économie privée devrait s'opérer de manière parfaitement transparente pour éviter toute accusation de censure.