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.