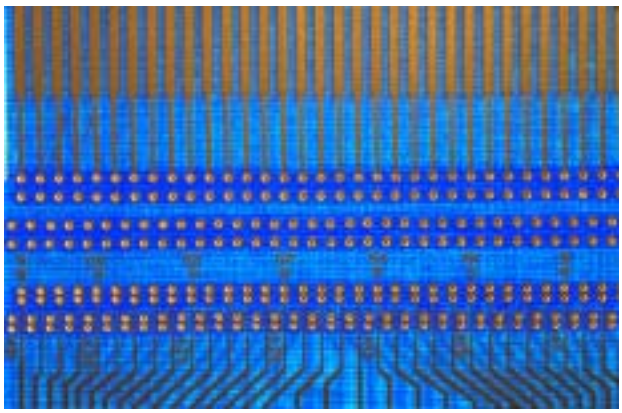
Netzwerk-



Kriminalität

Bericht der Expertenkommission

„Netzwerkkriminalität“

Eidg. Justiz- und Polizeidepartement
Bern, Juni 2003

Inhaltsverzeichnis

Abkürzungsverzeichnis und Glossar

a.a.O	am angegebenen Ort
a.F.	alte Fassung
a.M.	anderer Meinung
AB	Amtliches Bulletin der Bundesversammlung
ABl	Amtsblatt (Europäische Union)
Access-Provider	Zugangsdienstleister oder -vermittler
AJP	Aktuelle Juristische Praxis
BBl	Bundesblatt
BetmG	Betäubungsmittelgesetz (SR 812.121)
BGBl	Bundesgesetzblatt (Deutschland)
BGE	Bundesgerichtsentscheid
BGH	Bundesgerichtshof (Deutschland)
Bibl.	Bibliographie in diesem Bericht (S.12)
Browser	Darstellungprogramm für multimediale Inhalte, die mit sogenannten *Hyperlinks* (elektronischen Verweisen) miteinander verknüpft sind.
BÜPF	Bundesgesetz vom 6. Oktober 2000 betreffend die Überwachung des Post- und Fernmeldeverkehrs, SR 780.1
BV	Bundesverfassung, SR 101
Caching	Als *Cache* bezeichnet man einen Speicherbereich, auf den sehr schnell zugegriffen werden kann und der häufig zu lesende Daten aus einem anderen Speicher enthält. Beim Internet wird dies von Access-Providern zur Beschleunigung von Zugriffen ihrer Kunden auf populäre Webseiten verwendet.
Chat	Online-Kommunikation (Text, Ton, Bild) zwischen Internetbenutzern
Client	„Kunde"; ein an einem Netzwerk teilnehmender Computer
Content-Provider	Inhaltsanbieter
ders.	derselbe
DNS	*Domain Name System*: Das „Telefonbuch für das Internet" löst symbolische Namen wie z.B. www.bj.admin.ch in eine digitale Internetadresse auf.
Download	„Herunterladen" eines Internet-Inhalts auf den eigenen PC
E-Commerce	Electronic Commerce, elektronischer Handel über Internet
EGG	Elektronisches Geschäftsverkehr-Gesetz (Deutschland)
EJPD	Eidg. Justiz- und Polizeidepartement
E-Mail	Electronic Mail, elektronische Nachricht
EMRK	Europäische Menschenrechtskonvention, SR 0.101
FDV	Verordnung über die Fernmeldedienste, SR 784.101.1
File Sharing	Internetdienst, der es Endbenutzern erlaubt, die auf ihrem Rechner gespeicherten Dateien (z.B. Musik) anderen

	Internetbenutzern zum Herunterladen zur Verfügung zu stellen.
FMG	Fernmeldegesetz, SR 784.10
FN	Fussnote
FTP, ftp	*File Transfer Protocol*: Standardisiertes Protokoll zum Austausch von Dateien zwischen Client und Server.
GA	Goltdammer‘s Archiv für Strafrecht (Deutschland)
Hosting-Provider	Dienstleister, der seinen Kunden Speicherplatz auf einem Server zur Verfügung stellt
Hrsg.	Herausgeber
HTTP	*Hyper Text Transfer Protocol*: Das beim Worldwide Web verwendete Protokoll, mit welchem der Browser (siehe dort) auf Webseiten zugreifen kann
i.S.v.	im Sinne von
IP	*Internet-Protocol*: Das dem Internet zugrundliegende Protokoll zum kontrollierten weltweiten Austausch von Daten unabhängig vom verwendeten physischen Übertragungsmedium.
IPRG	Bundesgesetz über das Internationale Privatrecht, SR 291
ISP	*Internet Service Provider*: Internet Dienstanbieter
JO	Journal officiel de la République française
JZ	Juristenzeitung (Deutschland)
LAN	*Local Area Network*: Geschlossenes lokales Firmennetz
LFG	Luftfahrtgesetz, SR 748.0
Link	Verweis in einer Webseite auf eine andere Webseite oder auf multimediale Inhalte (Musik, Video).
m.N.	mit Nachweisen
m.w.H.	Mit weiteren Hinweisen
MMS	*Multimedia Messaging Service*: Übertragungsdienst für multimediale Daten zwischen Mobiltelefonen.
Monitoring	Durchforschen des Internet-Angebots durch eine staatliche Instanz.
MSchG	Markenschutzgesetz, SR 232.11)
N.	Note
n.F.	neue Fassung
Network-Provider	Netzdienstleister
Newsgroup	Elektronisches Diskussionsforum im Internet
OR	Obligationenrecht (SR 220)
P2P oder Peer-to-Peer	Protokolle zum direkten Datenaustausch zwischen Endbenutzern (siehe File-Sharing) ohne zentrale Vermittlungsinstanz.
PatG	Patentgesetz, SR 232.14
Proxy	*Proxies* sind Rechner, die zwischen lokale Netzwerke (LAN) und dem Internet geschaltet werden. Anstelle der einzelnen Rechner senden sie Datenpakete ans Internet und nehmen sie von dort entgegen. Proxies können die Geschwindigkeit der Verbindung steigern, indem sie als *Cache* (siehe dort)

	eingesetzt werden. Sie können auch zur Erhöhung der Sicherheit oder zur Kontrolle des Netzzugriffs verwendet werden, indem sie als "*Firewall*" bestimmte Anfragen nicht weiterleiten.
Router	Gerät zur Verbindung einzelner Netzwerkabschnitte und zur Weiterleitung von Datenpaketen über andere Router auf möglichst optimalen Strecken.
RTVG	Radio- und Fernsehgesetz, SR 784.40
Rz.	Randziffer
Server	Computer eines Netzwerks, der seine Daten den am Netzwerk teilnehmenden Computern zur Verfügung stellt.
SJZ	Schweizerische Juristen-Zeitung
SMS	*Short Message Service*: Kurzmitteilung über Mobiltelefon
SR	Systematische Sammlung des Bundesrechts
Sten.Bull.	Stenographisches Bulletin
StGB	Schweizerisches Strafgesetzbuch
StPO	Strafprozessordnung
SVG	Strassenverkehrsgesetz (SR 741.01)
TCP	*Transmission Control Protocol:* Übertragungsregeln unterhalb der Anwendungsebene für den gesicherten Datentransfer im Internet
TDG	Teledienstegesetz (Deutschland)
URG	Urheberrechtsgesetz, SR 231.1
URL	*Universal Resource Locator*: Einheitliche *Quellenadressierung* im Internet mit Angabe des zu verwendenden Zugriffsprotokolls: z.B. http://www.ibm.com (Zugriff mit http) oder ftp://ftp.linksys.com (Zugriff mit ftp).
UVEK	Eidg. Departement für Umwelt, Verkehr, Energie und Kommunikation
UWG	Bundesgesetz über den unlauteren Wettbewerb, SR 241
VE	Vorentwurf
VPB	Verwaltungspraxis des Bundes
WAP	*Wireless Access Protocol*: Eine Teilmenge von HTTP (siehe dort) zur Verwendung zwischen dafür eingerichteten Mobiltelefonen und speziellen Webservern, die Webinhalte für die kleinen Bildschirme der Mobiltelefone besonders aufbereiten.
Web	Netz, Kurzform für World Wide Web (s. dort)
World Wide Web	Weltweites Netz, Internet
WWW	World Wide Web
ZGB	Zivilgesetzbuch, SR 210
ZSR	Zeitschrift für Schweizerisches Recht
ZStrR	Schweizerische Zeitschrift für Strafrecht
ZStW	Zeitschrift für die gesamte Strafrechtswissenschaft

Bibliographie

Dieses Verzeichnis enthält nur die bibliographischen Angaben bzw. Fundstellen der im vorliegenden Bericht mehrfach zitierten Quellen, die zur Vereinfachung in den Fussnoten nur mit der Kurzbezeichnung (z.B. HÄFELIN/HALLER) und dem zusätzlichen Hinweis „Bibl." (Bibliographie) genannt werden.

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

NIGGLI, NATIONALES STRAFRECHT	Marcel Alexander Niggli, Nationales Strafrecht vs. globales Internet, in: Weber/Hilty/Auf der Maur (Hrsg.),Geschäftsplattform Internet II, Zürich 2001, S. 144 ff.
NIGGLI, RASSENDISKRIMINIERUNG	Marcel Alexander Niggli, Rassendiskriminierung, Kommentar, Zürch 1996
NIGGLI/SCHWARZENEGGER	Marcel Alexander Niggli/Christian Schwarzenegger, Strafbare Handlungen im Internet, SJZ 98 (2002), S. 61 ff.
PFENNINGER	Hanspeter Pfenninger, Rechtliche Aspekte des informellen Verwaltungshandelns, Diss. Freiburg 1996.
POPP	Peter Popp, in: Niggli/Wiprächtiger, Basler Kommentar, zu Art. 7 StGB, Basel 2003
REHBERG/DONATSCH	Jörg Rehberg/Andreas Donatsch, Strafrecht, Verbrechenslehre, 7. Aufl., Zürich 2001
RICHTLINIE	E-Commerce-Richtlinie der EU Richtlinie 2000/31/EG des Europäischen Parlamentes und des Rates vom 8. Juni 2000 über bestimmte Aspekte der Dienste der Informationsgesellschaft, insbesondere des elektronischen Geschäftsverkehrs, im Binnenmarkt („Richtlinie über den elektronischen Geschäftsverkehr“). ABl. Nr L. 178 vom 17.7.2000. S. 1-16 Link: http://europa.eu.int/eur-lex/pri/de/oj/dat/2000/l_178/l_17820000717de00010016.pdf
RIKLIN	Franz Riklin, Strafrecht, Allgemeiner Teil, 2. Aufl., Zürich 2002
RIKLIN/STRATENWERTH	Franz Riklin/Günter Stratenwerth, Medienstrafrecht/Kaskadenhaftung, in: Niggli/Riklin/Stratenwerth (Hrsg.), Die strafrechtliche Verantwortlichkeit von Internet Providern, medialex Sonderausgabe 2000, S. 13 ff.
SATZGER	Helmut Satzger Strafrechtliche Verantwortlichkeit von Zugangsvermittlern, Eine Untersuchung der Verantwortlichkeit für rechtswidrige Inhalte im Internet vor dem Hintergrund der neuen E-Commerce-Richtlinie der EG, Computer und Recht, 2/2001, S. 109 ff.
SCHMID	Niklaus Schmid, in Schmid (Hrsg.), Einziehung, Organisiertes Verbrechen, Geldwäscherei, Kommentar, Bd. 1, Zürich 1998
SCHULTZ, PRESSEDELIKT	Hans Schultz, Die unerlaubte Veröffentlichung - ein Pressedelikt, ZStrR 108 (1991) S. 273 ff.
SCHWARZENEGGER, ABSTRAKTE GEFAHR	Christian Schwarzenegger, Abstrakte Gefahr als Erfolg im Strafanwendungsrecht - Ein Leading case grenzüberschreitenden Internetdelikten, sic! 2001. S. 240 ff.

SCHWARZENEGGER, CRIMES	Christian Schwarzenegger Computer Crimes in Cyberspace, A comparative analysis of criminal law in Germany, Switzerland and Northern Europe Jusletter 14. Oktober 2002 www.weblaw.ch/jusletter/jsp?ArticleNr=1957
SCHWARZENEGGER, E-COMMERCE	Christian Schwarzenegger, E-Commerce - Die strafrechtliche Dimension, in: Arter/Jörg (Hrsg.), Internet-Recht und Electronic Commerce Law, Lachen und St. Gallen 2001
SCHWARZENEGGER, GELTUNGSBEREICH	Christian Schwarzenegger, Der räumliche Geltungsbereich des Strafrechts im Internet, ZStrR 118 (2000), S. 109 ff.
SEMKEN	Hartmut Semken (Un-)Möglichkeiten der Inhaltskontrolle mit technischen Mitteln im Internet, in: Cassani/Maag/Niggli (Hrsg.), Medien, Kriminalität und Justiz, Schweizerische Arbeitsgruppe für Kriminologie, Bd. 19. Chur/Zürich 2001, S. 249 ff.
TRECHSEL	Stefan Trechsel, Schweizerisches Strafgesetzbuch, Kurzkommentar, 2. Aufl., Zürich 1997
TRECHSEL/NOLL	Stefan Trechsel/Peter Noll Schweizerisches Strafrecht, Allgemeiner Teil I, Allgemeine Voraussetzungen der Strafbarkeit, 5. Aufl. Zürich 1998
TSCHANNEN/ZIMMERLI/KIENER	Pierre Tschannen/Ulrich Zimmerli/Regina Kiener, Allgemeines Verwaltungsrecht, Bern 2000
WEBER	Rolf H. Weber E-Commerce und Recht, Rechtliche Rahmenbedingungen elektronischer Geschäftsformen, Zürich 2001
WIDMER/BÄHLER	Ursula Widmer/Konrad Bähler, Rechtsfragen beim Electronic Commerce, Sichere Geschäftstransaktionen im Internet, 2. Aufl. Zürich 2000
ZELLER	Franz Zeller, in: Niggli/Wiprächtiger, Basler Kommentar, zu Art. 27 StGB, Basel 2003

Unklarheiten hinsichtlich der strafrechtlichen Verantwortlichkeit von Internet-Zugangsvermittlern und entsprechende parlamentarische Vorstösse führten zur Einsetzung der Expertenkommission „Netzwerkkriminalität“.
Dieser Bericht soll vorab Klärungen ermöglichen sowie Empfehlungen und Vorschläge an die Politik formulieren.

1. Einleitung

1.1 Ausgangslage

1.11 Pilotversuch mit „Internet Cops“

Seit Anfang 1998 führte das Bundesamt für Polizei (BAP) einen Pilotversuch mit Internet-Monitoring durch: Zwei Beamte fungierten als sog. „Internet Cops“ und führten gewissermassen „Streifenfahrten“ durch die Angebote auf dem Netz durch. In erster Linie nahmen sie aber Meldungen aus dem Publikum über illegale Inhalte entgegen und bearbeiteten sie weiter. Dabei wurde festgestellt, dass verschiedene Internet-Seiten Inhalte aufwiesen, die möglicherweise gegen Art. 261bis des Strafgesetzbuches (StGB), Rassendiskriminierung, verstossen.

1.12 Sperrempfehlung an die Zugangsvermittler

Im Juli des gleichen Jahres wandte sich die Bundespolizei in einem Rundschreiben an Internet-Service-Provider (ISP) in der Schweiz und bat diese, die Sperrung der inkriminierten Seiten zu prüfen. Sie wies die ISP unter anderem darauf hin, die Vermittlung des Zuganges auf solche Seiten könnte als Gehilfenschaft zur Haupttat qualifiziert werden. Das Rundschreiben löste bei den Providern starke Reaktionen aus. Sie zogen namentlich die technische Machbarkeit von Internet-Sperren und deren rechtliche Abstützung in Zweifel. In der Folge wurde eine gemeinsame Kontaktgruppe aus Vertretern der vom Thema berührten Dienststellen der Bundesverwaltung sowie der Providerbranche gebildet. Die Gruppe sollte vorab die sich stellenden technischen und rechtlichen Fragen vertieft klären.

1.13 Ein Gutachten...

Wegen der kontroversen Reaktionen der Kontaktgruppe auf ein erstes Grundlagenpapier zur Frage der Internet-Sperren ersuchte die Bundespolizei das Bundesamt für Justiz (BJ) um gutachterliche Prüfung der Frage der strafrechtlichen Verantwortlichkeit von Internet Service Providern für illegale Inhalte.

Das BJ bejahte in seinem Gutachten vom 24. Dezember 1999 [1] grundsätzlich die subsidiäre Verantwortlichkeit auch eines reinen Zugangsvermittlers im Sinne des Medienstrafrechts, vorausgesetzt dieser sei von einer Strafverfolgungsbehörde klar auf den illegalen Inhalt aufmerksam gemacht worden. Wo das Medienstrafrecht keine Anwendung finde, könnten die Provider als Gehilfen zur Haupttat bestraft werden.

Auf der Grundlage der Ausführungen im BJ-Gutachten präzisierte die Bundespolizei ihre Haltung in einem Positionspapier, das sie einer bereiteren Öffentlichkeit zugänglich machte [2].

1.14 ... und ein zweites Gutachten

Der als Vertreter der Providerbranche wirkende Verband Inside Telecom (VIT) lehnte die Schlussfolgerungen des BJ-Gutachtens als unrichtig ab und beauftragte die Professoren Marcel A. Niggli, Franz Riklin und Günter Stratenwerth die Frage der strafrechtlichen Verantwortlichkeit von Zugangsvermittlern ihrerseits zu prüfen.

Am 2. Oktober 2000 erstatteten die drei beauftragten Professoren ihr Gutachten [3]. Darin kamen sie in der zentralen Frage der strafrechtlichen Stellung reiner Zugangsvermittler zu im wesentlichen gegenteiligen Schlussfolgerungen als das BJ. Die Gutachter betonten stark den Aspekt der ihres Erachtens unklaren Rechtslage und postulierten gestützt darauf einen gesetzgeberischen Handlungsbedarf.

1.2 Politisches Umfeld

1.21 Die Motion Pfisterer

Am 14. Dezember 2000 reichte Ständerat Thomas Pfisterer, gemeinsam mit 27 Mitunterzeichnenden, folgende Motion ein:

> 1. Der Bundesrat wird eingeladen, zum Schutz des Internet im Interesse von Bevölkerung und Wirtschaft in erster Priorität rasch eine rechtssichere, praktikable, international möglichst harmonisierte Regelung im Strafrecht, eventuell in einzelnen weiteren Bestimmungen zu beantragen.
>
> 2. Er soll nötigenfalls unerlässliche weitere Rechtsänderungen beantragen (spätere Priorität).

In der Begründung unterstrich der Motionär die technischen und rechtlichen Besonderheiten von Computer-Netzwerken wie des Internet und leitete daraus einen dringenden Gesetzgebungsbedarf ab. Für die zu schaffende Rahmenordnung empfehle sich eine Anlehnung an die E-Commerce-Richtlinie der Europäischen

---

[1] Abgedruckt in VPB 64.75.

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

[3] Abgedruckt in medialex, Sondernummer 1/2000.

Union. Der Motionär entwarf einen möglichen Gesetzestext, der v.a. Ergänzungen der Artikel 27 und 340 StGB vorsieht (vgl. Wortlaut im Anhang [A])

Der *Bundesrat* betonte in seiner Stellungnahme zur Motion, auch ohne einschlägige Bestimmungen bewege sich das Internet nicht in einem gesetzlichen Niemandsland. Zur Stützung dieser Auffassung verwies er namentlich auf das Gutachten des Bundesamtes für Justiz. Im Übrigen bejahte er den schon früher bekundeten Willen des Bundesrates zu einer international abgestimmten Gesetzgebung auf diesem Gebiet und beurteilte den Regelungsvorschlag des Motionärs als prinzipiell tauglichen Ansatz. Er legte zudem Gewicht auf die Notwendigkeit einer in sich kohärenten Kriminalpolitik und der entsprechenden Gesetzgebung. Auch wenn er sich durch die Begründung der Motion nicht binden lassen wollte, erklärte sich der Bundesrat bereit, sie *entgegenzunehmen*.

Der *Ständerat* nahm die Motion am 6. März 2001 an [4]; der *Nationalrat* tat es ihm am 20. September 2001 gleich [5].

1.22 Weitere parlamentarische Vorstösse

Am 26 . September 2002 reichte Nationalrätin *Regine Aeppli* eine als allgemeine Anregung formulierte parlamentarische Initiative (02.452) [6] ein. Diese hat folgenden *Wortlaut*:

> Zur Effizienzsteigerung und Koordination der Strafverfolgung im Bereich der Netzwerkkriminalität, insbesondere der Kinderpornographie, sei eine Bundeskompetenz zu schaffen, wie sie in Art. 340bis StGB bei organisiertem Verbrechen und Wirtschaftskriminalität vorgesehen ist.

Als Begründung erinnert die Initiantin an das Ende 1999 vom Bund wieder eingestellte Internet Monitoring und die sich als schwierig erweisende Zusammenarbeit mit den Kantonen. Sie betont den Anstieg der Fälle von Internetkriminalität, v.a. im Bereich der Kinderpornographie und der Pädophilie, und erachtet daher das „jahrelange Kompetenzgerangel“ als unzumutbar. Auch die von der Schweiz unterzeichnete Konvention des Europarates über die Cyberkriminalität verlange die Einrichtung einer zentralen Anlaufstelle.

1.3 Die Expertenkommission

1.31 Einsetzung und Auftrag

Vor dem Hintergrund der Motion Pfisterer (oben Ziff. 1.21) und generell um die Fragen rund um den Missbrauch des Internet zu klären, setzte das EJPD am 22.

---

[4] AB 2001 S 27 f.

[5] AB 2001 N 1087 ff.

[6] Vgl. die frühere Motion Aeppli Wartmann (01.3196) vom 23. März 2001 (Internetkriminalität, Wirksamere Bekämpfung mit effizientem Verfahren); sie zielt in die gleiche Richtung wie die parlamentarische Initiative von 2002.

November 2001 eine Expertenkommission „Netzwerkkriminalität“ ein und erteilte ihr folgenden *Auftrag*:

> Die Expertenkommission "Netzwerkkriminalität" prüft, mit welchen rechtlichen, organisatorischen und technischen Massnahmen Rechtsverletzungen, die mit dem Medium Internet begangen werden, verhindert und geahndet werden können. Dabei prüft sie insbesondere die Frage, wie die strafrechtliche Verantwortlichkeit im Internet zu regeln sei. Wenn sich dies als zweckmässig erweist, schlägt sie zudem Regeln betreffend die zivilrechtliche Haftung und den Schutz des geistigen Eigentums vor. Ihre Arbeiten sollen in einen vernehmlassungsreifen Gesetzesentwurf münden.

Das EJPD verpflichtete die Kommission, ihren Bericht und Vorentwurf bis Ende 2003 abzuliefern.

1.32 Zusammensetzung

Die Expertenkommission stand unter dem *Vorsitz* von Dr. Peter Müller, Vizedirektor des Bundesamtes für Justiz [7]. Im Übrigen setzte sich die Kommission wie folgt zusammen:

- Prof. Dr. Felix Bommer, Assistenzprofessor für Strafrecht an der Universität Luzern
- Fürsprecher Hans-Ulrich Bühler, Bundesamt für Polizei
- Dr. Lukas Bühler, Institut für Geistiges Eigentum
- Maître Maurice Harari, Rechtsanwalt, Genf [8]
- Prof. Dr. Matthias Kaiserswerth, Zürich
- Prof. Dr. Laurent Moreillon, Assistenzprofessor für Strafrecht an der Universität Lausanne
- Prof. Dr. Marcel Alexander Niggli, Ordinarius für Strafrecht an der Universität Freiburg
- Prof. Dr. Isabelle Romy, Rechtsanwältin, Zürich; Professeure associée an der Universität Freiburg
- Prof. Dr. Christian Schwarzenegger, Assistenzprofessor für Strafrecht an der Universität Zürich; *Vizepräsident der Expertenkommission*
- Prof. Dr. Bernhard Waldmann, Assistenzprofessor für öffentliches Recht an der Universität Freiburg
- Dr. Ursula Widmer Rechtsanwältin und Geschäftsführerin des Verbandes Inside Telecom (VIT), Bern
- Dr. Franz Zeller, Bundesamt für Kommunikation

Das *Sekretariat* der Kommission führten Dr. Dorrit Schleiminger (bis September 2002), Dr. Peter Ullrich (ab Oktober 2002, Koordination des Berichts), Dr. Grace

[7] Seit 1. Februar 2003 Generalsekretär des Eidg. Departements für auswärtige Angelegenheiten (EDA).
[8] Bis Ende Oktober 2002.

Schild Trappe (ab Februar 2003), Dr. Stéphane Blanc und Patrick Gruber (beide Protokollführung), alle Mitarbeiter des Bundesamtes für Justiz.

1.33 Arbeitsweise der Kommission

Die Kommission versammelte sich zwischen Februar 2002 und März 2003 zu insgesamt zehn halb- und ganztägigen Sitzungen.

Sie zog zu einigen ihrer Sitzungen Herrn Philipp Kronig, lic.iur., MPA, Leiter der nationalen Koordinationsstelle für die Bekämpfung der Internet-Kriminalität (KOBIK) im Bundesamt für Polizei, als aussenstehenden Sachverständigen bei.

Mehrere Kapitel des Schlussberichts wurden wesentlich auf der Grundlage von Fachbeiträgen der Mitglieder der Expertenkommission erstellt:

- **Kapitel 2** (Kommunikation in Netzwerken): Prof. Schwarzenegger
- **Kapitel 3** (Technische Grundlagen): Prof. Kaiserswerth
- **Kapitel 5** (Verfassungsrechtliche Rahmenbedingungen): Prof. Waldmann
- **Kapitel 6** (Netzwerkkriminalität nach geltendem Strafrecht): Proff. Bommer, Niggli, Schwarzenegger
- **Kapitel 7** (Möglichkeit verwaltungsrechtlicher Massnahmen): Prof. Waldmann
- **Kapitel 8** (Zivilrechtliche Haftung): Dr. L. Bühler
- **Kapitel 9** (Gesetzesvorschlag): Proff. Bommer, Moreillon, Niggli, Schwarzenegger
- **Kapitel 10** (Parallele Gesetzgebung/weitere gesetzgeberische Aufgaben): Proff. Bommer, Niggli, Schwarzenegger, H.U. Bühler, Dr. Widmer

1.4 Die hauptsächlichen Fragen

Sehr *allgemein formuliert,* lautet die von der Expertenkommission zu beantwortende Frage:

> Wie können und sollen illegale Inhalte auf dem Internet verhindert werden, und wer ist für diese auf welche Weise verantwortlich?

Diese generelle Frage lässt sich in mehrere *Teilfragen* gliedern:

- Wie lassen sich die in Kommunikationsnetzen zirkulierenden Inhalte *technisch kontrollieren* und allenfalls *sperren* oder *beseitigen*? (Vgl. *Kapitel 3* des Berichts).
- Wer kann unter welchen Voraussetzungen für Rechtsverletzungen in Kommunikationsnetzen in der Schweiz *strafrechtlich* zur Verantwortung gezogen werden? (Vgl. *Kapitel 6, Ziff. 6.1 - 6.3; Kapitel 9*).
- Wie weit lassen sich *im Ausland verübte Rechtsverletzungen* in Kommunikationsnetzen in der Schweiz strafrechtlich verfolgen und ahnden? (Vgl. *Kapitel 6, Ziff. 6.4; Kapitel 9*).

- Sollen *die Kantone oder der Bund* für die Strafverfolgung bei Rechtsverletzungen in Kommunikationsnetzen zuständig sein? (Vgl. *Kapitel 6, Ziff. 6.5; Kapitel 9, Ziff. 9.4*).
- Bietet das *Verwaltungsrecht* Instrumente an, um Rechtsverletzungen in Kommunikationsnetzen zu verhindern? (Vgl. *Kapitel 7*).
- Wer haftet auf welche Weise *zivilrechtlich* für Schäden aus Rechtsverletzungen in Kommunikationsnetzen und für Schäden im Zusammenhang mit der Sperrung oder Beseitigung von illegalen Netzinhalten? (Vgl. *Kapitel 8*).

Die Zahl der Kommunikationsdienste und ihrer Nutzer hat in den letzten Jahren stark zugenommen. Das blieb nicht ohne Einfluss auf die Gesellschaft. Entsprechend hat sich die einschlägige Kriminalität entwickelt.

2. Kommunikation in Netzwerken: Fakten und Zahlen

2.1 Evolution der Informationstechnologien und sozialer Wandel

Die rasante Entwicklung der Informations- und Netzwerktechnologie in den letzten 20 Jahren hat wie kaum ein anderer Faktor die Lebens- und Kommunikations-gewohnheiten der Menschen beeinflusst und verändert.

2.11 Neue Vielfalt der Kommunikationsdienste

Wer sich zu einer Verabredung verspätete, musste früher eine Telefonzelle suchen und über entsprechendes Kleingeld verfügen, um dies dem Wartenden mitzuteilen. War der andere unterwegs, bestand keine Möglichkeit, ihn zu erreichen. Heute genügt ein Anruf oder ein *SMS* (Short Message Service) auf das *Mobiltelefon* (vgl. untenstehendes Kästchen).

Verbreitung von SMS

Im Jahr 2001 verzeichneten die Mobilfunk-Anbieter bei den SMS-Mitteilungen Wachstumsraten bis zu 50%. Bei Orange kamen im Jahr 2001 auf jeden Kunden 1,8 SMS täglich. Eine ähnliche Entwicklung weist auch die Swisscom aus, die ca. 7 Mio. Kurzmitteilungen pro Tag registrierte. Damit entfallen auf jeden Swisscom-Kunden 2 SMS täglich. Bei Sunrise haben die Zahlen des dritten Quartals 2001 im Vergleich zur Vorjahresperiode um 66,7% zugenommen. Das Unternehmen schätzt, dass auf jeden Kunden etwa 1,8 bis 2 SMS pro Tag entfallen[9].

Wer einen Leserbrief zur Zeitungsredaktion senden wollte, musste dies per Briefpost und mindestens einen Tag vor Redaktionsschluss tun. Heute genügt eine *E-Mail* (Electronic Mail, elektronische Nachricht), eventuell mit angehängter Textdatei, die in der Regel binnen Sekunden bei der Redaktion eintrifft.

Wer auf Arbeits- und Wohnungssuche war, musste auf die Ausgaben der Tageszeitungen mit entsprechenden Anzeigen warten, während man heute jederzeit entsprechende *Datenbanken im Internet* abrufen und den ersten Kontakt per E-Mail herstellen kann.

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

Das aktuelle Tagesgeschehen lässt sich auf den *Websites der verschiedenen Medienunternehmen* beinahe live mitverfolgen.

Anzahl aller aktiven Websites [10] **(weltweit)**

August 1995:	18'957
Dezember 1996:	603'367
Dezember 1997:	1'681'868
Dezember 1998:	3'689'227
Dezember 1999:	9'560'866
Dezember 2000:	25'675'581
Dezember 2001:	36'276'252
Dezember 2002	35'543'105

Wer Lust darauf hatte, sich mit einer Gruppe von Menschen auszutauschen, musste sich früher in Versammlungen, Veranstaltungen, Bars u.ä. begeben. Heute besteht die Alternative des *„Chattens" im Internet*, das den Beteiligten ein simultanes, auch anonymes Austauschen von Kurznachrichten ermöglicht. Für Internetnutzer mit schnellem Netzzugang besteht die Möglichkeit einer *Voice-Mail* oder einer *Videokonferenzschaltung*.

2.12 Grenzenlose Nutzung des Internet

Mit den oben in 2.11 beschriebenen Diensten des Internet haben sich auch die geographischen Grenzen der Kommunikation verflüchtigt. Denn die Nutzung bzw. der Abruf von Informationen ist weltweit von jedem Netzanschluss aus möglich. Immer mehr Personen verfügen privat oder am Arbeitsplatz über eine entsprechende Netzanbindung. Die Schweiz zählt im europäischen Vergleich zu den Ländern mit der höchsten Penetrationsrate (siehe untenstehendeTabellen).

Anzahl Personen mit Internet-Zugang von zu Hause (4. Quartal 2001)[11]

	Anzahl Personen (in Mio.)	Zuwachs im Vergleich zum 3. Quartal 2001 (in %)	Anteil der weltweiten Internetpopulation nach Regionen (in %)
USA/Kanada	191,7	6,1	39
Europa/Israel/Südafrika*	134,7	6,3	27
Ferner Osten, Australien, Neuseeland**	110,1	5,8	22
Lateinamerika***	20,7	0,7	4
Restliche Welt	41,0	5,1	8
Total	498,2		100

* Belgien, Dänemark, Deutschland, Finnland, Frankreich, Grossbritannien, Irland, Italien, Luxemburg, Niederlanden, Norwegen, Österreich, Schweden, Schweiz, Spanien; Israel; Südafrika
** Australien, Hong Kong, Indien, Japan, Neuseeland, Singapore, Südkorea, Taiwan
*** Argentinien, Brasilien, Mexiko

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

[11] ACNIELSEN ERATINGS.COM, abrufbar unter: www.eratings.com/news/2002/20020306.htm (Stand: 7.10.2002).

Haushalte mit Internetzugang und Anteil der Computer mit Internetzugang in Europa (4. Quartal 2001)[12]

	Haushalte mit Internetzugang (in %)	Anteil der Computer in privaten Haushalten mit Internetzugang (in %)
Schweden	57	87
Niederlanden	52	82
Dänemark	51	82
Norwegen	47	78
Schweiz	**43**	**78**
Finnland	42	81
Österreich	38	70
Grossbritannien	38	78
Deutschland	35	72
Italien	34	80
Belgien/Luxemburg	32	68
Frankreich	20	53
Spanien	18	48

2.13 Internet-Nutzung nimmt auch in der Schweiz zu

Seit 1997 ist die Internetnutzung in der Schweiz stark angestiegen: Damals nutzten erst rund 7 Prozent der Bevölkerung das Internet regelmässig, d.h. mehrmals pro Woche. Anfang 2002 gehörten bereits 42 Prozent zu diesem engen Nutzerkreis (ENK). Zum weiteren Nutzerkreis (WNK), also zu den Personen, welche das Internet ab und zu nutzen, zählten 1997 15 Prozent. Unterdessen hat sich dieser weitere Nutzerkreis auf 57 Prozent erhöht [13].

2.14 Internet-Nutzung hängt von Geschlecht, Bildung und Alter ab

Anfang 2002 war die Nutzungsquote bei den *Männern* deutlich höher als bei den Frauen: 52% gegenüber knapp 33%. Allerdings ist der Anteil der *Frauen* bei den Internetbenutzenden tendenziell im Steigen begriffen. 1997 gehörten gut 3% der Frauen zum ENK, 2000 waren es über 22%, 2002 die erwähnten 33%. Während die Quote der Internetnutzung bei den Frauen zwischen 1997 und dem Jahr 2001 um mehr als das Zehnfache zunahm, betrug der Zuwachs bei den Männern lediglich das Fünffache [14].

Der *Bildungsstand* hat einen bedeutenden Einfluss auf die Internetnutzung: Je höher die Bildung, desto höher die Internetnutzung. So nutzten im Jahr 2002 22 Prozent der Personen, die nur die obligatorische Schule besucht haben, das Internet regelmässig. Bei den Personen mit Sekundarschulabschluss beträgt der entsprechende Anteil 35 Prozent, bei jenen mit einer höheren Berufsausbildung gut 58 Prozent. Bei denjenigen Personen, die über einen Hochschulabschluss verfügen, sind es rund 71 Prozent [15].

---

[12] ACNielsen eRatings.com, abrufbar unter: www.eratings.com/news/2002/20020306.htm (Stand: 7.10.2002).

[13] http://www.statistik.admin.ch/stat_ch/ber20/indic-soc-info/ind30106d_1_synth.htm

[14] http://www.statistik.admin.ch/stat_ch/ber20/indic-soc-info/ind30106d_4_synth.htm

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

Ein wichtiges Merkmal der Internutzung ist das *Alter*. Menschen über 50 Jahre weisen eine deutlich geringere Internetnutzung auf als jüngere Menschen. Die intensivste Internetnutzung hatte Anfang 2002 die Altersgruppe der 14-19-Jährigen sowie die der 20-29-Jährigen: Von ihnen gehörten 56 Prozent bzw. 60 Prozent zum engeren Nutzerkreis. Bei den über 50-Jährigen zählten lediglich 20 Prozent zu dieser Nutzungsgruppe [16].

2.15 Das Internet: ein alltägliches Medium

Bis vor drei Jahren war die Internetnutzung am Arbeitsplatz höher als zu Hause. Unterdessen wird das Internet häufiger *zu Hause* als am *Arbeitsplatz* genutzt. 2002 haben rund 42 Prozent das Internet zu Hause eingesetzt, am Arbeitsplatz waren es gut 31 Prozent. Seine zunehmende Verbreitung im privaten Bereich zeigt, dass das Internet zu einem alltäglichen Medium geworden ist [17].

Auch differenziert nach *Sprachregionen* zeigen sich in der Schweiz Unterschiede bei der Internetnutzung: In der *Deutschschweiz* ist sie höher (43%) als in der *französischen und italienischen Schweiz* (41 resp. 34%) [18].

Das Internet wurde 2002 am häufigsten für *kommunikative Zwecke* verwendet: Über 91 Prozent der Nutzerinnen und Nutzer nennen das E-Mail. Am zweithäufigsten, 71 Prozent, ist das Benutzen von *Suchmaschinen*. An dritter Stelle wird das Internet für *Informationszwecke* verwendet (53%), für das Abrufen von Zeitungs- und Zeitschriftenartikeln. Demgegenüber machten 2002 lediglich 14% der Internetbenutzenden vom *Online-Shopping-Angebot* Gebrauch [19].

2.2 Netzwerkkriminalität

2.21 Herkömmliche und neue Straftaten

Die Schattenseiten der in Ziff. 2.1 dargestellten Entwicklung zeigen sich immer deutlicher: Auf der einen Seite erleichtern die neuen Kommunikationsmittel und -netze die Begehung „traditioneller“ [20] Straftaten; auf der anderen Seite bieten Computertechnologie und Netzwerke Angriffsflächen für neue Kriminalitätsformen [21] (siehe Beispiele unten).

---

[16] http://www.statistik.admin.ch/stat_ch/ber20/indic-soc-info/ind30106d_5_synth.htm

[17] http://www.statistik.admin.ch/stat_ch/ber20/indic-soc-info/ind30106d_311_synth.htm

[18] http://www.statistik.admin.ch/stat_ch/ber20/indic-soc-info/ind30106d_6_synth.htm

[19] http://www.statistik.admin.ch/stat_ch/ber20/indic-soc-info/ind30106d_319_synth.htm. Vgl. zu alldem auch MAJA HUBER/FLORENT COSANDEY /VOLKER TÄUBE, Indikatoren zur Informationsgesellschaft, in: Informationsgesellschaft Schweiz, Standortbestimmung und Perspektiven, Neuchâtel 2002, 22, mit zahlreichen weiterführenden Informationen über die Verbreitung von Computern, Modems, Handys sowie zur Nutzung durch Private, Unternehmen und die öffentliche Hand.

[20] D.h. von Straftaten, die schon bisher auftraten, bei denen aber die Informationstechnologie und die Kommunikationsnetze als neue, äusserst effektive und bequeme Tatmittel zum Einsatz kommen.

[21] Ein Überblick über die Erscheinungsformen der Internetkriminalität findet sich bei WIDMER/BÄHLER (Bibl.), S. 292 ff.; SCHWARZENEGGER, E-COMMERCE (Bibl.), S. 333 ff.; WEBER, (Bibl.), S.538 ff.

Beispiele für „traditionelle“ Straftaten

- Gewaltdarstellungen (Art. 135 StGB),
- unwahre Angaben über kaufmännische Gewerbe (Art. 152 StGB),
- Kursmanipulation (Art. 161bis StGB),
- Ehrverletzungen (Art. 173 ff. StGB),
- Verletzung des Geheim- oder Privatbereichs durch Aufnahmegeräte (Art. 179^{quater} StGB),
- Missbrauch einer Fernmeldeanlage (Art. 179^{septies} StGB),
- Pornographie (Art. 197 StGB),
- sexuelle Belästigung (Art. 198 StGB),
- Anleiten zur Herstellung von Sprengstoffen und giftigen Gasen (Art. 226 StGB),
- öffentliche Aufforderung zu Verbrechen oder zu Gewalttätigkeit (Art. 259 StGB),
- Störung der Glaubens- und Kultusfreiheit (Art. 261 StGB),
- Rassendiskriminierung (Art. 261bis StGB),
- Veröffentlichung amtlicher geheimer Verhandlungen (Art. 293 StGB),
- Verbreitung oder Kopieren eines urheberrechtlich geschützten Werkes (Art. 67 und 69 URG),
- unlautere Werbe- und Verkaufsmethoden und anderes widerrechtliches Verhalten (Art. 3 UWG i.V.m. Art. 23 UWG).

Beispiele für neue Kriminalitätsformen

- Unbefugte Datenbeschaffung (Art. 143 StGB),
- Unbefugtes Eindringen in ein Datenverarbeitungssystem (Art. 143bis StGB),
- Datenbeschädigung inklusive Herstellung und Verbreitung von Computerviren (Art. 144bis StGB),
- Betrügerischer Missbrauch einer Datenverarbeitungsanlage (Art. 147 StGB),
- Erschleichen einer Computerleistung („Zeitdiebstahl“, Art. 150 StGB),
- Nötigung durch unverlangte oder massenhaft versandte E-Mails oder „Denial of Service“-Attacken (Art. 181 StGB).
- Bei schweren Beeinträchtigungen der Kommunikationsnetze: Störung von Betrieben, die der Allgemeinheit dienen (Art. 239 Ziff. 1 Abs. 1 StGB).

2.22 Generelle Zunahme der Netzwerkkriminalität

Die wenigen empirischen Untersuchungen zum Thema deuten darauf hin, dass die Netzwerkkriminalität seit 1990 stark ansteigt [22]. Gemäss einer aktuellen Statistik der *National Consumers League* (USA) melden die Konsumenten jährlich immer mehr Betrugsfälle im Internet. Nach verschiedenen Geschäftsbereichen differenziert, ist das Opferrisiko bei Online-Auktionen am grössten (87 % der im ersten Halbjahr 2002 eingegangenen Meldungen). Weitere 6 % der vermeintlichen Schädigungen durch Betrug gehören in die Kategorie der generellen Warenverkäufe. Der durchschnittliche Vermögensschaden betrug 484 US-Dollar [23].

Die *Europäische Kommission* legte im Jahr 2001 einen Bericht vor, der bezüglich des Jahres 2000 die Erlöse aus Zahlungskartenbetrug auf 600 Mio. Euro schätzt, was

[22] Vgl. BUNDESAMT FÜR POLIZEI, „Cyberkriminalität“, Die dunkle Seite der Informationsrevolution, Bern 2001, abrufbar unter: www.isps.ch/site/fichiers/171.pdf (Stand: 7.10.2002); SCHWARZENEGGER, CRIMES (Bibl.), N 3 ff. und 42 f..

[23] NATIONAL CONSUMERS LEAGUE (ed.), 2002 Internet fraud statistics, abrufbar unter: www.fraud.org/02intstats.htm (Stand: 10.10.2002). Der Gesamtbetrag der gemeldeten Schäden betrug im Jahr 2000 noch $3’387’530, im ersten Halbjahr 2002 ist die Gesamtsumme schon auf $ 7’209'196 angestiegen. Diese statistischen Angaben sind allerdings nicht repräsentativ für die Gesamtheit aller Internet-Nutzer in den USA. Es ist davon auszugehen, dass nicht alle gemeldeten Fälle einem Betrug i.S.v. Art. 146 StGB entsprechen.

einer Zunahme von rund 50 % entspreche. Zahlungen über das Internet sind dabei überproportional vertreten [24].

Im Jahr 2001 nahm auch die Verbreitung von *Computerviren* sprunghaft zu. Diese bösartigen Codes, die häufig über angehängte Dateien („Attachments") von E-Mails, aber auch über infizierte Websites verbreitet werden, bergen ein erhebliches Schädigungspotential [25]. Gemäss Erhebungen der Hersteller von Anti-Viren-Programmen war im Jahr 2001 durchschnittlich jedes 370. E-Mail mit einem Virus infiziert, während die Werte im Jahr 2000 bei 1 Virus pro 700 E-Mails und im Jahr 1999 noch bei 1 Virus pro 1400 E-Mails lagen [26].

2.23 Zurückhaltende Strafverfolgung in der Schweiz

In der Schweiz werden nur wenige Fälle polizeilich registriert, und nur vereinzelt enden sie mit einer Verurteilung (siehe untenstehende Tabellen)[27]. Im übrigen betreffen die Verurteilungen wegen betrügerischen Missbrauchs einer Datenverarbeitungsanlage nur zu einem geringen Teil Netzwerkdelikte. In der Mehrzahl der Fälle handelt es sich um herkömmliche Missbräuche von Zahlungskarten.

Damit wird deutlich, dass die Strafverfolgung im Bereich der Computer- und Internetkriminalität noch stark im Rückstand ist. Dies vor allem gemessen an den Schäden und Gefahren, die beispielsweise mit dem Hacking oder der Verbreitung von Computerviren verbunden sind [28]. Ähnliche Defizite sind auch in den Bereichen der harten und weichen Pornographie, der Rassendiskriminierung und der Musik-, Software- und Filmpiraterie zu erkennen.

Polizeilich erfasste Computerdelikte (Zürich, 1996-2000)

Jahr	1996	1997	1998	1999	2000
Unbefugte Datenbeschaffung (Art. 143), Unbefugtes Eindringen in ein Datenverarbeitungssystem (Art. 143bis), Datenbeschädigung (Art. 144bis Ziff. 1), Herstellung usw. von Programmen zur Datenbeschädigung (Art. 144bis Ziff. 2)	8	38	11	19	40

[24] Kommission der Europäischen Union, Mitteilung vom 9.2.2001 zur Vorbeugung von Betrug und Fälschung im Zusammenhang mit bargeldlosen Zahlungsmitteln, KOM(2001) 11, abrufbar unter http://europa.eu.int/comm/internal_market/en/finances/payment/fraud/cardfraud.htm (Stand: 10.10.2002).

[25] Das sich im Mai 2000 weltweit verbreitende "I Love You" Virus soll nach Schätzungen der Swiss Re innert kürzester Zeit einen Schaden mehr als $ 1 Mia. verursacht haben, vgl. SWISS RE, National catastrophes and man-made disasters in 2000, sigma No. 2/2001, S. 7. Andere Quellen sprechen gar von einem wirtschaftlichen Schaden von $ 17 Mia.

[26] TAGES-ANZEIGER, Von Würmern und tanzenden CEOs, 24. Dezember 2001, 49: „Das Jahr des Wurms".

[27] Ähnlich ist die Situation in Deutschland, siehe SCHWARZENEGGER, CRIMES (Bibl.), N 3 ff.

[28] Vgl. auch die Befragungsresultate in KPMG (Hrsg.): 2001 global e.fr@ud.survey, o.O. 2001, abrufbar unter: www.kpmg.de/library/surveys/ (Stand: 9.10.2002)

Betrügerischer Missbrauch einer Datenverarbeitungsanlage (Art. 147)	786	1'162	1'612	1'673	2'100

Quelle: KRISTA 1996-2000 (Kriminalstatistik des Kantons Zürich)

Verurteilungen wegen Computerdelikten (Schweiz, 1995-2000)

Jahr	1995	1996	1997	1998	1999	2000
Unbefugte Datenbeschaffung (Art. 143)	1	2	2	2	4	3
Unbefugtes Eindringen in ein Datenverarbeitungssystem (Art. 143bis)	0	1	0	1	1	2
Datenbeschädigung (Art. 144bis Ziff. 1)	14	18	111	21	10	2
Herstellung usw. von Programmen zur Datenbeschädigung (Art. 144bis Ziff. 2)	1	0	2	2	1	3
Betrügerischer Missbrauch einer Datenverarbeitungsanlage (Art. 147)	52	223	372	393	416	422

Quelle: Bundesamt für Statistik, Strafurteilsstatistik 2002 (unveröffentlichte Auswertung).

2.24 Kriminalität ist technologieneutral

Ähnliche Kriminalitätsphänomene sind auch im Bereich der Mobiltelefonie festzustellen (z.B. sexuelle Belästigung, Ehrverletzung durch SMS, SMS-Flooding, u.a.) [29]. Mit dem grösstenteils vollzogenen Wandel von einem reinen Sprachkommunikationsmittel zu einem multifunktionalen Funkdatennetz, über welches dank neuer breitbandiger Datenübertragungskapazitäten immer mehr Dienste abgewickelt werden können (WAP-News, Mobile-Chat, Mobile-Games, Bilddatentransfer, SMS, E-Mail), potenzieren sich die Möglichkeit zur kriminellen Nutzung. Durch sog. Gateways - ein Gateway verbindet unterschiedliche Netze miteinander - sind einzelne Dienste des Mobilfunknetzes zudem mit dem Internet verbunden.

Obwohl in diesem Bericht die Probleme der Internetkriminalität im Vordergrund stehen, drängt es sich aufgrund der Konvergenz der elektronischen Kommunikationsnetze und -dienste auf, einen technologieneutralen Regelungsrahmen zu schaffen.

2.3 Die an der Netzwerk-Kommunikation Beteiligten

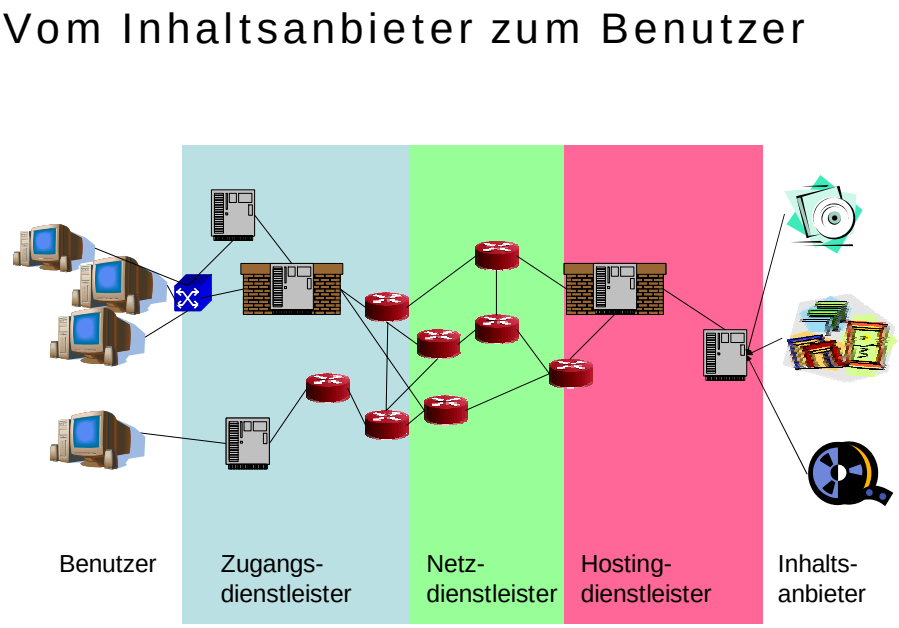
Das Bereitstellen, Bereithalten und Übermitteln von rechtswidrigen Inhalten oder rechtswidrig genutzten Informationen in Kommunikationsnetzen läuft über mehrere Stationen. Daher kommen als Täter oder Teilnehmer an der Tat immer mehrere Personen in Betracht.

Geht man beispielhaft vom World Wide Web (WWW) aus, das neben dem E-Mail-Dienst die meistgenutzte Art der Informationsübermittlung via Internet ist (oben 2.15), können mehrere Gruppen unterschieden werden:

[29] Siehe dazu die Beschwerden-Website www.handybetrug.ch (Stand: 9.10.2002)

2.31 Die Dienstleister

Die Dienstleister gliedern sich in vier verschiedene Gruppen (siehe untenstehende Grafik). Es gibt solche, die alle vier Leistungen anbieten (z.B. America Online, Bluewin), oder solche, die sich auf lediglich eine oder zwei Dienstleistungen spezialisiert haben.



2.311 Content-Provider

Die Content-Provider (Inhaltsanbieter) stellen eigene oder von Dritten übernommene Inhalte auf dem Internet zur Verfügung. Sie bedienen sich mindestens eines Access-Providers (unten 2.314) und stellen diese Inhalte auf einem eigenen Rechner oder aber demjenigen eines Hosting-Providers (unten Ziff. 2.312) zur Verfügung. Durch die vermehrte Verbreitung sogenannter *Peer-to-Peer*-Protokolle können auch normale Endbenutzer, die sonst nur als Konsumenten von Inhalten auftreten, eigene Inhalte anbieten. In diesen Fällen besorgt der Content-Provider selber das „Hosting“ seiner Daten.

2.312 Hosting-Provider

Die Hosting-Provider (in der Grafik: „Hostingdienstleister“) stellen ihren Kunden, den Content-Providern, einen Webserver zur Verfügung, auf dem diese eigene Webseiten anbieten können. Je nach Angebot, kann der Kunde mit dem Zugriff auf eine Webseite auch eigene Programme, die er dort abgelegt hat, zur Ausführung bringen lassen. Unter Umständen stellen Hosting-Provider auch Platz für andere Dienste zur Verfügung, z.B. E-Mail. Charakteristisch für diese Dienstleistung ist, dass der Hosting-Provider gewöhnlich nicht am Abspeichern der Informationen auf seinem Webserver beteiligt ist. Diesfalls handelt es sich um automatisierte Programmabläufe, die allein der Content-Provider veranlasst und kontrolliert.

2.313 Network-Provider

Die Network-Provider (in der Grafik: „Netzdienstleister“) verbinden sich über ihr Kommunikationsnetz mit verschiedenen Access-Providern, anderen Network-Providern und möglichen Grosskunden, die keinen eigenen Access-Provider (unten Ziff. 2.314) benötigen. Über diese Netze wird der Datentransport abgewickelt; auch dieser beruht auf automatisierten Programmabläufen.

2.314 Access-Provider

Die Access-Provider (in der Grafik: „Zugangsdienstleister“, auch Zugangsvermittler) vermitteln Endbenutzern oder Firmen den Zugang ins Internet. Dieser Zugang kann über das Telefon oder einen Breitbandzugang (ADSL, Cablemodem, Wireless Local Loop, Satellit, Mietleitung, usw.) erfolgen. In der Regel weist der Zugangsdienstleister den Endbenutzern dynamisch eine stets wechselnde Internetadresse zu. Firmen und Endbenutzer, die auch Inhalte bereitstellen wollen, erhalten jedoch üblicherweise eine oder einen ganzen Block fester Adressen aus dem Adressbereich, den der Zugangsdienstleister verwaltet. Auch diese Prozesse laufen automatisch ab, d.h. ohne manuelle Intervention des Access-Providers.

In der Regel betreiben die Zugangsdienstleister auch einen *Domain Name System* (DNS)-Server, der symbolische Namen auf Internetadressen auflöst [30]. Dies ist jedoch nicht zwingend nötig, da es auch öffentlich zugängliche DNS-Server gibt, die man nutzen kann, um symbolische Namen zu veröffentlichen bzw. symbolische Namen aufzulösen.

2.32 Die Nutzer

Die Nutzer bzw. Benutzer (User) stehen am anderen Ende des Kommunikationsprozesses. Sie sind es, welche die auf einem Web-Server bereitgehaltenen Informationen zu Hause, im Büro, im Cybercafé oder mobil mit ihrem Laptop oder Telefon abrufen.

2.33 Austauschbarkeit und Multifunktionalität

Die in Ziff. 2.31 und 2.32 beschriebenen Rollen sind austauschbar. Wer beispielsweise in einem Peer-to-Peer-Dienst (vgl. oben Ziff. 2.311) Musikdateien sucht und auf seine Festplatte lädt, ist als *Nutzer* zu bezeichnen. Autorisiert dieser Nutzer aber gleichzeitig den Online-Zugriff auf einen Teil seiner Festplatte, der Musikdateien zum Abruf und Download enthält, wird er zum *Content-Provider* (sowie *Hosting-Provider* seiner selbst).

Dienstleister üben häufig mehrere Funktionen gleichzeitig aus. So kann ein Medienunternehmen beispielsweise auf seiner Website neben eigenen Inhalten auch Dritten in einem Web-Forum Speicherplatz für deren Inhalte zur Verfügung stellen. Somit ist es in Bezug auf die eigenen Inhalte *Content-Provider*, aber hinsichtlich des

[30] Beispiel.: www.ofj.admin.ch wird so auf die numerische Adresse 193.5.216.22 abgebildet.

Web-Forums in der Regel blosser *Hosting-Provider*. Die Übergänge von einer Funktion zur anderen sind zudem *fliessend*.

Im erwähnten Beispiel kann das Medienunternehmen etwa auch bezüglich der fremden Informationen im Web-Forum zu einem Content-Provider werden, wenn ein verantwortlicher Mitarbeiter das Forum moderiert oder nur inhaltlich kontrollierte Beiträge veröffentlicht; dies wird als „Zueigenmachen“ der fremden Informationen betrachtet. Häufig ist auch die Doppelfunktion als Hosting- und Access-Provider.

2.34 Die Beteiligten an anderen Diensten des Internet

Die oben beschriebenen Funktionen der Beteiligten gelten ebenso für die anderen Dienste, die im Internet zum Einsatz kommen. Zu nennen sind vor allem E-Mail, Newsgroups, Dateitransfer (ftp), online-chat (IRC), Web-Streaming (Radio, Fernsehen,Video) u.a.

Grundsätzlich lassen sich diese Provider-Kategorien auch auf die Festnetz- und Mobilfunktelefonie sowie andere Kommunikationsformen übertragen (siehe unten Ziff. 2.4).

2.4. Netzwerke

2.41 Telekommunikation im Allgemeinen

Telekommunikation ist der technische Vorgang des elektrischen, magnetischen, optischen oder elektromagnetischen Sendens, Übertragens und Empfangens von Informationen jeglicher Art. Damit lassen sich Zeichen, Sprache, Bilder, Töne oder multimediale Dokumente, die von Computern, Mikroprozessoren oder anderen Geräten zumeist digital verarbeitet bzw. gespeichert werden, schnell und kostengünstig transferieren.

Die Datenübertragung selbst findet zum Teil noch mit analogen Techniken statt: Digitale Daten werden also zunächst in analoge Signale umgewandelt, die kontinuierlichen Veränderungen von elektrischen Spannungen, Schallwellen oder Magnetisierungen entsprechen; sie werden dann so an die Zielgeräte gesendet, welche sie wieder in digitale Daten zurückverwandeln.

2.42 Elektronisches Kommunikationsnetz

Als Kommunikationsnetz oder Datennetz bezeichnet man den Zusammenschluss von Computern oder anderen Telekommunikationsgeräten durch terrestrische *Kabel*netze oder kabellose *Funk*netze. Solche Kommunikationsnetze beruhen auf verschiedenen Übertragungstechniken und unterscheiden sich auch in der Art des logischen Datentransports.

Es ist daher wichtig, nicht nur vom „Internet“ zu sprechen, wenn strafrechtliche Probleme der Informationsübertragung diskutiert werden. Eine ehrverletzende

Äusserung oder ein kinderpornographisches Bild kann sowohl via das Internet (FTP, E-Mail, WWW), Mobiltelefonnetz (SMS, MMS) oder ein geschlossenes lokales Firmennetz (LAN), das sich nicht unbedingt der Internet-Technologie bedienen muss, übertragen werden.

2.43 Verschiedene Arten von elektronischen Kommunikationsnetzen

Spricht man von elektronischen Kommunikationsnetzen, empfiehlt es sich, das *Open Systems Interconnect* (OSI)-Referenzmodell der *International Standards Organization* (ISO) zur Begriffsdefinition zu verwenden. Dieses Modell geht *technologieunabhängig* davon aus, dass sich ein Netz in sieben Schichten zerlegen lässt, bei dem die jeweils höhere Schicht auf Diensten der darunterliegenden Schicht(en) aufsetzt und ihrerseits wiederum Dienste an höhere Schichten oder an die Benutzer (oder Endgeräte) zur Verfügung stellt. Auf der untersten Ebene (1) spricht man jeweils vom physischen Datentransport, der über die verschiedensten Medien (elektrisch, optisch usw.) erfolgen kann. Auf der höchsten Schicht (7) werden dem Nutzer Dienste angeboten, z.B. Telefonie, Fernsehen, E-Mail oder das World Wide Web.

In der Praxis unterscheidet man häufig zwischen *verschiedenen Arten von Netzen*, die entweder auf Grund der angebotenen Dienste [31] oder des physischen Übertragungsmediums [32] zu ihren Namen kommen. Wichtig ist jedoch, dass *zum einen* Netze unabhängig vom physischen Übertragungsmedium technisch miteinander verbunden werden können und dass *zum andern* die angebotenen Dienste auch auf anderen Medien als den ursprünglich dafür vorgesehenen angeboten werden können. Die Internetprotokolle stellen eine weltweit akzeptierte[33] Basis dar, auf der Endbenutzerdienste unabhängig vom physischen Übertragungsmedium angeboten werden können:

- **Telefonfestnetz**
  Es beruhte früher ausschliesslich auf *analoger* Übertragungstechnologie. Nunmehr ist es in der Grundstruktur zu einem *digitalen* Netz mit paketvermittelter Sprache [34] umgebaut worden. Bereits heute bedienen sich Telekommunikationsanbieter ansatzweise der Internettechnologie (*IP Telephony*) und vermitteln damit Telefongespräche über dieselbe physische Netzinfrastruktur, die jetzt das öffentliche Internet ausmacht. Bei neu einzurichtenden privaten Nebenstellenanlagen ist dies für Unternehmen schon jetzt eine gangbare

[31] Z.B. Mobiltelefonnetz, Kabelnetz (für Radio und Fernsehen).

[32] Wireless LAN (WLAN), Ethernet, Glasfasernetze.

[33] Bis 1994 strebten verschiedene Computerhersteller und die ISO danach, andere Kommunikationsprotokolle am Markt zu standardisieren. Durch ihre einfachere Struktur und ihre Verfügbarkeit in vielen Betriebssystemen erreichten jedoch die konkurrierenden Internetprotokolle den Durchbruch und haben sich inzwischen als der de-facto-Standard etabliert.

[34] Um unerwünschte Verzögerungszeiten bei der Sprachübermittlung zu vermeiden, wurde bisher eine dedizierte Leitung vom Anrufer zum Angerufenen geschaltet. Ein Nachteil ist dabei, dass diese Verbindung durch Sprechpausen nie voll genutzt wird. Wenn die Sprache dagegen künftig z.B. wie beim Internet Protokoll (IP) *in Pakete aufgeteilt* wird, die einzeln durch das Netz vermittelt werden, lassen sich die Pausen für andere Nutzer verwenden, und die Leitungskapazität wird dadurch vervielfacht.

Alternative, um über dieselbe physische Verkabelung zu telefonieren und ihre Rechner zu koppeln.

- **Mobiltelefonnetz**
  Das Mobiltelefon- bzw. Mobilfunknetz ist eine Erweiterung des Telefonfestnetzes. Neben der Sprachübermittelung und SMS (sowie multimedialen Erweiterungen) stellt es zusätzliche Dienste zur Verfügung, die über das Festnetz hinausgehen. Als physische Übertragungsverfahren werden in der Regel digitale paketorientierte Funktechniken (z.B. GSM, CDMA) verwendet, die vor allem auf die Übertragung von Sprache zugeschnitten sind. Inzwischen gibt es aber auch Versuche, Mobiltelefonie (wieder auf der Basis der *IP Telephony*) über drahtlose Datennetze (WLAN oder auch IEEE 802.11 genannt) durchzuführen.
- **TV-Kabelnetze**
  Die ursprünglich für die einseitige Verbreitung von Radio- und Fernsehsendungen eingerichteten TV-Kabelnetze sind mittlerweile in ihrem physischen Aufbau weitgehend auf den zweiseitigen Datenaustausch umgerüstet worden. Somit ist seit geraumer Zeit sowohl eine Anbindung ans Internet als auch an das Telefonnetz mittels IP Telephony möglich.
- **Stromkabelnetze**
  Auch traditionelle Verteilnetze für elektrischen Strom eignen sich für die Datenübertragung. So gibt es einige Energieversorgungsunternehmen, die damit experimentieren und erwägen, als Internet-Service-Provider und alternative Telefonieanbieter aufzutreten [35].

Wie aus dem oben Gesagten hervorgeht, nimmt das *Internet* eine Brückenfunktion namentlich zwischen den verschiedenen erwähnten physischen Netzen wahr. Es bietet auf einer logischen Ebene (OSI Schicht 3) einen universellen Dienst an, über den Datenübertragungen für die unterschiedlichsten Anwendungen möglich sind. Dazu gehören, neben den Computerdaten, auch Telefonie, Radio, Fernsehen und Video (dazu eingehend unten Kapitel 3).

2.44 Breiter Regelungsansatz erforderlich

Da verschiedene Kommunikationsprotokolle existieren und diese sich ständig weiterentwickeln, sollte man nicht TCP/IP und das Internet zum Ausgangspunkt einer gesetzlichen Regelung der Verantwortlichkeit machen. Vielmehr sollte sich deren Anwendungsbereich auf *alle weltumspannenden Übertragungsmedien* erstrecken, die es normalen Endbenutzern erlauben, sich an dieser Übertragung als vollwertige Teilnehmer zu beteiligen.

Durch diesen breiten Ansatz würde die Regelung für alle an der Informationsübermittlung und -bereitstellung in einem Kommunikationsnetz Beteiligten gelten, unabhängig von den jeweils eingesetzten Standards und Protokollen.

---

[35] Die Freiburgischen Elektrizitätswerke (FEW) und der Telekommunikations-Provider Sunrise bieten seit September 2001 einen Internet-Zugang über Stromkabel an, der als kostengünstige, flexiblere und leistungsfähigere Alternative zur herkömmlichen Zugangstechnik über das Telefonnetz aufgebaut werden soll.

2.5 Massen- und Individualkommunikation

Es ist wichtig, zwischen Straftaten im Bereiche der Individual- und solchen im Bereiche der Massenkommunikation zu unterscheiden. Denn in der Individualkommunikation gilt das *Fernmeldegeheimnis*. Das führt zu einem stärkeren *Schutz* des Informationsausstausches vor Eingriffen Dritter, inklusive Access-, Hosting- und Network-Providern.

2.6. Elektronische Kommunikationsnetze und Medien

2.61 Wichtige Abgrenzungen zwischen Fernmelde- und Medienrecht

Es ist wichtig, eine saubere *dogmatische Abgrenzung* zu ziehen zwischen

- den *Fernmeldedienstleistungen*, die sich auf das „fernmeldetechnische Übertragen von Informationen für Dritte“ (Art. 3 lit. b des Fernmeldegesetzes, FMG [36]) als technische, weitgehend automatisierte *Infrastrukturleistung* beziehen,

- und dem Bereich der *massenmedialen Informationsverbreitung*, die sich auf die *Informationsinhalte* bezieht.

Wird etwa eine Nachrichtensendung des Fernsehens wie „10 vor 10“ als Videostream über das Internet angeboten, so ergeben sich dabei *Überschneidungen* fernmelderechtlicher sowie medienrechtlicher Art. Da das Strafrecht an diese Unterscheidung anknüpft, indem es eine Sonderregelung für Mediendelikte statuiert (Art. 27, 322bis StGB), ist die klare Zuordnung der von den Beteiligten erbrachten Dienstleistungen in den entsprechenden Regelungsrahmen von eminenter Bedeutung [37].

Die erwähnten Überschneidungen (siehe auch untenstehende Grafik) verhindern auch, die Probleme allein im Kontext des Fernmeldegesetzes zu lösen bzw. allen an der Datenübertragung in Kommunikationsnetzen Beteiligten die Rolle eines Anbieters von Fernmeldediensten i.S.von Art. 3 lit. b und c FMG zuzuweisen [38].

---

[36] SR 784.10.

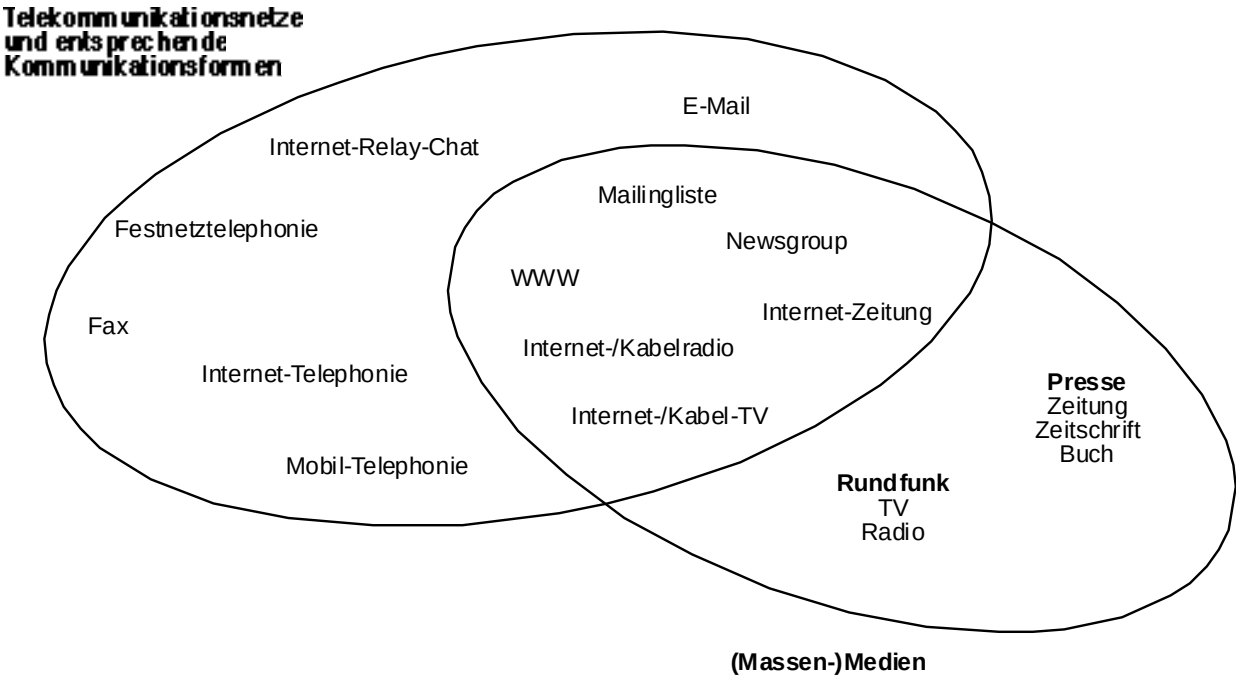
[37] Dazu eingehend: NIGGLI/SCHWARZENEGGER, (Bibl.), S. 61 ff.

[38] Art. 3 FMG

…

b. Fermeldedienst: fernmeldetechnische Übertragung von Informationen für Dritte;

c. fernmeldetechnische Übertragung: elektrisches, magnetisches, optisches oder anderes elektromagnetisches Senden oder Empfangen von Informationen über Leitungen oder Funk;



Problematisch an einer direkten Übernahme des Begriffes „Anbieter von Fernmeldedienstleistungen“ wäre, dass nur die Übertragung, nicht aber das Bereitstellen oder -halten zum Zwecke der fernmeldetechnischen Übertragung damit erfasst wird. Ausserdem sieht Art. 2 FMG eine Ausnahme für Programme i.S. des Radio- und Fernsehgesetzes (RTVG) [39] vor, worunter wohl auch bestimmte Sendungen des Internetradios und -fernsehens fielen. Schliesslich erstreckt sich das FMG nur auf Kommunikationsdienste, nicht aber auf Informations- und Mediendienste.

2.62 Technische Entwicklung hat das Recht überholt

In der klärungsbedürftigen Regelungsmaterie geht es um einen breiter gefassten Dienstleistungsbereich, namentlich um Kommunikations-, Informations- und Mediendienste (d.h. Kommunikationsträger *und* -inhalt). Durch die technische Entwicklung ist die Konvergenz dieser Bereiche weit fortgeschritten, während die rechtliche Normierung noch weitgehend auf einer Trennung zwischen Individual- und Massenkommunikation beruht.

2.63 Elektronisches Kommunikationsnetz als neuer Zentralbegriff

Gerade für in Kommunikationsnetzen auftretende strafbare Handlungen bedarf es dringend einer klaren Verantwortungsausscheidung zwischen Urhebern und Bereitstellern von Informationen, Diensteanbietern, die solche Informationen in einem Kommunikationsnetz zur Nutzung bereithalten, und Diensteanbietern, die lediglich den technischen Zugang zu solchen Informationen in Kommunikationsnetzen ermöglichen. Daher soll in diesem Bericht der bisher nicht verwendete Begriff des

[39] SR 784.40

„elektronischen Kommunikationsnetzes“ (kurz: Kommunikationsnetz) eingeführt werden (siehe dazu unten Ziff. 9.21).

Alternativ hierzu werden in der internationalen Literatur auch folgende Begriffe verwendet:

Informationssysteme (Begriff aus dem EU-Recht):
Der Begriff „Informationssystem“ wird im Rahmen der EU (III. Säule, Rahmenbeschluss über Angriffe auf Informationssysteme) bewusst im weitest möglichen Sinne verwendet, um dem Zusammenwachsen der elektronischen Netze und der unterschiedlichen über sie verbundenen Systeme Rechnung zu tragen. Er schliesst daher Computer, elektronische Organiser, Mobiltelefone, interne und externe Netze ebenso ein wie die Netze, Server und sonstigen Infrastrukturen des Internet.
Datennetz (Cybercrime Convention):
Als Rahmenbegriff wird in der Cybercrime Convention des Europarates von Datennetzen und der Datennetzkriminalität gesprochen.

Zugangs- und Inhaltskontrollen im Internet sind zwar teilweise möglich, doch sind sie ausserordentlich aufwändig und bleiben dennoch oft lückenhaft. Zudem findet sich für jedes Kontrollinstrument eine entsprechende Umgehungsmöglichkeit.

3. Technische Kontrollmöglichkeiten

3.1 Ziel und Grundsätze des Internet

Das Internet wurde mit dem Ziel entwickelt, ein sehr dezentral organisiertes, hochverfügbares *Kommunikationsnetz* bereitzustellen. Dieses sollte namentlich auch bei Ausfällen einzelner Knoten oder Verbindungen (z.B. als Folge eines militärischen Angriffs) seinen Nutzern weiterhin zur Verfügung stehen. Zu seinem Betrieb sind keine zentralen Instanzen nötig. Jeder Knoten ist für sich selbständig, und keine Organisation kontrolliert das Internet allein.

Jeder, der die technischen Möglichkeiten besitzt, kann sich an das Internet anschliessen. Die Protokolle, mit denen kommuniziert wird, und die Art der angebotenen Dienstleistungen werden in der sog. Internet Engineering Taskforce (IETF), einem offenen nicht-staatlichen Standardisierungsgremium, nach mehrheitlicher Übereinkunft aufgestellt, so dass niemand (kein Hersteller oder Staat) einzeln über Teile des Internet bestimmen kann. Auf Grund dieser dezentralen Organisation gibt es nur sehr begrenzte technische Möglichkeiten, den Zugang zu gewissen Diensten, Inhalten oder zu andern Teilnehmern zu kontrollieren bzw. einzuschränken.

3.2 Kontrollen

Man kann zwei Ansätze zur Kontrolle unterscheiden:

- ***Zugangskontrolle* : Welche Server oder welche Dienste kann ein Benutzer erreichen?**
- ***Inhaltskontrolle*: Welche Inhalte werden bereitgestellt? [40]**

[40] Eine gute Darstellung findet sich etwa bei ULRICH SIEBER, Verantwortlichkeit im Internet, München 1999 .

3.21 Zugangskontrolle

3.211 News

Bei News kann ein Hosting-Dienstleister (vgl. oben Ziff. 2.312) den Zugang zu gewissen Newsgruppen sperren, indem er sie nicht auf seine Infrastruktur kopiert. Er muss dazu von den Namen der Newsgruppen ausgehen und entscheiden, ob der Name Rückschlüsse auf mögliche illegale Inhalte erlaubt. Diese Unterscheidung kann im Einzelnen Schwierigkeiten bereiten, da in solchen Gruppen die Mehrzahl der Beiträge durchaus gesetzeskonform sein kann. Die Benutzer können eine Sperrung sehr leicht umgehen, indem sie auf andere öffentlich zugängliche News-Server ausweichen.

3.212 World Wide Web

Beim World Wide Web (WWW, Web) kann der Zugangsdienstleister (vgl. oben Ziff. 2.314) seine Benutzer anweisen, den Webzugriff über einen sogenannten *Proxy-Server* zu leiten, um populäre Internetseiten schneller zu laden. Der Proxy-Server fängt Anfragen für Webseiten ab und prüft in seinem lokalen Speicher, ob eine solche Seite vor kurzem aufgerufen wurde und zwischengespeichert ist. Trifft dies zu, beantwortet er die Anfrage direkt, ohne den gewünschten Inhalt erneut über das Internet zu holen.

Bietet der Zugangsdienstleister den Zugang zum Web nur über einen Proxy-Server an, so kann dieser auch dazu genutzt werden, Zugriffe auf bestimmte Webseiten (URL) oder Server (IP Adressen) zu verbieten (vgl. Beispiel im untenstehenden Kästchen).

Proxy-Server im arabischen Raum

***Etisalat,* der Internet-Zugangsanbieter in den Vereinigten Arabischen Emiraten (VAE), betreibt einen Proxy-Server als ausschliesslichen Zugang zum Web. Es existieren allerdings zahlreiche Beschreibungen, wie dieser Proxy-Server zu umgehen ist und damit auch in den VAE der - dort *illegale* - Zugang zu anderen Webseiten möglich wird [41].**

Da die Benutzung eines Proxy-Servers bei den Benutzern direkt im Web-Browser konfiguriert werden muss, somit vom Benutzer abhängig ist, bieten die öffentlichen Zugangsdienstleister in der westlichen Welt regelmässig auch den direkten Zugang zum WWW an. Entwicklungen neueren Datums sind sogenannte *transparente* Proxys (die nicht mehr im *Browser* des Benutzers konfiguriert werden müssen), mit deren Hilfe der Internetzugang beschleunigt wird und mit welchen man auch den Zugriff auf bestimmte URL kontrollieren könnte [42].

[41] z.B. http://djsyndrome.homestead.com/proxies1.html
[42] z.B.. die Content Engine von Cisco http://www.cisco.com/warp/public/cc/pd/cxsr/ces/index.shtml

Der Zugangsdienstleister kann auch seine *Router* [43] bzw. andere Geräte [44], über welche der Datenfluss geleitet wird, so konfigurieren, dass sie Datenpakete mit bestimmten Zieladressen (oder Quelladressen) oder gar HTTP-Pakete mit bestimmten URL herausfiltern und nicht zulassen. Die Einrichtung solcher Zugangskontrollen bedeutet jedoch in der Regel immer, dass der Datendurchsatz des *Routers* (oder der anderen Geräte) abnimmt, da für jedes Datenpaket die Liste der blockierten Adressen abgesucht werden muss.

Eine solche Filterung wird daher bei Zugangsdienstleistern, die viele Kunden bedienen, in der Regel nur sehr restriktiv verwendet werden können. Eine Verzögerung der Internet-Nutzung aufgrund einer Filterung wird von den Kunden, die sich an immer höhere Geschwindigkeiten gewöhnt sind, nicht akzeptiert. Es bestünde auch ein Gegensatz zu der aus technologie-, sozial-, bildungs-, und wirtschaftspolitischen Gründen erwünschten raschen Verbreitung von schnellen und kostengünstigen Internetzugängen.

Bei der Sperrung des Zugangs zu Servern oder Websites ist ferner zu berücksichtigen, dass dadurch häufig eine Vielzahl von rechtlich zulässigen Inhalten ebenfalls mitbetroffen ist. Wird z.B. der Server eines Hosting-Providers wie *geocities* gesperrt, können daduch Tausende von Websites betroffen sein.

Zudem gibt es auch hier für entsprechend motivierte und versierte Benutzer verschiedene *Umgehungsmöglichkeiten*: So gibt es etwa öffentliche Proxy-Server, die bei anderen Internetdienstleistern (z.B. im Ausland) stehen und den Zugang auf gesperrte Dienste indirekt ermöglichen [45].

Auch kann der Inhaltsanbieter seine Serveradresse ändern, so dass die bisherigen Filterregeln nicht mehr gültig sind und die eingerichtete Zugangssperre nutzlos wird. Die bisherigen Erfahrungen zeigen, dass Anbieter von illegalen Inhalten von dieser Möglichkeit jeweils schnell Gebrauch machen.

3.22 Inhaltskontrolle

Für eine solche Kontrolle muss der Hosting-Dienstleister regelmässig die auf seinen Rechnern angebotenen Inhalte (Texte und multimediale Daten) untersuchen. Angesichts der sehr grossen Datenvolumina (viele Tera-[Billionen-] Bytes) und der hohen Änderungsraten stellt eine derartige Inhaltskontrolle den Hosting-Dienstleister vor grosse, oft unlösbare Probleme.

Eine zuverlässige vollautomatisierte Suche nach urheberrechtlich geschützten oder gar nach illegalen Inhalten ist *unmöglich*. Algorithmen zur semantischen Text- bzw. Bildanalyse gibt es zwar, doch sind sie rechenintensiv und zudem fehleranfällig; die diesbezügliche Forschung ist denn auch noch im Gange.

---

[43] z.B. http://www.cisco.com/warp/public/44/jump/routers.shtml
[44] z.B. *Firewalls* http://www.checkpoint.com oder Geräte zur Bandbreitenverwaltung, z.B. www.packeteer.com
[45] Ein Verzeichnis findet man z.B. unter http://tools.rosinstrument.com/proxy/

Man kann zwar rasch nach „elektronischen Fingerabdrücken“[46] bekannter Texte oder multimedialer Daten suchen. Durch Abändern der Dateien - ein Bit genügt -, kann ein Anbieter jedoch problemlos vermeiden, dass sich seine Inhalte so identifizieren lassen. Angesichts der Vielzahl von Hosting-Dienstleistern kann ein Inhaltsanbieter in der Regel problemlos auf einen anderen Hosting-Dienstleister (auch in einem anderen Land) ausweichen, wenn er das Gefühl hat, seine angebotenen Inhalte würden zensiert.

Immer populärer werden *Peer-to-Peer* (P2P)-Dienste zum direkten Datenaustausch zwischen Endbenutzern ohne zentrale Vermittlungsinstanz. Bei diesen Diensten kann die Inhaltskontrolle nur durch den Endbenutzer erfolgen. Er kann bei *Filesharing-Diensten*, beispielsweise Gnutella oder Morpheus, entscheiden, welche Dateien er anbieten möchte. Nimmt er jedoch an einem Dienst wie *Freenet* [47] teil, dann ist ihm eine Inhaltskontrolle auf Grund des spezifischen Entwurfs verunmöglicht, da die angebotenen Daten verschlüsselt auf seinem Rechner abgelegt sind und er den Schlüssel nicht kennt.

3.3 Wirksamkeit

Zusammenfassend ist festzustellen, dass sich das Internet auf Grund seines Entwurfs *einer zentralen Kontrolle oder Aufsicht entzieht*. Alle uns bekannten Kontrollmassnamen lassen sich von mehr oder weniger geschickten Benutzern und auch von den Anbietern illegaler Inhalte umgehen.

Jede neue in Aussicht genommene Kontrollmassname zieht unmittelbar eine technische Entwicklung zum Zweck ihrer Umgehung nach sich [48]. Somit können verordnete Kontrollmassnahmen zwar die Zugangsschwelle zu illegalen Inhalten erhöhen, doch bleiben allemal Möglichkeiten, sie zu umgehen.

Insgesamt erscheint es bereits aus technischen Gründen *nicht sinnvoll*, Access-Provider zur Sperrung des Zugangs zu illegalen Inhalten zu verpflichten oder Hosting-Dienstleister zu verpflichten, die Gesetzeskonformität aller bei ihnen von Dritten angebotenen Inhalte präventiv zu kontrollieren.

---

[46] Ein „elektronischer Fingerabdruck“ ist häufig eine 32-160 Bit lange Binärzahl, die mit mathematischen Verfahren aus einem elektronischen Dokument oder Bild errechnet werden kann und für dieses charakteristisch ist. Wird auch nur ein Bit in dem Dokument geändert, so ändert sich auch der Fingerabdruck.

[47] http://freenetproject.org/ , Beschreibung auf Deutsch unter http://archiv.tu-chemnitz.de/pub/2002/0050/data/vortrag.html

[48] Die drohende Schliessung von *Napster* war einer der Gründe, um völlig dezentrale Filesharingdienste wie z.B. Gnutella zu entwickeln, bei denen kein zentraler Rechner mehr eine Vermittlungsfunktion wahrnimmt.

Die namentlich durch das World Wide Web ermöglichte weltweite Verbreitung von Informationen verlangt nach internationaler rechtlicher Koordination. Für die Schweiz ist deshalb von grosser Bedeutung, auf welche Grundsätze sich die EU-Länder in der „E-Commerce-Richtlinie" verständigt haben.

4. Die E-Commerce-Richtlinie der EU und ihre Umsetzung in den Nachbarstaaten der Schweiz

4.1 Allgemeines zur Richtlinie 2000/31 des Europäischen Parlaments und des Rates („E-Commerce-Richtlinie") vom 8. Juni 2000

Das Europäische Parlament und der Rat der Europäischen Union haben am 8. Juni 2000 die Richtlinie 2000/31/EG über bestimmte Aspekte der Dienste der Informationsgesellschaft, insbesondere des elektronischen Geschäftsverkehrs, im Binnenmarkt („Richtlinie über den elektronischen Geschäftsverkehr") erlassen [49].

Dieser 24 Artikel umfassenden Richtlinie werden 25 *Erwägungsgründe* vorausgeschickt. Danach soll die E-Commerce-Richtlinie gewährleisten, dass der elektronische Geschäftsverkehr *die Chancen des Binnenmarktes voll nutzen kann*. Dies soll geschehen durch *Beseitigung rechtlicher Hemmnisse*, die sich einerseits aus den unterschiedlichen innerstaatlichen Rechtsvorschriften und andererseits aus der Rechtsunsicherheit hinsichtlich der auf Dienste der Informationsgesellschaft anzuwendenden nationalen Regeln ergeben.

Um künftig *Rechtssicherheit* zu erreichen und das Vertrauen der Konsumenten (nach EU-Terminologie: „Verbraucher") zu gewinnen, müsse die Richtlinie einen klaren rechtlichen Rahmen für den Binnenmarkt bezüglich bestimmter rechtlicher Aspekte des elektronischen Geschäftsverkehrs festlegen.

Ziel der Richtlinie sei es, einen rechtlichen Rahmen zur Sicherstellung des freien Verkehrs von Diensten der Informationsgesellschaft zwischen den Mitgliedstaaten zu schaffen, *nicht aber, den Bereich des Strafrechts als solchen zu harmonisieren* [50,51].

---

[49] E-Commerce-Richtlinie, zitiert: RICHTLINIE (Bibl.).

[50] Siehe RICHTLINIE (Bibl.), S. 2 f., Ziff. 5-8. In Art. 1 Abs. 2 der Richtlinie wird allgemein gesagt, sie verfolge (nur) eine *Angleichung* bestimmter für die Dienste der Informationsgesellschaft geltender innerstaatlicher Regelungen, namentlich auch hinsichtlich der Verantwortlichkeit der Vermittler bzw. Provider.

[51] Eine *Harmonisierung des Strafrechts und Strafprozessrechts* verfolgt hingegen die Europaratskonvention über die Cyberkriminalität, ETS-No. 185, (*„Cybercrime-Convention"*), welche am 23. November 2001 in Budapest, namentlich auch von der Schweiz, unterzeichnet wurde. Der

Insbesondere sollen die grundlegenden Regeln des einzelstaatlichen Rechts, die die freie Meinungsäusserung betreffen, von dieser Richtlinie unberührt bleiben [52].

Nach dem *Grundsatz der Verhältnismässigkeit* seien in der Richtlinie nur diejenigen Massnahmen vorgesehen, die zur Gewährleistung des reibungslosen Funktionierens des Binnenmarktes unerlässlich seien. Wo dementsprechend ein Handeln auf Gemeinschaftsebene geboten sei, solle die E-Commerce-Richtlinie hingegen ein hohes Schutzniveau für die dem Allgemeininteresse dienenden Ziele, insbesondere für den Jugendschutz, den Schutz der Menschenwürde, den Verbraucherschutz und den Schutz der öffentlichen Gesundheit gewährleisten [53].

4.2 Die Artikel 12–15 der E-Commerce-Richtlinie (Verantwortlichkeit der Vermittler)

4.21 Vorbemerkungen

Die *Verantwortlichkeit der „Diensteanbieter"* [54], d.h. der Provider, ist *einer der wichtigsten Regelungsbereiche* der E-Commerce-Richtlinie. Er befindet sich dementsprechend im Zentrum der Richtlinie, in den Art. 12 – 15, unter dem Titel „Verantwortlichkeit der Vermittler".

Um dem in den Erwägungsgründen der Richtlinie definierten Ziel der Beseitigung von Rechtsunsicherheit [55] zu entsprechen, wird in Art. 12 - 15 vor allem gesagt, in welchen Fällen oder unter welchen Voraussetzungen die *Provider nicht verantwortlich* sind.

Begrifflich wird hier von „Ausnahmeregelungen" beziehungsweise „Ausnahmen", „Haftungsausschluss" oder „Beschränkung der Verantwortlichkeit" gesprochen [56]. Damit wird in der Richtlinie implizit vom *Prinzip der Verantwortlichkeit der Provider* ausgegangen. Auf welchen allgemeinen Grundsätzen diese Verantwortlichkeit beruht beziehungsweise wie diese begründet wird, bleibt dabei weitgehend offen; sie kann allenfalls - etwas schwerfällig - aus den Ausnahmeregelungen *e contrario* geschlossen werden [57].

---

offizielle Titel dieser europäischen Cybercrime-Konvention lautet „Convention on Cybercrime (Convention sur la cybercriminalité)". Der Wortlaut der Cybercrime-Convention ist unter http://conventions.coe.int im Internet abrufbar. Näheres zum Inhalt: unten Ziff. 10.21. - Vgl. ferner die *„Déclaration sur la liberté de la communication sur l'Internet"* des Ministerkomitees des Europarates vom 28. Mai 2003, in der sich die zentralen Grundsätze de E-Commerce-Richtlinie niedergeschlagen haben. Dieser Text ist unter folgender Adresse im Internet abrufbar: http://www.coe.int/T/F/Droits_de_l%27Homme/media/5_Ressources_documentaires/1_Textes_de_base/2_%20Textes_du_Comite_des_Ministres/PDF_D%E9claration%20libert%E9%20de%20communication%20sur%20Internet%20%20(f).pdf

[52] RICHTLINIE (Bibl.), S. 2, Ziff. 4.

[53] RICHTLINIE (Bibl.), S. 2, Ziff. 10.

[54] Die Definition hiezu ist in Art. 2 lit. b der RICHTLINIE (Bibl.) zu finden. „Diensteanbieter" ist demnach jede natürliche oder juristische Person, die einen Dienst der Informationsgesellschaft anbietet.

[55] RICHTLINIE (Bibl.), S. 6, Ziff. 40.

[56] RICHTLINIE (Bibl.), S. 6, Ziff. 42-46.

[57] Nach SATZGER (Bibl.), S. 109 ff., 111, hätten dementsprechend Art. 12-15 der Richtlinie die Funktion eines „Filters", d.h. die Richtlinie bezwecke damit „eine generelle Einschränkung der

Auch in den Erwägungsgründen wird nicht dargelegt, worauf die Verantwortlichkeit der Provider beruhen soll. Hingegen wird dort betont, die in der Richtlinie hinsichtlich Verantwortlichkeit festgelegten Ausnahmen würden nur Fälle abdecken, „in denen die Tätigkeit des Providers auf den technischen Vorgang beschränkt ist, ein Kommunikationsnetz zu betreiben und den Zugang zu diesem zu vermitteln, über das von Dritten zur Verfügung gestellte Informationen übermittelt oder zum alleinigen Zweck vorübergehend gespeichert werden, die Übermittlung effizienter zu gestalten. Diese Tätigkeit ist rein technischer, automatischer und passiver Art, was bedeutet, dass der Anbieter eines Dienstes der Informationsgesellschaft weder Kenntnis noch Kontrolle über die weitergeleitete oder gespeicherte Information besitzt.“ [58]

Mit Art. 12 bis 15 trifft die E-Commerce-Richtlinie prinzipiell eine einheitliche Verantwortlichkeitsregelung, d.h. eine *Horizontalregelung* für alle Rechtsgebiete (Strafrecht, Haftpflichtrecht, Urheberrecht, Wettbewerbsrecht usw.) [59]. Der breite Regelungsansatz erklärt auch, warum die Richtlinie keine die verschiedenen Rechtsgebiete umfassende Begründung der Rechtsgrundlagen einer Verantwortlichkeit der Diensteanbieter liefert. Soweit es in den EU-Mitgliedstaaten keine Rechtsgrundlage für eine Verantwortlichkeit eines Teils dieser Diensteanbieter gibt, greift die E-Commerce-Richtlinie ins Leere.

Ausserdem ist zu beachten, dass die EU gestützt auf den Vertrag zur Gründung der Europäischen Gemeinschaft (EGV) *keine Rechtsetzungsbefugnis im Gebiete des originären Strafrechts* hat. Die Modifikation der Strafbarkeitsvoraussetzungen stellt folglich eine mittelbare Auswirkung der Rechtsangleichung im Binnenmarkt dar, die sich grundsätzlich nur auf entgeltliche Dienstleistungen beziehen kann. Um die angestrebte Rechtssicherheit überhaupt verwirklichen zu können, sind die Mitgliedsstaaten daher aufgefordert, eine über den Binnenmarkt, also über den Kompetenzbereich des EU-Rechts, hinausgehende Umsetzung durchzuführen [12].

4.22 Art. 12: Keine Verantwortlichkeit für reine Durchleitung

Art. 12 Reine Durchleitung

(1) Die Mitgliedstaaten stellen sicher, dass im Fall eines Dienstes der Informationsgesellschaft, der darin besteht, von einem Nutzer eingegebene Informationen in einem Kommunikationsnetz zu übermitteln oder Zugang zu einem Kommunikationsnetz zu vermitteln, der Diensteanbieter nicht für die übermittelten Informationen verantwortlich ist, sofern er

a) die Übermittlung nicht veranlasst,
b) den Adressaten der übermittelten Informationen nicht auswählt und
c) die übermittelten Informationen nicht auswählt oder verändert.

Verantwortlichkeit für unerlaubte Netz-Aktivitäten Dritter, ohne dabei materiellrechtliche Vorschriften der nationalen Rechtsordnungen, die eine Rechtsverletzung begründen, als solche zu modifizieren“.

[58] RICHTLINIE (Bibl.), S. 6, Ziff. 42.

[59] Siehe hiezu NIGGLI/SCHWARZENEGGER (Bibl.), S. 63 ff., 66 ff. Zu den grossen Nachteilen dieser Regelungstechnik – im Gegensatz zur bereichsspezifischen Regelung – insbesondere betreffend das Rechtsgebiet Strafrecht siehe a.a.O., S. 66 ff..

[61] RICHTLINIE (Bibl.), S. 6, Ziff. 43.

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

(3) Dieser Artikel lässt die Möglichkeit unberührt, dass ein Gericht oder eine Verwaltungsbehörde nach den Rechtssystemen der Mitgliedstaaten vom Diensteanbieter verlangt, die Rechtsverletzung abzustellen oder zu verhindern.

Kurz ausgedrückt, befreit Art. 12 der E-Commerce-Richtlinie die Provider von einer Haftung für die so genannt reine Durchleitung (Access-Provider, Abs. 1). Auch für ein nur kurzzeitiges, automatisches Zwischenspeichern, welches allein der Datenübertragung dient, sollen die Access-Provider nicht verantwortlich sein (Abs. 2). In beiden Fällen wird vorausgesetzt, dass sie in keiner Weise mit der übermittelten Information in Verbindung stehen, sie insbesondere nicht abgeändert haben [61].

4.23 Art. 13 und 14: Keine Verantwortlichkeit für Caching und Hosting

Art. 13 Caching

(1) Die Mitgliedstaaten stellen sicher, dass im Fall eines Dienstes der Informationsgesellschaft, der darin besteht, von einem Nutzer eingegebene Informationen in einem Kommunikationsnetz zu übermitteln, der Diensteanbieter nicht für die automatische, zeitlich begrenzte Zwischenspeicherung verantwortlich ist, die dem alleinigen Zweck dient, die Übermittlung der Information an andere Nutzer auf deren Anfrage effizienter zu gestalten, sofern folgende Voraussetzungen erfüllt sind:

a) Der Diensteanbieter verändert die Information nicht;
b) der Diensteanbieter beachtet die Bedingungen für den Zugang zu der Information;
c) der Diensteanbieter beachtet die Regeln für die Aktualisierung der Information, die in weithin anerkannten und verwendeten Industriestandards festgelegt sind;
d) der Diensteanbieter beeinträchtigt nicht die erlaubte Anwendung von Technologien zur Sammlung von Daten über die Nutzung der Information, die in weithin anerkannten und verwendeten Industriestandards festgelegt sind;
e) der Diensteanbieter handelt zügig, um eine von ihm gespeicherte Information zu entfernen oder den Zugang zu ihr zu sperren, sobald er tatsächliche Kenntnis davon erhält, dass die Information am ursprünglichen Ausgangsort der Übertragung aus dem Netz entfernt wurde oder der Zugang zu ihr gesperrt wurde oder ein Gericht oder eine Verwaltungsbehörde die Entfernung oder Sperrung angeordnet hat.

(2) Dieser Artikel lässt die Möglichkeit unberührt, dass ein Gericht oder eine Verwaltungsbehörde nach den Rechssystemen der Mitgliedstaaten vom Diensteanbieter verlangt, die Rechtsverletzung abzustellen oder zu verhindern.

Wie schon im Falle der so genannt reinen Durchleitung [62] gilt der Haftungsausschluss nur dann, wenn der Proxy-Caching-Provider mit der übermittelten Information *in keiner Weise in Verbindung steht*. Ein Proxy-Caching-Provider, der absichtlich mit einem Content-Provider zusammenarbeitet, um rechtswidrige Handlungen zu begehen, leistet dagegen klar mehr, weshalb der Haftungsausschluss für ihn nicht gilt [63].

Art. 14 Hosting

(1) Die Mitgliedstaaten stellen sicher, dass im Fall eines Dienstes der Informationsgesellschaft, der in der Speicherung von durch einen Nutzer eingegebenen Informationen besteht, der Diensteanbieter nicht für die im Auftrag eines Nutzers gespeicherten Informationen verantwortlich ist, sofern folgende Voraussetzungen erfüllt sind:

a) Der Anbieter hat keine tatsächliche Kenntnis von der rechtswidrigen Tätigkeit oder Information, und, in bezug auf Schadenersatzansprüche, ist er sich auch keiner Tatsachen oder Umstände bewusst, aus denen die rechtswidrige Tätigkeit oder Information offensichtlich wird, oder
b) der Anbieter wird, sobald er diese Kenntnis oder dieses Bewusstsein erlangt, unverzüglich tätig, um die Information zu entfernen oder den Zugang zu ihr zu sperren.

(2) Absatz 1 findet keine Anwendung, wenn der Nutzer dem Diensteanbieter untersteht oder von ihm beaufsichtigt wird.

(3) Dieser Artikel lässt die Möglichkeit unberührt, dass ein Gericht oder eine Verwaltungsbehörde nach den Rechtssystemen der Mitgliedstaaten vom Diensteanbieter verlangt, die Rechtsverletzung abzustellen oder zu verhindern, oder dass die Mitgliedstaaten Verfahren für die Entfernung einer Information oder die Sperrung des Zugangs zu ihr festlegen.

Der Hosting-Provider kann eine Beschränkung der Verantwortlichkeit nur in Anspruch nehmen, wenn er, sobald ihm rechtswidrige Tätigkeiten bekannt oder bewusst werden, selber unverzüglich tätig wird, um die betreffende Information zu entfernen oder den Zugang zu ihr zu sperren [64].

4.24 Art. 15: Keine allgemeine Pflicht zur Überwachung

Art. 15 Keine allgemeine Überwachungspflicht

(1) Die Mitgliedstaaten erlegen Anbietern von Diensten im Sinne der Artikel 12, 13 und 14 keine allgemeine Verpflichtung auf, die von ihnen übermittelten oder gespeicherten Informationen zu überwachen oder aktiv nach Umständen zu forschen, die auf eine rechtswidrige Tätigkeit hinweisen.

(2) Die Mitgliedstaaten können Anbieter von Diensten der Informationsgesellschaft dazu verpflichten, die zuständigen Behörden unverzüglich

[62] Siehe oben Ziff. 4.22 am Ende.

[63] Vgl. RICHTLINIE (Bibl.), S. 6, Ziff. 44.

[64] RICHTLINIE (Bibl.), S. 6, Ziff. 46.

über mutmassliche rechtswidrige Tätigkeiten oder Informationen der Nutzer ihres Dienstes zu unterrichten, oder dazu zu verpflichten, den zuständigen Behörden auf Verlangen Informationen zu übermitteln, anhand deren die Nutzung ihres Dienstes, mit denen sie Vereinbarungen über die Speicherung geschlossen haben, ermittelt werden können.

Gemäss Art. 15 der E-Commerce-Richtlinie darf den oben aufgeführten Providern keine allgemeine Verpflichtung auferlegt werden, die von ihnen übermittelten und gespeicherten Informationen zu überwachen oder aktiv nach Umständen zu forschen, die auf eine rechtswidrige Tätigkeit hinweisen. Die Richtlinie hindert die Mitgliedstaaten allerdings nicht daran, Verfahren für die Entfernung von Informationen oder die Sperrung des Zugangs zu ihnen festzulegen [65].

4.3 Die Umsetzung von Art. 12-15 der E-Commerce-Richtline in den EU-Nachbarstaaten der Schweiz [66]

4.31 Deutschland

Deutschland hat sich mit seinem Gesetz über die Nutzung von Telediensten, kurz: *Teledienstegesetz* (TDG), vom 22. Juli 1997[67] - ähnlich wie die E-Commerce-Richtlinie, jedoch bereits ein paar Jahre zuvor - für eine *Horizontalregelung*, d.h. eine einheitliche Verantwortlichkeitsregelung im Bereich der Informations- und Kommunikationsdienste entschieden.

Die Horizontalregelung im nationalen Recht hat zur Folge, dass der jeweilige Provider bei Erfüllung der Voraussetzungen für den Verantwortlichkeitsausschluss weder zivil- noch strafrechtlich belangt werden kann. Auf welcher Stufe der Haftungs- bzw. Strafbarkeitsvoraussetzungen diese Frage zu prüfen ist, bleibt höchst unklar (Tatbestand, Rechtswidrigkeit, Schuld oder ausserhalb dieser Struktur liegender Prüfungspunkt, s. unten Ziff. 9.121). Fest steht demgegenüber, dass bei Nichtvorliegen der erwähnten Voraussetzungen die Haftung bzw. Strafbarkeit nach den jeweiligen Tatbeständen der in Betracht kommenden Rechtsgebiete zu prüfen ist.

Zur Umsetzung der Richtlinie hat der deutsche Gesetzgeber am 14. Dezember 2001 das Gesetz über die rechtlichen Rahmenbedingungen für den elektronischen Geschäftsverkehr (*Elektronisches Geschäftsverkehrsgesetz*, EGG) erlassen. Das EGG ist am 21. Dezember 2001 in Kraft getreten.

---

[65] RICHTLINIE (Bibl.), S. 6, Ziff. 44.

[66] Im „nicht-EU“, aber EWR- und EFTA-Nachbarstaat *Liechtenstein* wurde die E-Commerce-Richtlinie bis heute noch nicht umgesetzt, d.h. es gibt keine speziellen gesetzlichen Verantwortlichkeitsregeln in diesem Bereich. - Ein 2002 vom Schweizerischen Institut für Rechtsvergleichung im Auftrag des Bundesamtes für Justiz erstattetes Gutachten über die Gesetzgebungen der 15 EU-Staaten und der USA (Stand: 23. August 2002) enthält weitere einschlägige Informationen.

[67] Fundstelle: BGBl I 1997, 1870.

Durch Art. 1 EGG wurden *neue Verantwortlichkeitsregeln in das Teledienstegesetz eingeführt* [68] [69]: Die §§ 8 bis 11 TDG n.F. befinden sich im Abschnitt 3 des TDG unter dem Titel „Verantwortlichkeit".

§ 8 Allgemeine Grundsätze

(1) Diensteanbieter sind für eigene Informationen, die sie zur Nutzung bereithalten, nach den allgemeinen Gesetzen verantwortlich.

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

§ 8 Abs. 1 regelt explizit die Haftung für eigene Informationen. § 8 Abs. 2 setzt Art. 15 Abs. 1 (Keine allgemeine Überwachungspflicht) der E-Commerce-Richtlinie um. Von der in Art. 15 Abs. 2 der Richtlinie vorgesehenen Möglichkeit der Mitgliedstaaten, die Diensteanbieter zur Unterrichtung über mutmassliche rechtswidrige Tätigkeiten zu verpflichten, hat der deutsche Gesetzgeber keinen Gebrauch gemacht.

§ 9 Durchleitung von Informationen

(1) Diensteanbieter sind für fremde Informationen, die sie in einem Kommunikationsnetz übermitteln oder zu denen sie den Zugang zur Nutzung vermitteln, nicht verantwortlich, sofern sie
1. die Übermittlung nicht veranlasst,
2. den Adressaten der übermittelten Informationen nicht ausgewählt und
3. die übermittelten Informationen nicht ausgewählt oder verändert haben.

Satz 1 findet keine Anwendung, wenn der Diensteanbieter absichtlich mit einem der Nutzer seines Dienstes zusammenarbeitet, um rechtswidrige Handlungen zu begehen.

(2) Die Übermittlung von Informationen nach Absatz 1 und die Vermittlung des Zugangs zu ihnen umfasst auch die automatische kurzzeitige Zwischenspeicherung dieser Informationen, soweit dies nur zur Durchführung der Übermittlung im Kommunikationsnetz geschieht und die Informationen nicht länger gespeichert werden, als für die Übermittlung üblicherweise erforderlich ist.

Die reine Durchleitung und die reine Zugangsvermittlung werden hier - unter gewissen Voraussetzungen - von einer Verantwortlichkeit ausgenommen.

---

[68] Fundstelle: BGBl I 2001, 3721. Link zum TDG n.F.: http://bundesrecht.juris.de/bundesrecht/tdg/index.html

[69] Die „alten" bzw. ersten Verantwortlichkeitsregeln im TDG, namentlich § 5, haben zuvor zu Problemen geführt – insbesondere was die Frage der strafrechtlichen Haftung der Zugangsvermittler angeht. Siehe hiezu statt vieler SATZGER (Bibl.), S. 113 ff. mit Nachweisen und unten Ziff. 9.121.

§ 10 Zwischenspeicherung zur beschleunigten Übermittlung von Informationen

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

§ 9 Abs. 1 Satz 2 gilt entsprechend.

Mit § 10 TDG n.F. wird Art. 13 der E-Commerce-Richtlinie fast wörtlich übernommen und so das so genannte *Proxy-Caching von einer Haftung befreit*.

§ 11 Speicherung von Informationen

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

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

§ 11 TDG n.F. regelt schliesslich die Voraussetzungen für die Befreiung der Hosting-Provider von einer Verantwortlichkeit (Umsetzung von Art. 14 E-Commerce-Richtlinie).

4.32 Österreich

In Österreich ist die Verantwortlichkeit der Diensteanbieter im *E-Commerce-Gesetz (ECG)* [70], d.h. in seinem 5. Abschnitt, geregelt. Mit §§ 13 - 19 ECG hat Österreich zum einen weitgehend die Art. 12-15 der E-Commerce-Richtlinie umgesetzt; zum

[70] Der Langtitel dieses Gesetzes lautet: Bundesgesetz, mit dem bestimmte rechtliche Aspekte des elektronischen Geschäfts- und Rechtsverkehrs geregelt werden: siehe (österr.) BGBl. I Nr. 152/2001. Das ECG ist am 1.1.2002 in Kraft getreten und ist abrufbar unter: http://www.ris.bka.gv.at/bundesrecht/

andern ist es hinsichtlich Haftungsausschluss *noch etwas weiter gegangen*, indem es auch ausdrücklich die Verantwortlichkeit bei Suchmaschinen (§ 14) und bei Links (§ 17) ausgeschlossen hat. Bei den §§ 13 ff. ECG handelt es sich - wie in der E-Commerce-Richtlinie und im deutschen TDG - um *horizontale Regelungen:*

§ 13 Ausschluss der Verantwortlichkeit bei Durchleitung

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

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

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

§ 14 Verantwortlichkeit bei Suchmaschinen

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

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

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

§ 15 Ausschluss der Verantwortlichkeit bei Zwischenspeicherungen (Caching)

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

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

zu ihr gesperrt wurde oder dass ein Gericht oder eine Verwaltungsbehörde die Entfernung oder Sperre angeordnet hat.

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

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

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

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

§ 17 Ausschluss der Verantwortlichkeit bei Links

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

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

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

§ 18 Umfang der Pflichten der Diensteanbieter

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

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

(3) Die in § 16 genannten Diensteanbieter haben auf Grund der Anordnung einer Verwaltungsbehörde dieser den Namen und die Adressen der Nutzer ihres Dienstes, mit denen sie Vereinbarungen über die Speicherung von Informationen abgeschlossen

haben, zu übermitteln, sofern die Kenntnis dieser Informationen eine wesentliche Voraussetzung der Wahrnehmung der der Behörde übertragenen Aufgabe bildet.

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

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

§ 19 Weitergehende Vorschriften

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

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

4.33 Frankreich

Frankreich hat am 1. August 2000 eine wichtige Rechtsänderung hinsichtlich der Strafbarkeitsvoraussetzungen für Provider vorgenommen. An diesem Datum wurde nämlich in das Gesetz über die Kommunikationsfreiheit (*Loi du 1er août 2000 relative à la liberté de communication*[71,72]) Art. 43-8 Abs. 1, eingefügt. Diese Bestimmung steht im Kapitel VI (Dispositions relatives aux services de communication en ligne autres que de correspondance privée).

Mit Art. 43-8 Abs. 1 wurde das *Prinzip der eingeschränkten Verantwortlichkeit* eingeführt. Demnach haftet der Provider nur dann, wenn er nach einer richterlichen Aufforderung den Zugang zu einer rechtswidrigen Internetseite nicht sperrt. Art. 43-8 Abs. 2 hielt darüber hinaus noch fest, dass eine Strafbarkeit auch dann entstehen könne, wenn der Hosting-Provider von einem Nutzer informiert würde und darauf nicht reagiere. Diese Bestimmung wurde hingegen vom Conseil constitutionnel noch vor Inkrafttreten für *verfassungswidrig* erklärt [73].

Die französischen Verantwortlichkeitsbestimmungen für Provider lauten nun wie folgt:

> **Art. 43-7.** - Les personnes physiques ou morales dont l'activité est d'offrir un accès à des services de communication en ligne autres que de correspondance privée sont

[71] Siehe auch unten Ziff. 9.121.

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

[73] Vgl. Décision du Conseil constitutionnel no 2000-433 DC du 27 juillet 2000, JO du 2 août 2000, 11922 ff., 11926. Näher hiezu MOREILLON/DE COURTEN, (Bibl.), S.12, mit weiteren Hinweisen. Zur weiteren Entwicklung der diesbezüglichen Gesetzgebung in Frankreich nach diesem Entscheid des Conseil constitutionnel siehe unten Ziff. 9.121.

tenues, d'une part, d'informer leurs abonnés de l'existence de moyens techniques permettant de restreindre l'accès à certains services ou de les sélectionner, d'autre part, de leur proposer au moins un de ces moyens.

Art. 43-8. - Les personnes physiques ou morales qui assurent, à titre gratuit ou onéreux, le stockage direct et permanent pour mise à disposition du public de signaux, d'écrits, d'images, de sons ou de messages de toute nature accessibles par ces services, ne sont pénalement ou civilement responsables du fait du contenu de ces services que :
- si, ayant été saisies par une autorité judiciaire, elles n'ont pas agi promptement pour empêcher l'accès à ce contenu;.[...]

Art. 43-9. - Les prestataires mentionnés aux articles 43-7 et 43-8 sont tenus de détenir et de conserver les données de nature à permettre l'identification de toute personne ayant contribué à la création d'un contenu des services dont elles sont prestataires.
Ils sont également tenus de fournir aux personnes qui éditent un service de communication en ligne autre que de correspondance privée des moyens techniques permettant à celles-ci de satisfaire aux conditions d'identification prévues à l'article 43-10.
Les autorités judiciaires peuvent requérir communication auprès des prestataires mentionnés aux articles 43-7 et 43-8 des données mentionnées au premier alinéa. Les dispositions des articles 226-17, 226-21 et 226-22 du code pénal sont applicables au traitement de ces données.
Un décret en Conseil d'Etat, pris après avis de la Commission nationale de l'informatique et des libertés, définit les données mentionnées au premier alinéa et détermine la durée et les modalités de leur conservation.

Art. 43-10. - I. - Les personnes dont l'activité est d'éditer un service de communication en ligne autre que de correspondance privée tiennent à la disposition du public :
- s'il s'agit de personnes physiques, leurs nom, prénom et domicile ;
- s'il s'agit de personnes morales, leur dénomination ou leur raison sociale et leur siège social ;
- le nom du directeur ou du codirecteur de la publication et, le cas échéant, celui du responsable de la rédaction au sens de l'article 93-2 de la loi no 82-652 du 29 juillet 1982 sur la communication audiovisuelle ;
- le nom, la dénomination ou la raison sociale et l'adresse du prestataire mentionné à l'article 43-8.

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

4.34 Italien

Das Italienische Parlament hat mit dem Gesetz vom 1. März 2002 (n. 39, „Disposizioni per l'adempimento di obblighi derivati dall'appartenenza dell'Italia alle Comunità europee - Legge comunitaria 2001“) unter anderem die Umsetzung der E-Commerce-Richtlinie in das italienische Recht an die Regierung delegiert; einschlägig ist *Art. 31* (Attuazione della direttiva 2000/31/CE, relativa a taluni aspetti giuridici dei servizi della società dell'informazione, in particolare il commercio elettronico, nel mercato interno) [74].

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

Die Delegationsnorm, Art. 1 der Legge cumunitaria 2001, schreibt der Regierung vor, die entsprechende Verordnung innerhalb eines Jahres nach Inkrafttreten des Gesetzes zu erlassen. Diese Frist ist inzwischen [75] unbenützt abgelaufen.

> Die Bekämpfung der Netzwerkkriminalität folgt aus dem Verfassungsauftrag zur Verhinderung von Rechtsgutverletzungen. Der Staat ist aber beim Erlass der gebotenen Massnahmen an die Grundsätze der Verfassung gebunden und muss insbesondere die Grundrechte freier Kommunikation respektieren.

[75] D.h. nach der Publikation des Gesetzes in der Gazzetta Ufficiale n. 72 vom 26. März 2002 – Supplemento Ordinario n. 54 .

5. Verfassungsrechtliche Rahmenbedingungen

5.1 Der grundrechtliche Auftrag zum Rechtsgüterschutz

5.11 Gegenstand des Schutzauftrages

Die *grundrechtlich* gewährten *Freiheiten und Integritätsrechte* sind die zentralen Rechtsgüter, zu deren Erhaltung die Verfassung den Staat verpflichtet. Sie bilden in einem modernen demokratischen Verfassungsstaat wie der Schweiz gewissermassen einen Grundpfeiler, welcher die ganze Rechts- und Staatsordnung trägt [76].

Dieses Verständnis hat in der neuen Bundesverfassung (BV) [77] mit Art. 35 Abs. 1 („Die Grundrechte müssen in der ganzen Rechtsordnung zur Geltung kommen") seine ausdrückliche Verankerung gefunden. Grundrechte lassen sich heute nicht mehr nur als Abwehrrechte gegenüber dem Staat begreifen; vielmehr verpflichten sie diesen auch, für den tatsächlichen Schutz der in ihnen verbrieften Ansprüche und Freiheiten zu sorgen.

So verpflichten Art. 10 BV (physische und psychische Integrität) oder Art. 8 Abs. 2 BV (Schutz vor Diskriminierung) den Staat auch zum effektiven Schutz vor Beeinträchtigungen, die von Privaten ausgehen. Der verfassungsrechtliche Schutzauftrag ist *ergebnisbezogen*; er besteht unabhängig davon, wo die Rechtsgutverletzung begangen wird und welche (technischen) Mittel dafür verwendet werden. Zur Staatsaufgabe „Grundrechtsschutz" gehören somit die Bekämpfung und Verhinderung von Angriffen auf grundrechtlich geschützte Rechtsgüter insbesondere auch dann, wenn die Angriffe in elektronischen Kommunikationsnetzen erfolgen.

5.12 Die Erfüllung des Schutzauftrages

Im Hinblick auf die Erfüllung des verfassungsrechtlichen Schutzauftrages (vgl. oben Ziff. 5.11) stellen sich dem Gesetzgeber eine Reihe von *Fragen*:

- Mit welchem *Regelungsinstrumentarium* müssen Beeinträchtigungen und Verletzungen der Rechtsgüter bekämpft und verhindert werden? Reichen behördliche Empfehlungen aus, oder braucht es zivil-, straf- und/oder verwaltungsrechtliche Vorschriften?
- *Gegen wen* haben sich staatliche Schutzmassnahmen zu richten? Inwieweit sollen die Hersteller, Eigentümer und Betreiber von technischen Anlagen zur rechtlichen „Verantwortlichkeit" gezogen werden?
    - *Privatrecht*: Soll dem jeder Tätigkeit innewohnenden Schädigungspotenzial mit einer Verschuldens-, Kausal- oder Gefährdungshaftung begegnet werden?

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

- *Strafrecht*: Soll ein Straftatbestand als Vorsatz- oder Fahrlässigkeitsdelikt ausgestaltet werden? Wie weit reicht im letzteren Falle der Umfang der zu beachtenden Sorgfaltspflichten, bzw. wie weit können Schutzmassnahmen zugemutet werden?
- *Verwaltungsrecht*: Sollen sich polizeiliche Massnahmen zum Schutze der grundrechtlich geschützten Rechtsgüter nur an diejenigen richten, die deren Gefährdung oder Störung selbst oder durch das unter ihrer Verantwortung erfolgende Verhalten Dritter verursacht haben („Verhaltensstörer“) [78]? Oder sollen Massnahmen auch diejenigen Personen erfassen, welche über die Sache, die den ordnungswidrigen Zustand bewirkt, rechtliche oder tatsächliche Gewalt haben („Zustandsstörer“) [79]? Wie weit sind auch jene zu erfassen, die durch ihr Tun oder Unterlassen bewirken, dass andere die grundrechtlich geschützten Rechtsgüter gefährden oder beeinträchtigen („Zweckveranlasser“) [80]?

5.2 Verfassungsrechtliche Leitplanken des Rechtsgüterschutzes

Auf den ersten Blick mögen die oben gestellten Fragen (Ziff. 5.12) rein politischer Natur sein, die es mit entsprechenden Argumenten zu lösen gilt. In Wirklichkeit ist der Gesetzgeber in der Ausgestaltung der Massnahmen zur Verhinderung von Rechtsgüterverletzungen nicht frei, sondern seinerseits in mehrfacher Hinsicht *an die Verfassung gebunden:*

5.21 Effizienter Grundrechtsschutz

Die Verfassung (Art. 35 Abs. 1 BV) verpflichtet den Gesetzgeber, für einen *effektiven* und *effizienten* Schutz der Grundrechte zu sorgen[81]. Bei der Wahl des Regelungsinstrumentariums hat sich der Gesetzgeber an dieser Vorgabe zu orientieren.

5.22 Bundesstaatliche Kompetenzordnung

Aus Grundrechten lassen sich keine neuen Bundeskompetenzen ableiten. Der Grundrechtsschutz ist vielmehr nach Massgabe der Sachkompetenzordnung der

---

[78] Vgl. statt vieler BGE 122 II 70; 118 Ib 415. – Als „*Verhaltensstörer*“ könnte im vorliegenden Kontext etwa ein Content-Provider in Frage kommen.
[79] Vgl. statt vieler BGE 122 II 70; 118 Ib 415. – Als „*Zustandsstörer*“ könnte im vorliegenden Fall etwa ein Hosting-Provider in Frage kommen.
[80] Vgl. dazu BGE 99 Ia 511; HÄFELIN/MÜLLER (Bibl.), Rz. 2497 ff.; DANIEL THÜRER, Das Störerprinzip im Polizeirecht, in: ZSR 102 (1983) I 463 ff., 477 f. – Im vorliegenden Fall liesse sich allenfalls ein Access-Provider als „*Zweckveranlasser*“ qualifizieren.
[81] EJPD, Reform der Bundesverfassung, Erläuterungen zum Verfassungsentwurf von 1995, Bern 1995, S. 64; RENÉ RHINOW, Die Bundesverfassung 2000, Eine Einführung, Basel/Genf/München 2000, S. 152; PETER SALADIN, Grundrechte im Wandel, 3. A., Bern 1982, S. 294 ff., *ders*., Die Funktion der Grundrechte in einer revidierten Verfassung, in: Die Kunst der Verfassungsrevision, Schriften zur Verfassungsreform 1968-1996, Basel/Frankfurt a.M. 1998, S. 47 ff., 57 ff.

Bundesverfassung zu verwirklichen (Art. 42 ff. BV)[82]. Bundesrechtliche Massnahmen zum Schutz von grundrechtlich geschützten Rechtsgütern sind somit im vorliegenden Kontext nur dann zulässig, wenn die Bundesverfassung für den Bereich der Telekommunikationsnetzwerke eine entsprechende Bundeskompetenz begründet [83].

5.23 Institutionelle Schicht der Grundrechte

Bei der Ausgestaltung der Schutzvorkehren hat der Gesetzgeber vor allem die institutionelle Schicht der Freiheitsrechte, hier v.a. der *Grundrechte freier Kommunikation* [84], zu beachten.

Dabei ist in erster Linie auf deren fundamentale Rolle in einer demokratisch geprägten Gesellschaft hinzuweisen. Lehre[85] und Rechtsprechung[86] sehen in den Grundrechten freier Kommunikation nicht allein ein unentbehrliches Element menschlicher Entfaltung; darüber hinaus sprechen sie ihnen eine *Grundlagenfunktion für ein demokratisches Gemeinwesen* zu.

Die demokratische Auseinandersetzung soll aber nicht nur vor direkten, sondern auch vor indirekten Eingriffen geschützt werden. Solche indirekten Eingriffe können aus Massnahmen resultieren, welche die freie Kommunikation durch Androhung von Sanktionen für rechtswidrige Äusserungen faktisch hemmen und somit auf Bürgerinnen und Bürger abschreckend wirken (sog. „chilling effect“) [87]. Aus dem gleichen Grund bedürfen daher Eingriffe in Grundrechte der freien Kommunikation einer *genügend präzisen gesetzlichen Grundlage*[88].

5.24 Beachtung grundrechtlich geschützter Positionen

Der Gesetzgeber hat bei der Schaffung von Schutzmassnahmen die grundrechtlich geschützten Positionen der *Adressaten* dieser Massnahmen sowie jene von *Drittpersonen* zu berücksichtigen. Eingriffe in diese Grundrechte bedürfen einer genügenden gesetzlichen Grundlage[89], müssen durch ein öffentliches Interesse oder

---

[82] Statt vieler JEAN-FRANÇOIS AUBERT, Bundesstaatsrecht der Schweiz, Fassung von 1967, Neubearbeiteter Nachtrag bis 1990, Band I, Basel/Frankfurt a.M. 1991, ad N 699; HÄFELIN/HALLER (Bibl.), Rz. 1070.

[83] Vgl. dazu unten Ziff. 7.12.

[84] Art. 16 und 17 BV; vgl. auch Art. 10 EMRK.

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

[86] BGE 96 I 592.

[87] Vgl. dazu grundlegend JÖRG PAUL MÜLLER/MARKUS SCHEFER, Grundrechtliche Fragen zum Internet, Medialex 1997, S. 198 ff., 203: „Eine Verpflichtung von Anbietern (Systembetreiber, Diensteanbieter oder Inhaltsanbieter), nur legale Publikationen zu verbreiten, dürfte u.E. daher aus grundrechtlicher Sicht nur soweit gehen, als dadurch keine substantiellen Einbussen der Auseinandersetzung über Fragen von gesellschaftlichem Interesse am Internet zu befürchten sind.“

[88] Vgl. MÜLLER, GRUNDRECHTE (Bibl.), S. 210 f.

[89] Das Gesetzmässigkeitsprinzip dient darüber hinaus insbesondere auch dem Verfassungsgrundsatz der *Rechtssicherheit* (Art. 5 BV). Letzterer nimmt ebenfalls den Gesetzgeber in die Pflicht, zum Voraus bekannte und allgemein geltende Normen aufzustellen. Vgl. zum Ganzen YVO HANGARTNER,

durch den Schutz von Grundrechten Dritter gerechtfertigt werden können und zudem verhältnismässig sein. Der Kerngehalt des Grundrechts bleibt unantastbar (Art. 36 Abs. 1-4 BV).

5.241 Adressaten

Die *Internet-Provider* als hauptsächliche Adressaten der hier zu diskutierenden Schutzmassnahmen sind zunächst durch das Dachgrundrecht der *Meinungsfreiheit* (Art. 16 Abs. 1 BV) geschützt. Sie können sich hierin insbesondere auf das Grundrecht der *Medienfreiheit* (Art. 17 BV) berufen, in dessen unantastbarem Kern das *Verbot der Vorzensur* liegt (Art. 17 Abs. 2 i.V.m. Art. 36 Abs. 4 BV). Die Medienfreiheit schützt neben dem freien Übermitteln von Informationen über Presse, Radio und Fernsehen auch andere Formen der öffentlichen fernmeldetechnischen Verbreitung, insbesondere das Internet [90].

Provider können sich ausserdem auf die *Wirtschaftsfreiheit* (Art. 27 BV) berufen. Dagegen scheidet eine Berufung auf Art. 27 BV aus, wo Provider Dienste der Grundversorgung[91] sicherstellen und damit eine staatliche Aufgabe im Sinne von Art. 35 Abs. 2 BV erfüllen[92].

5.242 Drittpersonen

Die *Benutzer* des Internets („user“) müssen in ihrer *Informationsfreiheit* (Art. 16 Abs. 1 und 3 BV) geschützt werden. Diese umfasst insbesondere das Recht, Informationen frei zu empfangen. Als „frei empfangbar“ gelten namentlich auch Rundfunksendungen, die drahtlos oder kabelgebunden weiterverbreitet werden[93], sowie über das Internet verbreitete Informationen [94].

5.25 Verhältnismässigkeit

5.251 Im Allgemeinen

Bei der Beantwortung der Frage, wie weit der Gesetzgeber in der Wahrnehmung des Schutzauftrages zur Bekämpfung von Diskriminierungen und Integritätsverletzungen

---

Art. 5 BV, in: Ehrenzeller/Mastronardi/Schweizer/Vallender (Hrsg.), Die schweizerische Bundesverfassung, Kommentar, Zürich/Basel/Genf 2002, N 8; HÄFELIN/MÜLLER, (Bibl.), N 372.

[90] Vgl. zum Ganzen DENIS BARRELET, § 45 Les libertés de la communication, in: Thürer/Aubert/Müller (Hrsg.), Verfassungsrecht der Schweiz/Droit constitutionnel suisse, Zürich 2001, S. 721 ff.. Rz. 40 ff.; ferner auch MÜLLER, GRUNDRECHTE (Bibl.), S. 275. – Im Zusammenhang mit der nicht an die Allgemeinheit gerichteten Kommunikation gesteht das Bundesgericht auch den E-Mail-Providern zumindest die treuhänderische Berufung auf das Grundrecht des *Fernmeldegeheimnisses* (Art. 13 Abs. 1 BV) zu; BGE 126 I 50 ff., 57.

[91] Vgl. Art. 92 Abs. 2 BV, Art. 1 Abs. 2 lit. a FMG sowie Art. 14 ff. FMG.

[92] Vgl. dazu etwa auch GIOVANNI BIAGGINI, § 49 Wirtschaftsfreiheit, in: Thürer/Aubert/Müller (Hrsg.), Verfassungsrecht der Schweiz/Droit constitutionnel suisse, Zürich 2001, S. 779 ff., Rz. 11 mit Hinweisen; ISABELLE HÄNER, Grundrechtsgeltung bei der Wahrnehmung staatlicher Aufgaben durch Private, in: AJP/PJA 2002, S. 1144 ff., 1146, 1150.

[93] Vgl. BGE 120 Ib 64 ff.; MÜLLER, GRUNDRECHTE (Bibl.), S. 292 f.

[94] Vgl. dazu RAIMUND KROPP, Zensur im Internet, in: perspektive 21, Brandenburgische Hefte für Wissenschaft und Politik, Informationsgesellschaft, Heft 3/1998, S. 28 ff., 29.

in die Grundrechte freier Kommunikation eingreifen kann, steht hier der *Grundsatz der Verhältnismässigkeit* (Art. 36 Abs. 3 BV; Art. 5 Abs. 2 BV) im Vordergrund [95]. Verhältnismässig sind nur Massnahmen, die zur Erreichung des Zwecks *geeignet* und zudem *erforderlich* sowie *zumutbar* sind.

5.252 Eignung

Das Verhältnismässigkeitsprinzip verbietet grundrechtsbeschränkende Massnahmen, die keinen Beitrag zur Erreichung des angestrebten Zwecks leisten und somit ungeeignet sind. Der gegen die rechtliche Erfassung von Access-Providern erhobene Einwand, Zugangssperren liessen sich technisch in einfacher Weise umgehen, erhält in dieser Sicht zur politischen Dimension noch eine rechtliche Grundlage. Entsprechendes gilt für Vorschriften, welche die Provider zur Installation von Filterprogrammen verpflichten; denn es lassen sich heute praktisch alle Filter relativ leicht unterlaufen und umgehen [96].

5.253 Erforderlichkeit

Das Verhältnismässigkeitsprinzip verbietet sodann Massnahmen, die in persönlicher, sachlicher, örtlicher und zeitlicher Hinsicht über das zur Erreichung des Regelungszwecks (also des Schutzes der bedrohten Rechtsgüter) Erforderliche hinausgehen.

5.254 Zumutbarkeit

Um verhältnismässig zu sein, müssen Schutzmassnahmen überdies den davon Betroffenen zugemutet werden können. Demnach findet die persönliche „Verantwortlichkeit" [97] für Kriminalität im Cyberspace ihre Grenze in der Zumutbarkeit ihrer rechtlichen Erfassung für die Provider.

Im *Strafrecht* darf die Verantwortlichkeit (ausserhalb von Vorsatzdelikten) nur so weit gezogen werden, als Schutzmassnahmen zumutbar erscheinen, so dass deren Nichteinhaltung geradezu als Verletzung einer Sorgfaltspflicht und damit als Fahrlässigkeit zu qualifizieren ist.

Auch im *Privatrecht* spielt das Kriterium der Zumutbarkeit eine Rolle, wenn es um die Einführung einer einfachen oder strengen Kausalhaftung geht.

Ein Zweckveranlasser gilt auch im *Verwaltungsrecht* nur dann als Störer, wenn ihm der polizeiliche Eingriff zugemutet werden kann, also wenn der Eingriff im Hinblick auf den Schutz des Rechtsgutes verhältnismässig erscheint.

---

[95] Auch der Bundesgesetzgeber bleibt – trotz Art. 191 BV – daran gebunden.
[96] Vgl. dazu SEMKEN (Bibl.), S. 249 ff., 269.
[97] Der Begriff der Verantwortlichkeit wird hier in einem weiten Sinne verstanden und schliesst die Spezialitäten der Verwendung in Straf-, Zivil- und Verwaltungsrecht ein. Von einem solchen Verständnis scheint auch die *E-Commerce-Richtlinie* der Europäischen Union auszugehen, vgl. insbesondere die Überschrift ihres Abschnitts 4 (siehe dazu auch oben Kapitel 4).

5.26 Rechtsgleichheit und Willkürverbot

Ungeachtet des Umfangs der grundrechtlich geschützten Positionen der Internet-Provider bleibt der Gesetzgeber stets an das *Rechtsgleichheitsgebot* (Art. 8 BV) und an das *Willkürverbot* (Art. 9 BV) gebunden.

So kann es verfassungsrechtlich problematisch sein, die Rechtswidrigkeit einer Darstellung im Internet breiter zu fassen als in anderen Publikationen (z.B. im Bereich der Druckerpresse) [98]. Das Rechtsgleichheitsgebot hindert den Gesetzgeber zwar nicht daran, den spezifischen Gefährdungslagen jedes einzelnen Mediums durch differenzierende Vorschriften Rechnung zu tragen, doch braucht es für eine ungleiche Behandlung ausreichende sachliche Gründe. In diesem Sinne können unterschiedliche Regelungen für die verschiedenen Medien mit deren unterschiedlichen Einwirkungsintensität auf das Publikum [99] oder mit deren unterschiedlichem Zielpublikum sowie - damit zusammenhängend - mit der unterschiedlichen Verbreitungsart gerechtfertigt werden[100].

Die Einführung von - im Vergleich zum (benachbarten) Ausland - strengeren Regelungen kann schliesslich zu einer Benachteiligung der inländischen Provider führen, welche aus verfassungsrechtlicher Sicht nicht ganz unproblematisch erscheint.

---

[98] Vgl. MÜLLER, GRUNDRECHTE (Bibl.), S. 246 f.

[99] So erfasst beispielsweise auch das „Brutaloverbot“ von Art. 135 StGB nur Ton- oder Bildaufnahmen, nicht aber das geschriebene Wort.

[100] So behandelt beispielsweise das Pornographieverbot von Art. 197 Ziff. 1 StGB einschlägige Äusserungen an Radio und Fernsehen strenger als pornographische Schriften, Ton- oder Bildaufnahmen, die an Personen über 16 Jahren angeboten werden dürfen.

Das geltende Strafrecht gibt auf die wichtigsten Fragen im Zusammenhang mit der Verfolgung und Ahndung von Straftaten, die mittels Netzwerken verübt werden, keine klare oder keine befriedigende Antwort.

6. Netzwerkkriminalität nach geltendem Strafrecht

6.1 Allgemeines

6.11 Fragestellung

Im Unterschied zu anderen kriminellen Handlungen ist der Täter bei der Netzwerkkriminalität notwendigerweise auf die *technische Infrastruktur* angewiesen, die von einer Mehrzahl von Beteiligten (häufig juristischen Personen), angeboten wird [101]. Ein weiteres zentrales Charakteristikum der von den Hosting-, Network- und Access-Providern erbrachten Dienstleistungen [102] ist das weitgehend *automatisierte Ablaufen* dieser Prozesse.

Wegen der Parallelität [103] zum *Medienstrafrecht* ist zunächst zu klären, ob auch die Sachverhalte der Netzwerkkriminalität unter die Art. 27 und Art. 322bis StGB fallen [104] oder ob sie nach den *allgemeinen Regeln des StGB*, d.h. insbesondere jenen über die Gehilfenschaft (Art. 25 StGB), zu beurteilen sind [105].

Hinzu kommt, dass die strafbare Handlung, die Infrastrukturleistungen der anderen Beteiligten sowie der Abruf der Informationen durch Nutzer an geographisch völlig unterschiedlichen Orten stattfinden können. Netzwerkkriminalität ist daher häufig *grenzüberschreitend* und wirft die Frage auf, wann die Schweiz überhaupt Strafhoheit hat und, falls Schweizer Strafhoheit besteht, auf welche der angesprochenen Verhaltensweisen sich diese allenfalls erstreckt [106].

Eng damit verknüpft sind die Fragen nach den *Ermittlungskompetenzen* (Abgrenzung von Bundesgerichtsbarkeit und kantonaler Gerichtsbarkeit, Art. 340 ff. StGB) und nach dem Gerichtsstand (örtliche Zuständigkeit, Art. 346 ff. StGB).

---

[101] Zu den Beteiligten und ihren Funktionen, s. oben Kapitel 2, Ziff. 3.

[102] D.h. des Bereithaltens und Übermittelns von Informationen in Netzwerken.

[103] Es geht hierbei auch um Veröffentlichung (Bereitstellen), Verbreitung und Konsum (Nutzung) von Informationen. Ausserdem sind eine Vielzahl von Personen an der Veröffentlichung und Verbreitung beteiligt.

[104] Dazu unten Ziff. 6.2.

[105] Dazu unten Ziff. 6.3.

[6] Dazu unten Ziff. 6.4.

6.12 Begriff der Netzwerkkriminalität

Der Begriff der Netzwerkkriminalität umfasst eine grosse Anzahl von Delikten [107], die ganz unterschiedlich definiert und klassifiziert werden können. Die unten stehende *Tabelle* enthält eine Auswahl der wichtigsten und häufigsten *Netzwerkdelikte* (1. Spalte). Sie differenziert nach dem jeweiligen *Deliktstypus*, von welchem abhängt, ob überhaupt von einem Tatort in der Schweiz gesprochen werden kann (2. Spalte). Auf diesem Anknüpfungskriterium beruht in den meisten Fällen die schweizerische Strafhoheit, welche Grundvoraussetzung für jede Strafverfolgung in der Schweiz ist. Schliesslich werden die Straftatbestände danach sortiert, ob sie den *Mediendelikten* zuzuordnen sind und somit unter die Sonderregelungen von Art. 27 und Art. 322bis StGB fallen oder nicht (3. Spalte). Die Einteilung entspricht der aktuellen bundesgerichtlichen Rechtsprechung, soweit eine solche schon besteht, und versucht, ein Bild der gegenwärtigen Rechtslage zu zeichnen. Einige dieser Zuordnungen sind jedoch gerichtlich nicht geklärt und in der Lehre umstritten.

Der Deliktstypus der wichtigsten Netzwerkdelikte und ihr Verhältnis zum Medienstrafrecht [108]

STRAFTATBESTAND	DELIKTSTYPUS	MEDIENDELIKTE [109]
Gewaltdarstellung, Art. 135 StGB	abstraktes Gefährdungsdelikt	kein Mediendelikt
Unbefugte Datenbeschaffung, Art. 143 StGB	Erfolgsdelikt [110] (strittig, a.A.: schlichtes Tätigkeitsdelikt)	kein Mediendelikt
Unbefugtes Eindringen in ein Datenverarbeitungssystem („Hacking"), Art. 143bis StGB	Erfolgsdelikt [111] (strittig, a.A.: schlichtes Tätigkeitsdelikt)	kein Mediendelikt
Datenbeschädigung, Art. 144bis Ziff. 1 StGB (Löschen, Verändern, Unbrauchbarmachen)	Erfolgsdelikt	kein Mediendelikt
Datenbeschädigung, Art. 144bis Ziff. 2 StGB („Computerviren"-Tatbestand)	abstraktes Gefährdungsdelikt (Ziff. 2)	kein Mediendelikt (ausser ev. in der Variante des Anleitung-Gebens)
Betrug, Art. 146 StGB	Erfolgsdelikt	kein Mediendelikt
Computerbetrug, Art. 147 StGB	Erfolgsdelikt	kein Mediendelikt
Kursmanipulation, Art. 161bis StGB	**abstraktes Gefährdungsdelikt**	fraglich, wohl Mediendelikt (in der Variante der Informationsverbreitung)

[107] Vgl. oben Kapitel 2, Ziff. 2.2.

[108] Vgl. SCHWARZENEGGER, E-COMMERCE (Bibl.), S. 342 und 350.

[109] Vgl. BGE 125 IV 206 ff., der sich allerdings explizit nur zur Einteilung der Gewaltdarstellungen (Art. 135 StGB), zur harten Pornographie (Art. 197 Ziff. 3 StGB) und zum Leugnen von Völkermord (Art. 261bis Abs. 4 StGB) äussert. Die anderen Zuordnungen sind daher (noch) nicht höchstgerichtlich geklärt. Eine Klassifizierung i.S. des bundesgerichtlichen Standpunktes findet sich in TRECHSEL/NOLL, (Bibl.), S. 229 m.N.; GUTACHTEN BJ (Bibl.), S. 834 f.

[110] SCHWARZENEGGER, GELTUNGSBEREICH (Bibl.), S. 122, ein räumlich und zeitlich abtrennbarer Aussenerfolg ist nachweisbar; a.M. NIKLAUS SCHMID, Computer- sowie Check- und Kreditkarten-Kriminalität, Zürich 1994, StGB 143 N 17 und StGB 143bis N 11; CASSANI, (Bibl.), S. 253.

[111] Siehe vorstehende Fussnote.

Ehrverletzungen, Art. 173 ff. StGB	Erfolgsdelikte	Mediendelikte
Weiche Pornographie, Art. 197 Ziff. 1 StGB (Jugendschutz)	abstraktes Gefährdungsdelikt	fraglich, wohl kein Mediendelikt
Weiche Pornographie, Art. 197 Ziff. 2 StGB (Schutz von Erwachsenen vor ungewollter Konfrontation mit Pornographie)	konkretes Gefährdungsdelikt	kein Mediendelikt
Harte Pornographie, Art. 197 Ziff. 3 StGB	abstraktes Gefährdungsdelikt	kein Mediendelikt
Herstellen, Verbergen, Weiterschaffen von Sprengstoffen und giftigen Gasen, Art. 226 Abs. 3 StGB (Anleitung-Geben zur Herstellung)	abstraktes Gefährdungsdelikt	fraglich, wohl kein Mediendelikt, weil sich das Delikt nicht in einer Publikation erschöpft (Anleitung an bestimmte Person erforderlich)
Schreckung der Bevölkerung, Art. 258 StGB	Erfolgsdelikt	kein Mediendelikt
Aufforderung zu Verbrechen oder Gewalt, Art. 259 StGB	abstraktes Gefährdungsdelikt	Mediendelikt
Rassendiskriminierung, Art. 261bis StGB	schlichtes Tätigkeitsdelikt	kein Mediendelikt (Abs. 4, Leugnung des Völkermordes), ebenso wohl Abs. 1-3
Wirtschaftlicher Nachrichtendienst, Art. 273 StGB	abstraktes Gefährdungsdelikt	fraglich, wohl Mediendelikt
Aufforderung und Verleitung zur Verletzung militärischer Dienstpflichten, Art. 276 StGB	abstraktes Gefährdungsdelikt	Mediendelikt
Veröffentlichung amtlicher geheimer Verhandlungen, Art. 293 StGB	abstraktes Gefährdungsdelikt	Mediendelikt
Verletzung des Amtsgeheimnisses, Art. 320 StGB	schlichtes Tätigkeitsdelikt	Mediendelikt
Verletzung des Berufsgeheimnisses, Art. 321 StGB	schlichtes Tätigkeitsdelikt	Mediendelikt
Urheberrechtsverletzung Werkexemplar herstellen, Art. 67 Abs. 1 lit. e URG	schlichtes Tätigkeitsdelikt	kein Mediendelikt
Werkexemplare anbieten, veräussern oder verbreiten, Art. 67 Abs. 1 lit. f URG	schlichtes Tätigkeitsdelikt	kein Mediendelikt (ausser ev. in der Variante des Anbietens)
Verletzung verwandter Schutzrechte insbes. Art. 69 Abs. 1 lit. c, lit. f URG	schlichtes Tätigkeitsdelikt	kein Mediendelikt
Unlautere Werbe- und Verkaufsmethoden insbes. Art. 3 i.V.m. Art. 23 UWG	abstraktes Gefährdungsdelikt	Mediendelikt

6.2 Strafbarkeit nach dem Medienstrafrecht?

6.21 Die neuen Bestimmungen zum Medienstrafrecht

Mediendelikte sind dadurch charakterisiert, dass die strafbare Handlung durch eine *Veröffentlichung in einem Medium* begangen wird und sich zugleich in dieser Veröffentlichung *erschöpfen* muss. Gemäss Art. 27 und Art. 322bis StGB gelten bei

diesen Delikten spezielle Regeln für die Teilnahme am Veröffentlichungsprozess [112]. Grundsätzlich macht sich bloss der Autor der illegalen Veröffentlichung strafbar (Art. 27 Abs. 1 StGB). Kann dieser aber nicht ermittelt oder in der Schweiz nicht vor Gericht gestellt werden (Art. 27 Abs. 2 StGB), ergibt sich aus Art. 322bis StGB eine subsidiäre, exklusive Strafbarkeit des verantwortlichen Redaktors oder, wo ein solcher fehlt, der für die Veröffentlichung verantwortlichen Person.

In dieser seit 1. April 1998 in Kraft stehenden Strafbestimmung wird das *vorsätzliche* Nichtverhindern einer inkriminierten Veröffentlichung mit Gefängnis oder Busse bedroht. Die Strafbarkeit ist aber gegenüber dem früheren Pressestrafrecht insofern verschärft worden, als auch die *fahrlässige* Nichtverhinderung mit erfasst wird. Nachdem Art. 27 StGB keine Aufzählung der Mediendelikte enthält, muss der Katalog der von dieser Sonderregelung erfassten Straftatbestände durch Auslegung aus diesen selbst ermittelt werden (vgl. obige Tabelle, 3. Spalte, im einzelnen bestehen noch Unklarheiten).

6.22 Neuer Bundesgerichtsentscheid zum Begriff des Mediendelikts

Komplizierend tritt hinzu, dass nach einem 1999 ergangenen Bundesgerichtsentscheid nicht alles, was sich medial veröffentlichen lässt und sich in der Veröffentlichung erschöpft, auch immer ein Mediendelikt ist [113]. Das Bundesgericht erwähnt in seiner Entscheidung explizit die Gewaltdarstellungen (Art. 135 StGB), harte Pornographie (Art. 197 Ziff. 3 StGB) und das Leugnen von Völkermord (insbesondere durch die „Auschwitzlüge“, Art. 261bis Abs. 4 StGB), die nicht zu den Mediendelikten zu zählen seien.

Begründet wird dies einerseits damit, dass der Gesetzgeber bei den Nicht-Mediendelikten gerade die Veröffentlichung der inkriminierten Inhalte *verhindern* und deshalb kaum einer bestimmten Gruppe von Tatbeteiligten eine privilegierte Stellung einräumen wollte. Andererseits seien bei den Nicht-Mediendelikten eine ganze Reihe anderer Tathandlungen mit Strafe bedroht, so dass die Privilegierung der medialen Art des Verbreitens vom Gesetzgeber in diesen Fällen nicht beabsichtigt gewesen sein könne. Zudem sei die Schweiz im Hinblick auf die Rassendiskriminierung durch die Ratifizierung des Internationalen Übereinkommens gegen die Rassendiskriminierung *völkerrechtlich verpflichtet*, jede Verbreitung rassistischer Äusserungen ohne Ausnahme zu verfolgen [114].

Im Kern geht es hierbei um die Frage, ob die *Privilegierung* der Medienverantwortlichen nicht einer Verletzung des *Gleichbehandlungsgebotes* (Art. 8 Abs. 1 BV) gleichkomme und damit verfassungswidrig sei. Dem ist entgegenzuhalten, dass schon die Einführung der pressestrafrechtlichen Regeln vom Gedanken geprägt war, dass das gemeine Strafrecht den Bedürfnissen einer freien Presse nicht ausreichend Rechnung trage und dass ihre Förderung daher nur durch eine Einschränkung der Strafbarkeit der am Presseerzeugnis Beteiligten möglich sei

---

[112] Zur Entstehungsgeschichte und zum Sinn der medienstrafrechtlichen Sonderregelung, s. RIKLIN, (Bibl.), S. 243 ff.; ZELLER (Bibl.) N 3 und 10 ff.

[113] BGE 125 IV 211 f., so schon SCHULTZ, PRESSEDELIKT (Bibl.), S. 278 und TRECHSEL/NOLL (Bibl.), S. 229. Vgl. GUTACHTEN BJ (Bibl.), S. 832 ff.

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

[115]. Der ungehinderte Fluss von Informationen und der freie Austausch von Meinungen ist nicht nur ein unentbehrliches Element *menschlicher Entfaltung*, sondern darüber hinaus Grundlage jedes demokratischen Staatswesens. Da sich der Schweizer Gesetzgeber bei der Neuregelung des Medienstrafrechts für eine Fortsetzung der Privilegierung entschieden hat und dabei insbesondere den *Schutz der Medienfreiheit* (vgl. Art. 17 BV) im Auge hatte, ist davon auszugehen, dass *alle medialen Veröffentlichungen nach Art. 27 und Art. 322bis StGB beurteilt werden* sollten, falls sie sich in der Veröffentlichung erschöpfen.

Deshalb ist die Kategorisierung der Mediendelikte gemäss den Kriterien von BGE 125 IV 206 ff. *fragwürdig* (siehe obige Tabelle, 3. Spalte). Dieser Entscheidung ist denn auch zahlreiche *Kritik* erwachsen [116]. Mit den bundesgerichtlichen Argumenten lassen sich letztlich alle Äusserungs- und Verbreitungsdelikte aus dem Anwendungsbereich des Medienstrafrechts ausschliessen, sind doch die einzelnen Strafnormen immer darauf ausgerichtet, unzulässige Aussagen in allen Verbreitungsvarianten - im medialen und nicht-medialen Kontext - zu unterbinden. Dies würde beispielsweise auch für die *Ehrverletzungsdelikte* gelten, bei denen verschiedenste Tathandlungs-Modalitäten erfasst sind (Wort, Schrift, Bild, Gebärde oder andere Mittel, vgl. Art. 176 StGB).

6.23 Drei Auslegungsansätze

6.231 Provider sind für die Veröffentlichung verantwortlich — Anwendbarkeit des Medienstrafrechts

Ein erster Auslegungsansatz zu Art. 27 StGB [117] versteht den Internetdienst des World Wide Web als Medium der Massenkommunikation, weshalb Art. 27 und Art. 322bis StGB prinzipiell auf Veröffentlichungen im WWW Anwendung finden. Strafbar ist demzufolge einzig der *Content-Provider*, wenn er ermittelt oder in der Schweiz vor Gericht gestellt werden kann.

Bei Fehlen eines belangbaren Content-Providers besteht für den Hosting-Provider eine subsidiäre Verantwortlichkeit unter den Voraussetzungen von Art. 27 Abs. 2 StGB. Er ermöglicht es dem Autor bzw. Content-Provider erst, mit seinen Inhalten auf das Internet zu gelangen, und tritt daher nach dieser Auffassung als für die Veröffentlichung Verantwortlicher in Erscheinung. Seine Strafbarkeit bemisst sich – soweit überhaupt ein Mediendelikt vorliegt – nach Art. 322bis StGB.

Weiter gilt nach dieser Auslegung auch der *Access-Provider* als subsidiärer Medienverantwortlicher i.S.v. Art. 27 Abs. 2 StGB, falls weder der Content- noch der

---

[115] Sten Bull SR 1931, S. 68 und 76; weiterführend ZELLER (Bibl.), N 10 ff.

[116] FRANZ RIKLIN, Kaskadenhaftung – quo vadis?, Medialex 2000, 208; RIKLIN/ STRATENWERTH, (Bibl.), S. 13 ff.; DORRIT SCHLEIMINGER/CHRISTOPH METTLER, Strafbarkeit der Medienverantwortlichen im Falle der Rassendiskriminierung, Art. 27, Art. 261bis Abs. 4 StGB, Bemerkungen zu BGE 125 IV 206 ff., AJP 2000, S.1039 ff.; REHBERG/ DONATSCH (Bibl.), S. 166; SCHWARZENEGGER, E-COMMERCE (Bibl.), S. 349 ff.; RIKLIN (Bibl.), S. 245; ZELLER (Bibl.), N 32.

[117] Botschaft über die Änderung des schweizerischen Strafgesetzbuches und des Militärstrafgesetzes (Medienstraf- und Verfahrensrecht), BBl 1996 IV 527 und 549; GUTACHTEN BJ (Bibl.), S. 832 ff. m.N.

Hosting-Provider gefasst oder vor Gericht gestellt werden kann. Die Strafbarkeit des Access-Providers ergibt sich dann ebenfalls aus Art. 322bis StGB [118].

6.232 Provider sind für die Veröffentlichung nicht verantwortlich — Anwendbarkeit der allgemeinen Regeln

Ein *zweiter Auslegungsansatz* kritisiert diese Ansicht, weil sie den Unterschied zwischen der Medienfunktion des WWW, die sich im elektronischen Veröffentlichungsprozess erschöpft (Bereitstellen), und der Telekommunikationsfunktion des WWW, die alle technischen Aspekte der Datenspeicherung und -übertragung umfasst (Bereithalten, Übermittlung), vernachlässigt [119]. Nur bei Medienunternehmen, die ihre Inhalte parallel im Offline- und Online-Bereich auf einem eigenen Webserver publizieren (Bereitstellen = Veröffentlichung), trifft diese Ansicht zu [120].

Im Normalfall ist aber der *Hosting-Provider* weder aktiv am Veröffentlichungsprozess des Content-Providers beteiligt, noch überwacht er passiv die entsprechenden Informationsübertragungen. Die Daten werden vom Content-Provider per Webpublishing-Software direkt und automatisiert auf dem Web-Server des Hosting-Providers abgelegt. Der Hosting-Provider betreibt mit anderen Worten *einzig die technische Infrastruktur* zum Bereithalten der Informationen und ist deshalb – von der erwähnten Ausnahme abgesehen – keine für die Veröffentlichung verantwortliche Person [121]. In dieser Funktion fällt er überhaupt nicht in den Regelungsbereich des Medienstrafrechts, wobei nach dieser Auffassung dann allerdings eine Strafbarkeit nach den allgemeinen Voraussetzungen der Gehilfenschaft in Betracht zu ziehen ist (vgl. hierzu unten Ziff.6.3) [122].

Der *Access-Provider* wirkt ebenfalls nicht an der Veröffentlichung von verbotenen Inhalten auf fremden Servern mit. Seine Dienstleistung beschränkt sich auf das Zurverfügungstellen eines Zugangs zum Internet. Die vom Nutzer veranlasste Datenübertragung läuft automatisiert und unüberwacht ab. Da es sich hierbei um eine Art „Gehilfenschaft“ zugunsten des Nutzers handelt, der die Informationen auf dem Internet sucht und abruft, gehört der Access-Provider keinesfalls in den Regelungsbereich von Art. 27 Abs. 2 und Art. 322bis StGB [123].

---

[118] GUTACHTEN BJ (Bibl.), S. 841 ff.

[119] Verdeutlicht durch NIGGLI/SCHWARZENEGGER (Bibl.), S. 65 f.

[120] Beispiel: Eine Tageszeitung publiziert einen Artikel sowohl in der gedruckten Morgenausgabe als auch auf der selbständig betriebenen Website. Eine direkte Beteiligung am Publikationsprozess ist ebenfalls gegeben, wenn der Hosting-Provider die Informationen auf einem Datenträger entgegennimmt, um sie danach für den Content-Provider auf seinem Web-Server zu publizieren.

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

[122] Eine Ausdehnung des Medienstrafrechts auf den Kreis der technischen Verbreiter des Medieninhaltes wird nach dieser Ansicht abgelehnt. Siehe RIKLIN/STRATENWERTH (Bibl.), S. 19 f.; SCHWARZENEGGER, E-COMMERCE (Bibl.), S. 351; NIGGLI/SCHWARZENEGGER (Bibl.), S. 62; RIKLIN (Bibl.), S. 251. Vgl. die entsprechende explizite Regelung in den USA, Section 230(c) (2) Communications Decency Act: „No provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider.“

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

6.233 Provider sind für die Veröffentlichung nicht verantwortlich — Anwendbarkeit des Medienstrafrechts

Ein *dritter Auslegungsansatz* stimmt mit der vorgenannten Ansicht darin überein, dass Hosting- und Access-Provider keine für die Veröffentlichung verantwortliche Personen i.S.v. Art. 27 Abs. 2 StGB sind. Weil sich aber der Kreis der nach Art. 27 Abs. 2 StGB subsidiär Verantwortlichen nicht mit dem Kreis der von einer Bestrafung ausgenommenen Personen deckt, schliesst er nicht aus, dass Hosting-Provider und Access-Provider gleichwohl unter die Sonderregelung von Art. 27 StGB fallen. Die Verbreiter, welche in der gesetzlichen Aufzählung der subsidiär Verantwortlichen fehlen, können nach dieser Ansicht unabhängig von ihrem Tatbeitrag von jeglicher strafrechtlichen Verantwortung ausgeklammert sein [124].

In diesem Sinne entschied das *Bundesgericht* kürzlich im Kontext eines pressestrafrechtlichen Sachverhaltes (Anbringen ehrverletzender Plakate, BGE 128 IV 53). Darin wird die strafrechtliche Verantwortlichkeit von Personen verneint, die im Rahmen der Herstellung und Verbreitung eines strafrechtlich relevanten Medienerzeugnisses ausschliesslich dessen Veröffentlichung übernehmen. Gemäss dieser Entscheidung kommt eine Bestrafung des Verbreiters rechtswidriger Äusserungen bloss dann in Betracht, wenn er nicht medienspezifisch tätig ist, wenn er also ausserhalb der vorgesehenen Produktions- und Verbreitungskette mitwirkt (BGE 128 IV 68).

Wird dieser Auslegungsansatz auch auf die Publikation und Verbreitung im Internet angewendet, gehören sowohl der Hosting- als auch der Access-Provider zu den Verbreitern, die *straflos bleiben* müssten [125]. Stossende Resultate, die sich aus dieser weitgehenden Privilegierung ergeben können [126], müssen dann durch eine Begrenzung des Anwendungsbereichs des Medienstrafrechts verhindert werden [127].

6.24 Art. 27 StGB passt nicht auf das Internet

Der Anwendungsbereich des Medienstrafrechts ist infolge der in diesem Abschnitt aufgezeigten Auslegungsunterschiede *unklar*, und zwar sowohl im Hinblick auf die Zuordnung zur Gruppe der Mediendelikte („Strafbare Handlung, die sich in der Veröffentlichung erschöpft“, vgl. Tabelle oben in Ziff. 6.12, 3. Spalte) als auch bezüglich seiner Anwendbarkeit auf Hosting- und Access-Provider.

Abgesehen von den unterschiedlichen Auslegungsansätzen ist augenfällig, dass Art. 27 StGB auf das Zusammenwirken von Autoren, Redaktoren und anderen für die Publikation Verantwortlichen gemünzt ist und kaum auf die Verhältnisse im WWW, in Newsgroups, Mailinglisten usw. passt. Der Informationsanbieter publiziert in diesen Internet-Diensten meistens selbständig und automatisiert, *ohne Zwischenschaltung einer Redaktion,* einer Kontrollinstanz, eines Druckers usw. Die Stellung des Hosting-

---

[124] ZELLER (Bibl.), N 32. Vgl. hierzu RIKLIN (Bibl.), S. 250 f.

[125] Vgl. ZELLER (Bibl.), N 35 ff. und 56 f. (offen gelassen).

[126] Zu denken ist an sensible Bereiche wie die Pornographie (Art. 197 StGB), Aufforderung zu Verbrechen oder Gewalt (Art. 259 StGB) oder Rassendiskriminierung (Art. 261bis StGB).

[127] Diesen Weg hat das Bundesgericht in BGE 125 IV 206 ff. bereits eingeschlagen.

oder Access-Providers lässt sich daher kaum mit jener der Akteure in den klassischen Massenmedien der Presse und des Rundfunks vergleichen.

Eine Neuregelung der Strafbarkeit der verschiedenen Beteiligten muss daher eine *explizite Trennung zwischen der Medien- und der Telekommunikationsfunktio*n des WWW und anderer Netzwerkdienste anstreben (vgl. dazu oben Kapitel 2).

6.3 Strafbarkeit nach den allgemeinen Regeln des StGB?

Wendet man bei Nicht-Mediendelikten (siehe Tabelle oben in Ziff. 6.12, 3. Spalte) die allgemeinen Zurechnungsregeln von Täterschaft und Teilnahme an, so stellen sich für den Hosting- und Access-Provider eine ganze Reihe weiterer Fragen, deren Lösung ungewiss ist [128]. Klar ist nur, dass für den Inhalt einer ins Netz gestellten Website derjenige als Täter verantwortlich ist, auf den sie nach Existenz und Inhalt zurückgeht (Content-Provider). Bereits beim Hosting-Provider, der einem Dritten (gegen Entgelt) Speicherplatz zur Verfügung stellt, den dieser nach eigenem Gutdünken nutzen kann, ist umstritten, wie er an einer durch diesen Dritten im World Wide Web begangenen Straftat mitwirkt; Entsprechendes gilt erst recht für den Access-Provider. Das hat *verschiedene Gründe:*

Ob der Hosting-Provider *Täter oder nur Gehilfe* der fraglichen Tat ist, hängt von der Beschreibung der Tathandlung in der jeweiligen Strafnorm ab. *Täter* ist derjenige, von dem man sagen muss, er habe die Tathandlung (in eigener Person) ausgeführt, wogegen der *Gehilfe* gerade dies nicht tut. Aber die Grenze zwischen diesen beiden Rollen ist just bei den hier interessierenden Tatbeständen über weite Strecken verwischt, weil sie Handlungsweisen als tatbestandsmässig verbieten, die weit im *Vorfeld der eigentlichen Rechtsgutsverletzung* liegen. So genügt nach Art. 197 Ziff. 1 StGB das blosse Zugänglichmachen von pornographischen Schriften an Personen unter 16 Jahren (ebenso Art. 197 Ziff. 3 StGB „harte Pornographie“, Art. 135 StGB „Gewaltdarstellungen“), was den Hosting-Provider zum Täter machen würde.

Typisch für den Hosting-Provider ist jedoch, dass es zum Zeitpunkt, in dem er den Vertrag betreffend Überlassung von Speicherplatz mit dem jeweiligen Nutzer (Content-Provider) schliesst, ungewiss ist, welche Art von Informationen dieser ins Netz stellen will und wird. Die Handlung, mittels deren der Hosting-Provider „zugänglich macht“, ist ein *Blanko-Akt*; er bezieht sich auf die künftigen Informationen des Content-Providers, nicht aber auf pornographisches, rassendiskriminierendes oder ähnliches Material. Er macht z.B. nicht pornographische Bildaufnahmen (Art. 197 Ziff. 1 StGB) zugänglich, sondern zunächst nur eine – vorerst noch – leere Website. Diese wird erst durch das Handeln desjenigen pornographisch, der sie entsprechend füllt. Demnach würde der Hosting-Provider den objektiven Tatbestand nicht erfüllen.

Entsprechend lässt sich auf der *subjektiven Seite des Tatbestandes* argumentieren: Der Hosting-Provider kann keine Kenntnis davon haben, welche Informationen der Content-Provider ins Netz stellen will und wird. Zwar weiss er aus Erfahrung, dass sich im WWW auch illegale Informationen finden; aber dieses allgemeine Wissen

[128] Bei Ausklammerung der technischen Verbreiter vom Medienstrafrecht gilt dies ganz allgemein für Hosting- und Access-Provider (s. oben Ziff. 6.2).

vermag noch keinen Vorsatz bezüglich Straftaten zu begründen, deren Begehung und erst recht deren nähere Beschaffenheit völlig ungewiss ist. Also fehlt es im Moment der Vornahme der „Tathandlung“ des Hosting-Providers [129] am Vorsatz; somit würde auch aus diesem Grund seine Strafbarkeit für aktives Tun entfallen.

Erst im Zeitraum *nach* Vertragsschluss kann bei ihm ein allfälliges Wissen über rechtswidrige Informationen auf seinem Server entstehen. Regelmässig geschieht dies durch *Hinweise von Nutzern* des WWW, die den Hosting-Provider eventuell sogar auffordern, eine Webseite wegen der behaupteten (Straf-)Rechtswidrigkeit der darauf enthaltenen Informationen zu sperren oder zu entfernen. Geht der Hosting-Provider dem Hinweis nach, kann er so das für eine Straftat – wie z.B. Art. 135 oder Art. 197 StGB – nötige Wissen erlangen. Zweifelhaft ist in diesem Fall aber, ob er sich durch aktives Tun oder allenfalls Unterlassen strafbar machen würde.

Aus der *bundesgerichtlichen Praxis* lassen sich keine zuverlässigen Schlüsse ziehen; insbesondere können die im „*Telekiosk-Entscheid*“ [130] getroffenen Feststellungen nicht unbesehen auf den Fall des Hosting-Providers übertragen werden [131]. Dort hatte das Bundesgericht ein Tun des damaligen Generaldirektors der Abteilung Telekommunikation der ehemaligen PTT darin erblickt, dass dieser die Einführung des Systems „Telekiosk 156“ angeordnet hatte und die notwendigen Installationen auf seine Anweisung hin vorgenommen wurden. Das Zur-Verfügung-Stellen dieser Installationen wurde als aktives Tun gewertet [132] und der Generaldirektor wegen Gehilfenschaft zur unzüchtigen Veröffentlichung und zur Pornographie (Art. 204 aStGB und Art. 197 Ziff. 1 StGB) verurteilt.

Bei Tathandlungen wie dem „Überlassen“ oder insbesondere dem „Zugänglich-machen“ ist die im Strafrecht zentrale *Unterscheidung von Tun und Unterlassen* unsicher. Die bundesgerichtliche Praxis behandelt als Tun auch das Weiterwirkenlassen von Folgen einer früher zulässigerweise vorgenommenen Handlung, wenn diese eine vorsätzlich-rechtswidrige Dritthandlung unterstützt. Das ist äusserst zweifelhaft [133]. Denn wenn der Hosting-Provider einen Hinweis auf eine strafrechtlich relevante Webpage einfach ignoriert, ist schwer zu sehen, worin mit Bezug auf die fragliche Webpage ein Handeln zu erblicken wäre, selbst wenn der Hinweis zutrifft und der Hosting-Provider sich selber davon überzeugt hat. Vorzuwerfen ist ihm dann das Unterlassen des Einschreitens. Solches wäre nur dann strafbar, wenn ihn eine besondere Rechtspflicht zum Handeln treffen würde (sog. Garantenstellung) [134].

---

[129] Diese besteht im Abschliessen des Hosting-Vertrages, das in der Regel automatisiert mit dem Ausfüllen eines Online-Formulars erfolgt.

[130] BGE 121 IV 109 (sog. Telekiosk-Fall).

[131] Ausführlich RIKLIN/STRATENWERTH, (Bibl.), S. 23 f.

[132] BGE 121 IV 109, 120 E. 3b.

[133] Zudem: Im Fall Telekiosk war *ein* Anbieter dieser Dienstleistung betroffen (weil es nur einen gab), bei den Hosting-Providern betrifft die Frage ca. 100 Unternehmen.

[134] Die Lehre geht von einem Unterlassen aus, s. FRANZ RIKLIN: Information Highway und Strafrecht, in: Reto M. Hilty (Hrsg.): Information Highway. Beiträge zu rechtlichen und tatsächlichen Fragen, Bern/München 1996, 578; Diese Frage wurde im deutschen Recht vor Inkrafttreten des Teledienstegesetzes (TDG) ausführlich diskutiert, s. Ulrich SIEBER: Strafrechtliche Verantwortlichkeit für den Datenverkehr in internationalen Computernetzen, Teil 2, JZ 1996, 494 ff.

Eine *Garantenstellung* kann nach anerkannter Rechtsprechung und Lehre aus einem vorausgehenden gefährdenden Tun entstehen (sog. Ingerenz). Wer in voraussehbarer Weise durch sein Handeln für Rechtsgüter Dritter eine Gefahr schafft, ist verpflichtet, alles zu unternehmen, damit sich diese Gefahr nicht verwirklicht. Das Tun des Hosting-Providers besteht darin, dass er Interessierten Speicherplatz zur Verfügung stellt. Das aber ist eine völlig alltägliche und für sich *legale Handlung*, die keine besondere Gefahr schafft [135].

Die Gefahr bzw. die strafbare Handlung resultiert erst aus der missbräuchlichen Verwendung dieses Speicherplatzes durch einen Dritten (Content-Provider), der vorsätzlich und rechtswidrig mittels der ins Netz gestellten Informationen eine Straftat begeht [136]. Man kann die Situation vergleichen mit der Frage, ob ein Wirt verpflichtet ist, seine Gäste, denen er Spielkarten geliehen hat, vom verbotenen Glücksspiel abzuhalten, oder ob der Eigentümer eines Hauses dafür zu sorgen hat, dass dessen Bewohner darin keine Straftaten verüben. Die erste Frage hat das Bundesgericht bejaht [137], die zweite verneint [138]. Auch in diesem Punkt herrscht also *wenig Klarheit* [139].

Die für den Hosting-Provider getroffenen Feststellungen gelten sinngemäss auch für den *Access-Provider*. Der Unterschied liegt nur darin, dass dieser noch weiter weg vom (Haupt-)Täter anzusiedeln ist. Er hat mit ihm überhaupt keine – also auch keine automatisierten – vertraglichen Beziehungen, sondern ist nur mit dem Endnutzer vertraglich verbunden.

6.4 Das Problem der Strafhoheit

Die Frage, welcher Staat Strafgewalt über grenzüberschreitende Netzwerkdelikte hat, ist eine der am stärksten umstrittenen auf dem Gebiet des Internetstrafrechts [140]. Das Strafanwendungsrecht (Art. 3 ff. StGB) bestimmt autonom und ohne Rücksicht auf Überschneidungen mit den Hoheitsansprüchen anderer Staaten, wo das schweizerische Strafrecht anwendbar sein und wer unter die schweizerische Strafhoheit fallen soll. Ist letztere begründet, hat das Gericht schweizerisches Strafrecht anzuwenden [141].

---

[135] Diese Erscheinung wird unter dem Stichwort der „harmlosen Gehilfenschaft“ kontrovers diskutiert, vgl. etwa GRACE SCHILD TRAPPE: Harmlose Gehilfenschaft, Bern 1995; WOLFGANG WOHLERS: Gehilfenschaft durch „neutrale“ Handlungen, ZStrR 1999, 425 ff.; MARC FORSTER: Der Wirtschaftsalltag als strafrechtsdogmatischer „Hort des Verbrechens“, Festschrift Niklaus Schmid, Zürich 2001, 127 ff.

[136] Und dabei auch den mit dem Hosting-Provider geschlossenen Vertrag verletzt, weil dieser das Angebot strafrechtlich relevanter Informationen verbietet.

[137] BGE 81 IV 201.

[138] BGE 79 IV 147.

[139] Zusammenfassend zur deutschen Diskussion, MARTIN POPP: Die strafrechtliche Verantwortung von Internet-Providern, Berlin 2002, 121 ff., der von einer Garantenstellung aus tatsächlicher Herrschaft über eine gefährliche Sache (Überwachungsgarantenstellung) ausgeht und eine Unterlassungsstrafbarkeit grundsätzlich bejaht. Diese ist jedoch durch die explizite Regelung in § 11 TDG eingeschränkt.

[140] Überblick bei SCHWARZENEGGER, GELTUNGSBEREICH (Bibl.), S. 109 ff.

[141] Ausnahmen: Die Artikel 5 Abs. 1, 6 Ziff. 1, 6bis Ziff. 1 StGB verpflichten den Schweizer Richter, das ausländische Strafrecht anzuwenden, falls es milder ist.

Grenzen erwachsen dieser nationalstaatlichen Definitionsmacht allenfalls aus dem *Völkerrecht*, doch geht auch dieses sehr weit in der Anerkennung von „sinnvollen“ Anknüpfungspunkten [142]. Folglich kann es im Strafrecht zu mehrfacher Strafverfolgung und Sanktionierung bezüglich der gleichen Straftat kommen. Diese Gefahr besteht insbesondere bei Netzwerkdelikten, die durch die Verbreitung von strafbaren Inhalten auf dem WWW einen weltweiten Wirkungskreis haben.

Das schweizerische Strafanwendungsrecht kennt eine Vielzahl von *Anknüpfungsregeln*. Ausser nach dem *Territorialitätsprinzip* [143], das den Regelfall darstellt, können grenzüberschreitende Straftaten auch nach dem Flaggenprinzip [144], dem Staatsschutzprinzip [145], dem aktiven [146] und passiven [147] Personalitätsprinzip sowie nach dem Weltrechtsprinzip [148] der schweizerischen Strafgewalt unterstehen [149].

Die Anknüpfung nach dem Territorialprinzip wird durch das beschränkte *Ubiquitätsprinzip* [150] konkretisiert: die Straftat gilt dann als in der Schweiz begangen, wenn entweder der Ort der Ausführung oder der Ort des Erfolgseintritts im Inland liegt. Folglich können auch im Ausland ausgeführte, aber inländische Rechtsgüter verletzende bzw. gefährdende [151] Straftaten zu den Inlandtaten gezählt werden.

6.41 Ort der Ausführung bei Netzwerkdelikten

Massgebend für die Bestimmung des Ausführungsortes ist immer der *physische Aufenthaltsort des Täters* im Moment der Tathandlung. Verbietet das Strafgesetz beispielsweise das Anpreisen, Anbieten, Zeigen, Auffordern, Verbreiten oder Zugänglichmachen bestimmter Informationen [152], ist der Ausführungsort dort, wo der Täter den Übermittlungs- oder Abspeicherungsbefehl betätigt, mit dem die Datenverarbeitung durch automatisierte Programmabläufe in Gang gesetzt wird.

---

[142] COUNCIL OF EUROPE, European Committee on Crime Problems: Extraterritorial criminal jurisdiction, Criminal Law Forum 1992, S. 441 ff. Dazu auch Cour Permanente de Justice Internationale [CPJI], Recueil des Arrêts, Sér. A, No. 10, 1927 („Lotus“-Entscheidung).

[143] In der Schweiz verübte Taten, Art. 3 Ziff. 1 Abs. 1 StGB

[144] Auf einem unter Schweizer Recht stehenden Luftfahrzeug oder Schiff verübte Taten, Art. 97 Luftfahrtgesetz vom 21. Dezember 1948 (LFG, SR 748.0), Art. 4 Abs. 2-3 des Bundesgesetzes über die Seeschiffahrt unter Schweizer Flagge vom 23.9.1953 (SR 747.30).

[145] Gegen die Existenz bzw. staatliche Rechtsgüter der Schweiz gerichtete Taten, Art. 4 Abs. 1 StGB, mit Deliktskatalog.

[146] Von Schweizer Staatsangehörigen verübte Taten, Art. 6 Ziff. 1 StGB.

[147] Gegen strafrechtlich geschützte Rechtsgüter Schweizer Staatsangehöriger gerichtete Taten, Art. 5 Abs. 1 StGB.

[148] Jede gegen universelle Rechtsgüter gerichtete Tat, vgl. Art. 6bis StGB, Art. 19 Ziff. 4 Betäubungsmittelgesetz vom 3. Oktober 1951 (BetmG, SR 812.121).

[149] Die Art. 3–7 StGB gelten nach Massgabe von Art. 333 Abs. 1 StGB (Vorbehalt abweichender Regelungen) auch für das Nebenstrafrecht.

[150] Art. 7 StGB.

[151] Eigentlich werden nicht Rechtsgüter gefährdet oder verletzt, sondern die Handlungs- oder Angriffsobjekte, in denen die Rechtsgüter jeweils konkret verkörpert sind.

[152] Vgl. Art. 135 StGB (Gewaltdarstellungen), Art. 173 Ziff. 1 und Art. 174 Ziff. 1 StGB (Ehrverletzungen), Art. 179 Abs. 2 StGB (Verletzung des Schriftgeheimnisses), Art. 197 Ziff. 1–3 StGB (Pornographie), Art. 259 StGB (Öffentliche Aufforderung zu Verbrechen oder zur Gewalttätigkeit), Art. 261bis (Rassendiskriminierung) usw.

Fordert der Straftatbestand *Öffentlichkeit*, ist auf den Aufenthaltsort des Täters im Moment der Eingabe des Befehls abzustellen, mit dem die Daten durch automatisierte Programmabläufe auf den öffentlichen Bereich der Festplatte eines Rechners (Web-Server, Usenet-Server) transferiert werden [153]. Der Transport der Daten zum Server und die dortige Speicherung erfolgen nicht mehr durch den Täter, sondern laufen automatisch ab. Daher ist der *Ort des Servers nicht der Ausführungsort* [154].

Eine Besonderheit bei Netzwerkdelikten besteht darin, dass der Ausführungsort, der herkömmlicherweise den Standardanknüpfungspunkt liefert, den Strafverfolgungsbehörden häufig unbekannt bleibt und teilweise gar nicht eruiert werden kann.

6.42 Ort des Erfolgseintritts bei Netzwerkdelikten

Da Netzwerkdelikte häufig im Ausland ausgeführt werden, im Inland aber Wirkungen zeigen, stellt sich die zentrale Frage nach der Bedeutung des Erfolges in Art. 7 Abs. 1 StGB [155]. Dabei ist umstritten, ob es bei allen Straftatbeständen einen (zum gesetzlichen Tatbestand gehörenden) Erfolg gibt oder dies bei bestimmten Deliktstypen, namentlich den abstrakten Gefährdungsdelikten und den schlichten Tätigkeitsdelikten, nicht der Fall ist. Es lassen sich *zwei Auslegungsansätze* unterscheiden:

6.421 Technischer Erfolgsbegriff

---

[153] Zum Begriff der Öffentlichkeit allgemein im StGB und speziell in Art. 261bis StGB (Rassendiskriminierung) NIGGLI, RASSENDISKRIMINIERUNG, (Bibl.), N 691 ff.; GERHARD FIOLKA/ MARCEL ALEXANDER NIGGLI, Der Begriff der Öffentlichkeit im Strafrecht am Beispiel der Bundesgerichtsentscheide vom 21. Juni 2000 und vom 23. August 2000 betreffend Rassendiskriminierung, AJP 2001, 533 ff. m.N.

[154] Vgl. unveröffentl. Entscheid der Anklagekammer des Bundesgerichts vom 11. August 1999 (8G.43/1999), S. 5. Teilweise wird unter Rückgriff auf die Theorie der langen Hand auch der Standort des Zielservers als Ort der Ausführungshandlung bezeichnet, s. POPP (Bibl.), N 6 m.N. Dagegen spricht allerdings die nachweisbare Intention des schweizerischen Gesetzgebers, der das Ubiquitätsprinzip in Art. 7 StGB bewusst auf den Ausführungs- und Erfolgsort beschränkte, um die vom Täter in Bewegung gesetzten oder benützten elektronischen Kräfte („lange Hand“) auszuschliessen, s. EMIL ZÜRCHER, Erläuterungen zum Vorentwurf vom April 1908, Bern 1914, S. 25 f. Nach dieser Auslegung kann es u.U. zu völlig zufälligen Anknüpfungen am Standort des Zielservers kommen, der in einem Land stehen kann, das mit der Tat sonst überhaupt nichts zu tun hat, vgl. SCHWARZENEGGER, E-COMMERCE (Bibl.), S. 339 f.

[155] Das Bundesgericht hatte bisher noch keine Gelegenheit, zur Frage der Erfolgsanknüpfung bei grenzüberschreitenden Internetdelikten Stellung zu nehmen, s. aber zu Deutschland BGHSt 46, 212 (Volksverhetzung). Zum aktuellen Meinungsstand in der Lehre SCHWARZENEGGER, GELTUNGSBEREICH (Bibl.), S. 120 f.; SCHWARZENEGGER., ABSTRAKTE GEFAHR (Bibl.), S. 240 ff.; NIGGLI, NATIONALES STRAFRECHT (Bibl.), S. 144 ff.; WEBER (Bibl.), S. 536 ff. Vgl. zur Rechtlage in Deutschland: LEHLE (Bibl.); HILGENDORF (Bibl.), S. 650 ff.; KOCH (Bibl.), S. 703 ff. alle m.w.N.

Nach *herrschender Lehre* [156] *und Rechtsprechung* [157] orientiert sich die Auslegung des Erfolgsbegriffs in Art. 7 StGB an der Einteilung in die verschiedenen Deliktsarten, also in schlichte Tätigkeitsdelikte bzw. Erfolgsdelikte und in konkrete bzw. abstrakte Gefährdungsdelikte. Diese Einteilung basiert wiederum auf den unterschiedlichen Voraussetzungen, die nach der allgemeinen Tatbestandslehre für die Erfüllung der jeweiligen Tatbestände vorliegen müssen. Da nach dieser Auffassung mit „Erfolg" nach Art. 7 StGB ein im Tatbestand umschriebener, zeitlich und räumlich vom Handlungsort abtrennbarer Aussenerfolg (Erfolg im technischen Sinne) gemeint ist, kann bei schlichten Tätigkeitsdelikten und abstrakten Gefährdungsdelikten nicht daran angeknüpft werden (vgl. Tabelle oben Ziff. 6.12, 2. Spalte).

Mit Ausführung der Handlung sind diese Delikte nämlich schon vollendet, so dass es bei ihnen keinen – vom Ort der Handlung unterscheidbaren – Ort des Erfolgseintrittes geben kann. Konsequenz: Gehört eine mittels Internet verübte Straftat zu den schlichten Tätigkeitsdelikten oder den abstrakten Gefährdungsdelikten, kann sie nur dann in der Schweiz verfolgt werden, wenn sie hier ausgeführt wurde. Handelt der Täter dagegen im Ausland, fehlt es an der schweizerischen Strafgewalt nach dem Territorialitätsprinzip [158].

Dieser Ansatz hat *einerseits* Vorteile: So verhindert er eine Allzuständigkeit der Schweiz im Bereiche der Äusserungsdelikte, die weltweit wahrnehmbar sind, und damit eine Überforderung der schweizerischen Strafverfolgungsbehörden mit sinnlosen Verfahren gegen Täter, die sich im Ausland aufhalten. *Andererseits* liegt in der Einschränkung des Anknüpfungskriteriums des Erfolgsorts in Art. 7 StGB gleichzeitig der Nachteil dieses Ansatzes: dadurch wird nämlich eine *Umgehung des schweizerischen Strafrechts ermöglicht*.

Beispiel: Eine Gruppe Schweizer Skinheads möchte das Web als Werbegefäss für ihre rechtsextreme Aktivität benutzen. Falls sie im Inland den Holocaust verleugnende Texte auf einen Web-Server laden, unterstehen sie der schweizerischen Strafhoheit. Reisen sie aber zu diesem Zweck in die Niederlande oder nach Schweden und laden von dort aus die Inhalte auf das Web, ist eine Strafverfolgung in der Schweiz mangels Strafhoheit nicht möglich [159]. Da der Gesetzgeber die Tatbestände in der Regel unabhängig von den möglichen Konsequenzen für das Strafanwendungsrecht konzipiert, sind die Anknüpfungen teilweise nicht einleuchtend. Bei Art. 197 Ziff. 2 StGB erscheint beispielsweise eine Anknüpfung möglich (Schutz der Erwachsenen vor Konfrontation mit weicher

---

[156] Vgl. zusammenfassend TRECHSEL (Bibl.), Art. 7 N 6; REHBERG/DONATSCH (Bibl.), S. 42 alle m.N.

[157] Das Bundesgericht hatte seine Rechtsprechung zum Begriff des Erfolges in BGE 105 IV 326, der wiederholten Kritik von HANS SCHULTZ folgend, geändert, vgl. zusammenfassend BGE 125 IV 180 ff. In BGE 128 IV 145, 153 rückt es neuerdings wieder von diesem Erfolgsverständnis ab: „Le Tribunal fédéral a longtemps considéré … que la notion de résultat selon l'art. 7 CP s'interprétait de la même manière que pour la définition du délit matériel (…). Il s'est récemmment distancié de cette solution et est revenu à une interprétation plus large de la notion de résultat."

[158] CASSANI (Bibl.), S. 246; NIGGLI, RASSENDISKRIMINIERUNG (Bibl.), N 63 f.; WIDMER/BÄHLER (Bibl.), S. 310 f.; zu Deutschland: HILGENDORF (Bibl.), S 650 ff.; KOCH (Bibl.), S. 703 ff. m.w.N.

[159] Die sog. „Auschwitzlüge" (Art. 261bis Abs. 4 StGB, schlichtes Tätigkeitsdelikt) ist straflos u.a. in den USA, Kanada, Dänemark, den Niederlanden, Schweden und Grossbritannien, vgl. KOCH (Bibl.), S. 704 m.N. Eine Anknüpfung ist auch nach dem aktiven Personalitätsprinzip (Art. 6 Ziff. 1 StGB) nicht möglich, weil es an der Voraussetzung der doppelten Strafbarkeit fehlt. Ähnliche Überlegungen können für international tätige Hosting- und Acess-Provider für die Wahl des Standortes massgebend sein, s. HEINE (Bibl.), S. 106.

Pornographie, konkretes Gefährdungsdelikt), nicht aber bei Art. 197 Ziff. 3 StGB (harte Pornographie, abstraktes Gefährdungsdelikt).

6.422 Erfolg als Verletzung oder Gefährdung eines Angriffsobjektes

Der *zweite Auslegungsansatz* [160] geht demgegenüber davon aus, dass jeder Tatbestandskonstruktion des Besonderen Teils des Strafgesetzbuches eine Verletzung oder eine Gefährdung eines Angriffsobjekts zugrundeliegen muss. Der Erfolg besteht bei den *abstrakten Gefährdungsdelikten* in der Schaffung einer sehr nahen Gefahr für noch nicht konkretisierte Angriffsobjekte (beispielsweise könnte ein beliebiges Kind in der Schweiz mit der im Ausland auf einem Webserver eingestellten weichen Pornographie konfrontiert werden, Art. 197 Ziff. 1 StGB), und der Ort, auf den sich diese abstrakte Gefahr erstreckt, lässt sich bestimmen. Ausserdem ist zu beachten, dass bei dieser Deliktsart der Ort der Ausführungshandlung und der Ort des derart definierten Erfolgseintritts keineswegs immer zusammenfallen. Hinsichtlich Netzwerkdelikten folgt daraus, dass eine Anknüpfung an den Erfolgsort nach Art. 7 Abs. 1 StGB zu bejahen ist, wenn sich die nahe Gefahr der Wahrnehmung durch die Möglichkeit des Abrufs der widerrechtlichen Inhalte in der Schweiz realisiert.

Die Stärke dieses Ansatzes liegt darin, dass er den Gedanken des *Rechtsgüterschutzes* in den Vordergrund stellt und sich nicht an der Konstruktion des jeweiligen Tatbestandes orientiert. Weiter ergibt sich auch ein Anknüpfungspunkt für Teilnahmehandlungen, die gemäss der Bundesgerichtspraxis nach dem Recht zu beurteilen sind, das auf die Haupttat Anwendung findet (vgl. unten Ziff. 6.43). Nachteilig erscheint die Vielzuständigkeit und eventuelle Kollision mit anderen Strafhoheiten.

Zur Verhinderung von Doppelbestrafungen und einer unnötigen Überforderung der Strafverfolgungsbehörden mit aussichtslosen Verfahren bedarf es hier anderer *Einschränkungsmassnahmen*: Internationale Zusammenarbeit durch Ersuchen an andere Staaten, die Strafverfolgung zu übernehmen (Art. 88 IRSG, SR 351.1), Auslieferungsgesuche, Reduktion der Fälle durch Anwendung des *Opportunitätsprinzips* auf im Ausland ausgeführte Taten, bei denen einzig der Erfolg im Inland eintritt, Beschränkung auf Fälle, bei denen das völkerrechtliche Kriterium des „sinnvollen“ Anknüpfungspunktes in der Schweiz gegeben ist [161].

---

[160] FRANZ RIKLIN, Information Highway und Strafrecht, in: R. M. Hilty (Hrsg.), Information Highway, Bern/München 1996, 581 f.; SCHWARZENEGGER, GELTUNGSBEREICH (Bibl.), S. 123 ff.; SCHWARZENEGGER, ABSTRAKTE GEFAHR (Bibl.), S. 249 ff.; LAURENT MOREILLON, Nouveaux délits informatiques sur Internet, Medialex 2001, 25 f.; WEBER (Bibl.), S. 538 (Einschränkung: eine erhebliche Betroffenheit des Verletzten); s. auch HEINE (Bibl.), S. 109 („naheliegend für UWG-Straftaten“, im allgemeinen offen gelassen). Implizit auch Arrêt du Tribunal correctionnel du District de Lausanne, 7 juillet 1997, Medialex 1997, 235 (harte Pornographie); zu Deutschland: BGHSt 46, 212; DIRK-M. BARTON, Mulitmedia-Strafrecht, Neuwied/Kriftel 1999, 146 ff.; BERND HEINRICH, Der Erfolgsort beim abstrakten Gefährdungsdelikt, GA 1999, 79 ff.; LEHLE (Bibl.), S. 57 ff. m.w.N.

[161] Eine flexible Lösung findet sich beispielsweise in Art. 4 Abs. 1 Ziff. 4 der Berner StPO. Ebenso in Art. 8 Abs. 2 lit. d des Vorentwurfs zu einer Schweizerischen Strafprozessordnung, Bern 2001: Sofern dem nicht wesentliche Interessen der Privatklägerschaft entgegenstehen, sehen Staatsanwaltschaft und Gerichte von der Strafverfolgung ab, wenn … „die Straftat bereits von einer ausländischen Behörde verfolgt oder die Verfolgung an eine solche abgetreten wird.“ Vgl. die Erläuterungen dazu im Begleitbericht zum Vorentwurf für eine Schweizerische Strafprozessordnung, Bern 2001, S. 36.

6.43 Die Anknüpfung von Teilnahmehandlungen

Bei in der Schweiz ausgeführten Teilnahmehandlungen (Anstiftung, Art. 24 StGB; Gehilfenschaft, Art. 25 StGB) zu einem Internetdelikt, das vollumfänglich im Ausland realisiert wird, gilt nach der Rechtsprechung des Bundesgerichts der inländische Ausführungsort des Teilnehmers wegen der Akzessorietät zur Haupttat nicht als Anknüpfungspunkt im Sinne von Art. 7 StGB [162]. Infolge der Akzessorietät entfällt für eine Vielzahl von Internet-Sachverhalten die schweizerische Strafhoheit. Fasst man die Regeln über den räumlichen Geltungsbereich als materielle Voraussetzung der Strafbarkeit auf, fällt damit auch die strafrechtliche Verantwortlichkeit dahin [163]. Eine Strafverfolgung gegen einen inländischen Hosting- oder Access-Provider wegen einer Gehilfenhandlung ist damit nicht möglich [164]. Entsprechendes gilt für die Strafverfolgung gegen einen Link-Setzer bei Hyperlink-Verweisung auf eine Webseite im Ausland.

Das Bundesgericht stützt sich bei seiner Praxis auf die Unrechtsteilnahme-Theorie, wonach die Strafbarkeit des Teilnehmers im Regelfall von jener des Haupttäters abhängt. Dessen Beurteilung richte sich nach dem ausländischen Recht und obliege allein dem Gericht am Ort der Tatausführung. Diese Position wird jedoch teilweise angezweifelt, weil es im Strafanwendungsrecht nicht um die Akzessorietät der Strafbarkeit, sondern um die Frage der Lokalisierung einer Straftat gehe [165]. Abgesehen vom Spezialfall der versuchten Anstiftung zu einem Verbrechen (Art. 24 Abs. 2 StGB) seien Anstiftung und Gehilfenschaft nur strafbar, soweit sie erfolgreich sind, d.h. die Haupttat zumindest versucht wird.

Entsprechend muss bei der Gehilfenschaft beispielsweise zwischen einer Ausführungshandlung – irgendein die Haupttat fördernder Beitrag – und dem Erfolg – Durchführung bzw. Versuch der Haupttat – unterschieden werden. Führe der Täter die Gehilfenhandlung in der Schweiz aus, müsse dies genauso zur Begründung der hiesigen Strafhoheit genügen, wie dies bei einem Betrug ganz selbstverständlich sei, bei dem allein die arglistige Täuschungshandlung in der Schweiz verwirklicht werde [166]. Um stossende Resultate zu verhindern, wird einschränkend vorgeschlagen, in solchen Fällen als weitere Voraussetzung die Strafbarkeit der Haupttat am Ort, wo sie begangen wurde, zu verlangen [167].

---

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

[163] POPP (Bibl.) vor Art. 3 N 4; für Prozessvoraussetzung SCHWARZENEGGER, GELTUNGSBEREICH (Bibl.), S. 127.

[164] Es sei denn, die Haupttat unterstehe aufgrund Art. 3 (Erfolg), 4, 5, 6 oder 6bis StGB der Schweizer Strafhoheit. Dann ist diese auch für die Teilnahme begründet.

[165] SCHWARZENEGGER, E-COMMERCE (Bibl.), S. 346; vgl. HANS SCHULTZ, Gesetzgebung und Rechtsprechung der Schweiz im internationalen Strafrecht 1970 bis 1972, SJIR Bd. XXIX, S. 416 f.; TRECHSEL (Bibl.), Art. 7 N 8; POPP (Bibl.), Art. 7 N 14 m.N. Anders als das Bundesgericht z.T. auch die kantonale Praxis, s. HANS SCHULTZ, Gesetzgebung und Rechtsprechung der Schweiz im internationalen Strafrecht 1942 bis 1963, SJIR Bd. XX, S.192 f.

[166] Gemeint sind also Betrugsfälle, deren Erfolge, d.h. Irrtum, Vermögensdisposition und -schaden, vollumfänglich im Ausland eintreten, s. dazu CHRISTIAN SCHWARZENEGGER: Handlungs- und Erfolgsort beim grenzüberschreitenden Betrug, Festschrift Niklaus Schmid, Zürich 2001, S. 158 f. m.N.

[167] Prinzip der identischen Norm, TRECHSEL (Bibl.), Art. 7 N 8 m.N.

6.44 Fallbeispiele (vgl. Anhang)

Ob ein Internet-Delikt in der Schweiz zur Anklage gebracht werden kann, ist – wie in den vorstehenden Abschnitten dargelegt – in vielfacher Hinsicht *unklar*. Anhand dreier Beispielfälle soll im *Anhang* stichwortartig die Komplexität des Zusammenwirkens von Strafanwendungsrecht und materiellem Strafrecht sowie der Sonderregeln des Medienstrafrechts illustriert werden. Viele der auftretenden Fragen können nicht eindeutig beantwortet werden.

Als *erster Fall* soll dazu das Bereitstellen einer kinderpornographischen Bilddatei auf einer Webseite dienen (Art. 197 Ziff. 3 StGB), als *zweiter Fall* eine Aufforderung zu einem Brandanschlag in einer Newsgroup (Art. 259 Abs. 1 StGB) und als *dritter Fall* eine Webseite mit Texten, die für eine systematische Herabsetzung einer bestimmten Ethnie eintreten (Art. 261bis Abs. 2 StGB). WWW und Newsgroup stehen hier austauschbar für Internetdienste, die sich an die Öffentlichkeit richten.

Die ausführliche Darstellung der drei Fälle in verschiedenen Konstellationen findet sich im Anhang.

6.5 Bundesgerichtsbarkeit oder kantonale Gerichtsbarkeit?

Direkt aus den Schwierigkeiten der Bestimmung der Strafhoheit (vgl. oben Ziff. 6.4) ergibt sich auch für die Strafverfolgung ein Problem. Grundsätzlich ist im Falle eines Internet-Delikts nämlich bei Aufnahme der Ermittlungen nicht bekannt, wo die Tat ausgeführt wurde. Daraus folgt, dass Strafverfahren bei Delikten via Internet zumeist von nicht zuständigen Behörden angehoben werden und diese Verfahren erst im Verlauf der Ermittlungen an die zuständigen Behörden abgetreten werden können [168].

Alternativ bliebe einzig eine Anknüpfung an den Erfolg. Versteht man aber unter Erfolg mit der heute herrschenden Lehre und Rechtsprechung [169] den Erfolg im Sinne des Tatbestandes, so können Delikte, die keinen Erfolg in diesem Sinne kennen (also z.B. die meisten sog. Äusserungsdelikte, s. Tabelle oben Ziff. 6.12, 2. Spalte) geographisch allein am Ausführungsort angeknüpft werden.

Wenn man eine weite Definition des „Erfolgs“ i.S.v. Art. 7 StGB vertritt, erlaubt dies zwar, eine schweizerische Zuständigkeit für die Strafverfolgung nach Art. 7 StGB zu begründen, weil der Erfolg damit grundsätzlich *ubiquitär* wird, d.h. überall dort eintritt, wo die fragliche Information wahrnehmbar ist. Was international möglicherweise erwünscht ist, führt übersetzt in inländische Verhältnisse aber zu einer eigentlichen Proliferation der Zuständigkeiten, d.h. dazu, dass jede Strafverfolgungsbehörde, die sich zuständig fühlt bzw. durch eine Anzeige zuständig wird, auch zuständig ist [170].

Nach Art. 346 Abs. 1 StGB sind zur Verfolgung die Behörden des Ausführungsortes zuständig bzw. – sofern nur der Erfolg in der Schweiz eingetreten ist – die Behörden des Erfolgsortes. Die zweitgenannte Konstellation dürfte bei Internet-Delikten

---

[168] NIGGLI, NATIONALES STRAFRECHT (Bibl.), S. 169 f.
[169] Anders jüngst BGE 128 IV 145, 153.
[170] NIGGLI, INTERNET-KRIMINALITÄT, (Bibl.), S. 6 f.

zumindest vorläufig die Normalvariante darstellen. Damit ergibt sich *erstens* die Frage, wie bei Delikten zu verfahren sei, die keinen Erfolg im Sinne des Tatbestandes kennen. *Zweitens* ergibt sich als Konsequenz, dass selbst bei Anwendung einer weiten Definition des Erfolges im Sinne von Art. 7 StGB die Schweiz zwar zur Verfolgung zuständig wird, innerstaatlich die Verfolgung aber von Zufälligkeiten abhängt. Nach Art. 346 Abs. 2 StGB sind nämlich bei Eintritt des Erfolgs an mehreren Orten - also im Rahmen eines weiten Verständnisses des Erfolges bei Äusserungsdelikten grundsätzlich immer – die Behörden desjenigen Ortes zuständig, an welchem die Untersuchung zuerst angehoben wurde. Das heisst, dass – zumindest bei Ehrverletzungen, Gewaltdarstellungen, Pornographie, Rassendiskriminierung, aber auch bei der Anleitung zur Herstellung von Computerviren (Art. 144bis Ziff. 2 StGB) – grundsätzlich jede schweizerische Strafverfolgungsbehörde zuständig ist, sobald eine entsprechende Erstanzeige eingegangen ist [171].

Diese umfassende Zuständigkeit aller schweizerischen Strafverfolgungsbehörden für alle Internet-Delikte führt zu massiv *überlappenden Kompetenzen*. In anderen Fällen besteht ein erheblicher *Koordinationsbedarf*, wie der kürzlich prominent gewordene „Fall Landslide“ aufgezeigt hat [172].

Die Situation könnte konsequent nur über eine entsprechende *Kompetenz des Bundes* entschärft werden. Genau dies sieht die am 26. September 2002 eingereichte parlamentarischen Initiative Aeppli Wartmann (Pa.Iv. 02.452, vgl. oben Ziff. 1.22) vor. Angeregt wird darin eine Bundeskompetenz im Sinne von Art. 340bis StGB (Organisiertes Verbrechen und Wirtschaftskriminalität), d.h. eine Kompetenz des Bundes in all jenen Fällen, in welchen die Tat zum wesentlichen Teil im Ausland oder in mehreren Kantonen begangen wurde, also dem Standardfall der Internet-Delikte zumindest bei Äusserungsdelikten.

[171] NIGGLI, INTERNET-KRIMINALITÄT (Bibl.), S. 6 f.

[172] Auf einer kommerziellen Website in den USA konnten Nutzer kinderpornographische Bilddateien gegen Kreditkartenzahlung ansehen und herunterladen. Nachdem die Täter festgenommen wurden, betrieb das FBI die Website weiter und übermittelte dem Bundesamt für Polizei via INTERPOL die Kreditkartenangaben der Schweizer Kunden von Landslide. Im Herbst 2002 kam es zu einer koordinierten Aktion der kantonalen Strafverfolgungsbehörden („Genesis“), wobei allerdings Informationen darüber in einzelnen Kantonen schon an die Öffentlichkeit gelangten, als andere Kantone noch nicht mit der Durchsuchung und Beschlagnahme von Computern bei den Tatverdächtigen in ihrem Zuständigkeitsbereich fertig waren.

Die Einführung zulässiger und gebotener verwaltungsrechtlicher Instrumente erfordert weder eine Revision des geltenden Telekommunikationsrechts noch ein neues Gesetz. Entsprechende Massnahmen lassen sich vielmehr in die vorgeschlagene Revision des StGB integrieren. Auf einen speziellen verwaltungsrechtlichen Flankenschutz kann daher verzichtet werden.

7. Möglichkeit verwaltungsrechtlicher Massnahmen

7.1. Ausgangslage

7.11 Bedürfnis nach verwaltungsrechtlichen Massnahmen

Die Expertenkommission hat sich die Frage gestellt, ob es zur Bekämpfung von Rechtsgutverletzungen in Kommunikationsnetzen neben strafrechtlicher allenfalls auch *verwaltungsrechtlicher* Regelungen und Massnahmen bedarf. Diese könnten gegebenenfalls helfen, Rechtsgutverletzungen vorzubeugen, und zudem dort wirken, wo das (schweizerische) Strafrecht nicht angewendet werden kann.

Dieser Bedarf nach verwaltungsrechtlicher Unterstützung muss sich freilich an den Garantien orientieren, die sich aus den Grundrechten freier Kommunikation ergeben[173]. Die möglichen verwaltungsrechtlichen Massnahmen sind zudem in jedem Fall auf eine *flankierende*, das Strafrecht *ergänzende* Funktion zu begrenzen.

7.12 Bundeskompetenz

Das Fernmeldewesen (insbesondere die Netze der Telekommunikation) und die elektronischen Medien werden durch Art. 92 (Post- und Fernmeldewesen) bzw. Art. 93 BV (Radio und Fernsehen) erfasst: Aufgrund beider Verfassungsbestimmungen steht es dem Bund zu, *alle* in diesen Sachbereichen auftretenden Fragen zu regeln. Diese Bundeskompetenzen sind zudem *ausschliesslicher* Natur; sie verbieten kantonale Regelungen ungeachtet der Lückenhaftigkeit einer bundesgesetzlichen Ordnung [174].

---

[173] Vgl. oben Kapitel 5.

[174] Vgl. etwa ROLF H. WEBER, § 60 Energie und Kommunikation, in: Thürer/Aubert/Müller (Hrsg.), Verfassungsrecht der Schweiz/Droit constitutionnel suisse, Zürich 2001, S. 943 ff., Rz. 27; ferner auch ANDREAS KLEY, Bundeskompetenzen mit ursprünglich derogatorischer Wirkung aus historischer Perspektive, in: recht 1999, S. 189 ff., 200.

7.13 Geltende Rechtslage

7.131 Fernmelderecht

Das Fernmelderecht regelt als Infrastrukturrecht in erster Linie den Transport von Informationen, welche fernmeldetechnisch übertragen werden (vgl. Art. 2 i.V.m. Art. 3 lit. b, c FMG). Dabei ist das Internet vor allem als Plattform für die Individual-Kommunikation (E-Mail, Voice over IP, Datenübermittlung) oder für die fernmeldetechnische Verbreitung von Informationen erfasst, die nicht als Radio- oder Fernsehsendungen gelten.

Nur vereinzelte Bestimmungen beziehen sich auf den *Inhalt* der übertragenen Informationen [175]. Diese vermögen aber für verwaltungsrechtliche Massnahmen der hier interessierenden Art nicht als Grundlage zu dienen.

7.132 Rundfunkrecht

Das RTVG ist auf Radio- und Fernsehsendungen traditionellen Zuschnitts ausgerichtet und für Anordnungen der hier interessierenden Art nicht geeignet. Auch das neue Radio- und Fernsehgesetz soll lediglich die Veranstaltung, die Verbreitung und den Empfang eigentlicher Programme regeln[176]. Ein Programm ist eine vom Veranstalter zusammengestellte, für die Allgemeinheit bestimmte, zeitlich angesetzte und kontinuierlich angebotene Folge von Sendungen, welche fernmeldetechnisch verbreitet wird.

So spielt etwa das Internet bloss als Verbreitungs-Infrastruktur eine Rolle. Werden eigentliche Radio- und Fernsehprogramme über das Internet verbreitet, so unterstehen sie dem RTVG. Andere Internet-Dienste regelt das Rundfunkrecht hingegen auch künftig nicht.

7.133 Fazit

Das geltende Recht kennt also *keine Vorschriften*, die als Grundlage für verwaltungsrechtliche Massnahmen zur Bekämpfung von Rechtsgutverletzungen in Kommunikationsnetzen herangezogen werden könnten. Provider werden in der Regel nur mit Bezug auf die Übermittlung von Informationen durch das FMG verwaltungsrechtlich erfasst.

---

[175] Vgl. z.B. Art. 43 ff. FMG (Fernmeldegeheimnis), Art. 48 FMG (Einschränkung des Fernmeldeverkehrs aus wichtigen Gründen), Art. 49 FMG (Fälschen und Unterdrücken von Informationen), Art. 31 FDV (Pflicht der Anbieter von Diensten der Grundversorgung, eine unentgeltliche Möglichkeit zur Sperrung abgehender Verbindungen zu Diensten mit erotischem oder pornografischem Inhalt zur Verfügung zu stellen).

[176] UVEK, Erläuterungen zum Entwurf für ein neues Radio- und Fernsehgesetz (RTVG), Vernehmlassung Dezember 2000, S. 18 f. – Die Botschaft zur Totalrevision des neuen RTVG wurde vom Bundesrat am 18. Dezember 2002 verabschiedet; vgl. BBl 2003, 1569 ff.

7.2 Mögliche verwaltungsrechtliche Instrumente

7.21 Polizeirechtliche Regelungen und Anordnungen

Im Vordergrund steht die Schaffung einer gesetzlichen Grundlage für polizeirechtliche Anordnungen zur Wahrung *spezifischer Rechtsgüter*. Die Zulässigkeit einer solchen Regelung hängt von der Art der darin vorgesehenen *Massnahmen* ab.

7.211 Bewilligungspflichten

Die Einführung einer Bewilligungspflicht für das *Aufschalten einer Website* ist mit dem Verbot der *Vorzensur* (Art. 17 Abs. 2 BV) unvereinbar [177].

Auch eine Bewilligungspflicht für das *Anbieten von Speicherplatz* für Informationen Dritter, die für die Allgemeinheit bestimmt sind, kann auf eine unzulässige Vorzensur hinauslaufen; dies zumal wenn die Erteilung einer solchen Bewilligung an die Installation von bestimmten Sicherungsmassnahmen (z.B. Filtern) gekoppelt wird.

7.212 Verpflichtung zur Inhaltskontrolle

Denkbar wäre ferner die Schaffung einer Spezialnorm, welche die Provider zur Durchführung von *Inhaltskontrollen* verpflichtet und deren Einhaltung durch *Aufsichtsmassnahmen* durchgesetzt werden könnte. Damit liesse sich u.U. auch die gesetzliche Verpflichtung zur Installation eines *automatisierten Kontrollsystems* verbinden, das bestimmte Informationen herausfiltert oder vom öffentlichen Zugang ausnimmt.

Solche Regelungen würden aber den Providern staatliche Rechtsanwendungshoheit übertragen und ihnen damit ermöglichen, selber zu bestimmen, welche Inhalte als illegal herausgefiltert werden müssen, was in der Verfassung keine Stütze findet [178]. Diese Möglichkeit könnte zudem von den Providern dazu missbraucht werden, um gezielt ihre Konkurrenz auszuschalten und unlauteren Wettbewerb zu betreiben [179].

Eine allgemeine gesetzliche Pflicht zur Inhaltskontrolle dürfte sich zudem in den meisten Fällen als ungeeignet und damit als unverhältnismässig erweisen. Denn Schutzfilter und -programme lassen sich durch einfache technische Operationen relativ leicht umgehen. Da im (benachbarten) Ausland keine entsprechenden

---

[177] Vgl. im gleichen Sinne die „Déclaration sur la liberté de la communication sur l'Internet" des Ministerkomitees des Europarates vom 28. Mai 2003: http://www.coe.int/T/F/Droits_de_l%27Homme/media/5_Ressources_documentaires/1_Textes_de_base/2_%20Textes_du_Comite_des_Ministres/PDF_D%E9claration%20libert%E9%20de%20communication%20sur%20Internet%20%20(f).pdf

[178] Vgl. mit dem gleichen Ergebnis die „Déclaration sur la liberté de la communication sur l'Internet" (a.a.O.)

[179] Vgl. SEMKEN, (Bibl.), S. 270 f., mit dem einleuchtenden Beispiel des Einsatzes eines „Kinderschutzfilters" durch einen Provider, der gleichzeitig Content-Provider ist, mit dem Ziel, gewisse Produkte der Konkurrenz ausschalten zu können.

Vorschriften bestehen, dürfte eine solche Regelung zumindest bei den Access-Providern ohnehin weitgehend wirkungslos sein [180].

7.213 Melde- und Anzeigepflicht

Wo eine Melde- bzw. Anzeigepflicht der Provider mit der (vorgängigen) Pflicht zur Durchführung einer Inhaltskontrolle gekoppelt ist, bleibt sie aus den oben genannten Gründen unzulässig. Dagegen erscheint es nicht von vornherein unstatthaft, Provider, die aufgrund von direkt an sie gerichteten Hinweisen Dritter konkrete Kenntnis von einer mutmasslichen Rechtsgutverletzung haben, zu einer entsprechenden Meldung bzw. Anzeige an eine Behörde zu verpflichten [181]. Denn damit wird dem Provider weder die staatliche Rechtsanwendungshoheit übertragen, noch wird er zur Durchführung einer Inhaltskontrolle verpflichtet. Allerdings muss die Bestimmung des Kreises der meldepflichtigen Provider unter dem Gesichtspunkt des Rechtsgleichheitsgebots nach sachlichen Gründen erfolgen.

Nach Auffassung der Expertenkommission ist es sinnvoll, diese beschränkte Meldepflicht in die vorgeschlagene Neufassung von Art. 322bis Ziff. 1 Abs. 2 StGB aufzunehmen und ihre Erfüllung auf diese Weise durch die Androhung von strafrechtlichen Sanktionen sicherzustellen[182].

7.214 Monitoring

Ob auch das „*Monitoring* “ [183] als Vorzensur oder als rechtfertigungsfähige (Art. 36 BV) Nachzensur zu gelten hat, ist umstritten[184]. Bei einer derartigen Massnahme wäre aber jedenfalls darauf zu achten, dass sich die Kontrolle nicht durch technische Automatismen vornehmen lässt; denn Rechtsgutverletzungen können immer nur durch Menschen festgestellt werden. Die aus einer solchen Nachzensur hervorgehende Sperrung oder Beseitigung von Websites müsste als (anfechtbare) Verfügung ausgestaltet werden.

---

[180] Gemäss Art. 15 Ziff. 1 der E-Commerce-Richtlinie der EU (vgl. dazu oben Kapitel 4) wird es den Mitgliedstaaten sogar untersagt, den Access-, Caching- und Hosting-Providern eine allgemeine Pflicht aufzuerlegen, die von ihnen übermittelten und gespeicherten Informationen zu überwachen oder aktiv nach Umständen zu forschen, die auf eine rechtswidrige Tätigkeit hinweisen.

[181] Vgl. auch Art. 15 Ziff. 2 der E-Commerce-Richtlinie der EU, wonach die Mitgliedstaaten Anbieter von Diensten der Informationsgesellschaft dazu verpflichten können, die zuständigen Behörden unverzüglich über mutmassliche rechtswidrige Tätigkeiten oder Informationen der Nutzer ihres Dienstes zu unterrichten.

[182] Vgl. dazu unten Kapitel 9. – Die Meldepflicht beschränkt sich sinnvollerweise auf Provider, die fremde Informationen automatisiert in einem elektronischen Kommunikationsnetz bereithalten („Hosting-Provider“).

[183] „Monitoring“ wird hier verstanden als systematische, durch staatliche Stellen durchgeführte Kontrolle von im Kommunikationsnetz verbreiteten Informationen auf potenzielle Rechtsgüterverletzungen.

[184] Vgl. zum Ganzen eingehend MARKUS SCHEFER, Die Kerngehalte von Grundrechten, Habil. Bern 2001, S. 462 ff. – Seit Januar 2003 recherchiert die neu geschaffene „Koordinationsstelle für die Bekämpfung der Internet-Kriminalität“ (KOBIK) nach strafbaren Handlungen, die im Internet begangen werden. Nach Auffassung der Expertenkommission handelt es sich hierbei um eine Art „Streifenfahrt im Internet“, welche zwar durchaus als „Monitoring“ qualifiziert werden kann, sich diesfalls jedoch hinreichend begründen lässt und daher vor der Verfassung standhält.

7.215 Sperrungs- und Beseitigungsverfügungen

Die Schaffung einer gesetzlichen Regelung, die aufgrund des „Störerprinzips“ sowohl den Content- als auch den Hosting-Provider als potenzielle Adressaten einer Beseitigungsverfügung nennt, ist *rechtmässig*. Ist der Provider mit der konkreten behördlichen Anordnung nicht einverstanden, kann er sie gerichtlich überprüfen lassen. Nach Auffassung der Expertenkommission ist es jedoch sinnvoll, die gesetzliche Grundlage für solche Verfügungen in der vorgeschlagenen Bestimmung von Art. 322bis Ziff. 1 Abs. 5 StGB unterzubringen [185].

Mit Bezug auf Access-Provider erweist sich dagegen bereits eine generell-abstrakte Verpflichtung, den Zugang zu bestimmten Daten einzuschränken, als *ineffizient* und damit *unverhältnismässig*. Denn solche Zugangsbeschränkungen lassen sich trotz grossem Aufwand der Provider technisch relativ leicht umgehen [186].

7.22 Erweiterung von Konzessionspflicht und -voraussetzungen?

7.221 Grundsätzliches

Nach geltendem Fernmelderecht knüpft die Konzessionspflicht an den unabhängigen Betrieb von Fernmeldeanlagen an. Inhaltliche Aspekte bilden dabei kein Kriterium. Da die meisten Provider der Schweiz keine Anlagen zur fernmeldetechnischen Übertragung von Informationen unabhängig betreiben, unterliegen sie grundsätzlich keiner Konzessions-, sondern allenfalls einer Meldepflicht (Art. 4 Abs. 2 FMG).

Zur Bekämpfung der Netzwerkkriminalität könnten theoretisch der persönliche Umfang der Konzessionspflicht erweitert und gleichzeitig die Konzessions-anforderungen für Anbieter von Fernmeldedienstleistungen auf die inhaltliche Ebene ausgedehnt werden. Damit würden die *Access-Provider* verpflichtet, den Inhalt der über ihre Infrastrukturanlagen fliessenden Datenströme zu kontrollieren. Eine solche Regelung *widerspricht* jedoch nicht nur der heutigen Entwicklung, sondern erweist sich ausserdem als *unzulässig:*

7.222 Widerspruch zum heutigen Trend

Die Einführung zusätzlicher Konzessionspflichten läuft eindeutig dem heutigen Trend zuwider. Im Bereich des RTVG soll die Meldepflicht zur Regel werden. Eine Konzessionspflicht soll nur noch dort bestehen, wo beschränkt verfügbare Güter (z.B. Frequenzen) zuzuteilen oder öffentliche Gelder (Anteile aus den Empfangsgebühren) auszurichten sind.

Auch die im Juni 2002 in die Vernehmlassung geschickte *Teilrevision des Fernmeldegesetzes* will das bisherige umfassende Konzessionssystem für Fernmeldedienste aufgeben und dafür gleichzeitig die staatliche Aufsicht effizienter ausgestalten[187].

---

[185] Vgl. dazu unten Kapitel 9.
[186] Vgl. allerdings weitergehend Art. 12 Ziff. 3 E-Commerce-Richtlinie der EU; s. oben Kapitel 4.
[187] Vgl. zum Ganzen <http://www.bakom.ch/de/telekommunikation/grundlagen/konsult/fmg/index.html>.

7.223 Unzulässigkeit

Unzulässig ist eine Delegation staatlicher Inhaltskontrolle an Konzessionäre, wenn sie zu einer *Vorzensur* (Art. 17 Abs. 2 BV) führt, da sie dann den Kerngehalt der Meinungs- und Medienfreiheit tangiert.

Doch auch eine an den Konzessionär delegierte Inhaltskontrolle, die als *Nachzensur* erscheint, ist unzulässig. Denn eine solche Regelung entlässt die Rechtsanwendungshoheit aus der staatlichen Sphäre in die Gefahr von Willkür und Missbrauch.

Durch die Erweiterung der Konzessionsanforderungen auf inhaltliche Aspekte würden die Access-Provider gezwungen, ein Sicherheits- und Kontrollsystem zu installieren und zu betreiben; dies aber erscheint unverhältnismässig und damit unzulässig (vgl. oben Ziff. 7.212).

7.23 Gentlemen‘s Agreement

Als Alternative zum klassischen Polizeirecht bieten sich für den Schutz der bedrohten Rechtsgüter auch *informelle Absprachen* („Gentlemen’s Agreements“) an. Diese zielen auf eine Verhaltenssteuerung, ohne aber rechtsverbindliche Pflichten zu begründen [188]. Sie sind vor allem im Umweltrecht sowie im Wirtschaftsverwaltungsrecht verbreitet.

Das Legalitätsprinzip steht solchen Absprachen nicht entgegen, ausser dort, wo Sinn und Zweck einer Norm deren Anwendung ausdrücklich oder implizit - beispielweise durch Verweisung auf die Handlungsformen der Verfügung oder des Vertrags - untersagen [189].

Im vorliegenden Zusammenhang erscheinen informelle Absprachen aber nur in begrenztem Ausmass geeignet. Zwar liessen sich damit die für die Provider technisch möglichen und zumutbaren Kontroll- und Sicherungsmassnahmen einvernehmlich bestimmen. Es müsste aber gleichzeitig sichergestellt werden, dass die Bestimmung der illegalen Inhalte von Informationen und damit die Rechtsanwendungshoheit im Einzelfall bei den staatlichen Behörden verbleibt. Ausserdem stossen informelle Absprachen an ihre Grenzen, wo sie in die Grundrechte Dritter – wie z.B. die Informationsfreiheit des Publikums oder die Wirtschaftsfreiheit anderer Provider – eingreifen. Die Lehre fordert in solchen Fällen eine vorgängige Anhörung der betroffenen Dritten, andernfalls in der Sache verfügt werden muss [190]. Im Übrigen werden die Grenzen informeller Absprachen, deren Umfang bisher noch wenig geklärt ist[191], im vorliegenden Kontext deutlicher als in anderen Rechtsbereichen sichtbar.

---

[188] HÖSLI (Bibl.), S. 39 f.; PFENNINGER (Bibl.), S. 228; HÄFELIN/MÜLLER (Bibl.), N 734 ff., 737; TSCHANNEN/ZIMMERLI /KIENER (Bibl.), S. 265.
[189] Vgl. HÖSLI (Bibl.), S. 168 ff.; PFENNINGER (Bibl.), S. 81 ff., 102 ff.
[190] TSCHANNEN/ ZIMMERLI/KIENER (Bibl.), S. 267.
[191] HÄFELIN/MÜLLER (Bibl.), Rz. 736.

7.3 Fazit: Verzicht auf verwaltungsrechtlichen Flankenschutz

Die verfassungsrechtlichen Leitplanken (Verbot der Vorzensur, Verhältnismässigkeitsprinzip) schränken den Umfang der zulässigen verwaltungsrechtlichen Regelungen stark ein. Nach Auffassung der Expertenkommission bedarf es jedoch für die Einführung der (an sich) verwaltungsrechtlichen Instrumente, die von Verfassungs wegen zulässig und zugleich geboten sind, keiner Revision des geltenden Telekommunikationsrechts, und erst recht nicht der Schaffung eines neuen Gesetzes. Die entsprechenden Massnahmen lassen sich vielmehr in die hier vorgeschlagene Revision des StGB integrieren und darüber hinaus allenfalls mit laufenden Gesetzgebungsverfahren verknüpfen:

- Eine verwaltungsrechtliche *Meldepflicht* erweist sich angesichts des vorgeschlagenen neuen *Art. 322bis Ziff. 1 Abs. 2 StGB* als überflüssig. Diese Bestimmung enthält eine beschränkte, aber hinreichende Meldepflicht für Hosting-Provider (vgl. unten Kapitel 9).
- Statt eine separate verwaltungsrechtliche Grundlage für *Beseitigungs- und Sperrungsanordnungen* gegenüber Hosting- und Content-Providern zu schaffen, kann über die von der Expertenkommission vorgeschlagene Bestimmung von Art. 322bis Ziff. 1 Abs. 5 StGB ungeachtet des Vorliegens schweizerischer Strafhoheit auf die Beseitigung illegaler Informationen hingewirkt werden (vgl. unten Kapitel 9). Gegen an Access-Provider gerichtete Löschungs- und Sperranordnungen, sei es basierend auf einer extensiven Auslegung von Art. 58 StGB oder aufgrund von Normen des kantonalen Strafprozessrechts, sprechen demgegenüber dieselben Gründe, wie sie bereits im Zusammenhang mit verwaltungsrechtlichen Sperrmassnahmen dargestellt worden sind (oben Ziff. 7.215).

Anstelle eines verfassungsrechtlich nicht immer unbedenklichen „*Monitorings*“ könnte eine gesetzliche Grundlage für *verdeckte Ermittlungen* geschaffen werden. Ein solches Verfahren verspräche insbesondere mehr Effizienz im Kampf gegen strafrechtlich relevante Inhalte in Kommunikationsnetzen. Die Expertenkommission verzichtet indes darauf, im vorliegenden Kontext eine solche Rechtsgrundlage vorzuschlagen und begnügt sich mit dem Hinweis auf das zur Zeit in den eidgenössischen Räten behandelte Bundesgesetz über die verdeckte Ermittlung (BVE).

Die zivilrechtliche Verantwortlichkeit im Zusammenhang mit Rechtsverletzungen im Internet richtet sich nach dem Obligationenrecht und den spezialgesetzlichen Haftungsnormen. Spezifische Bestimmungen für Internet-Provider fehlen heute. Eine entsprechende künftige Gesetzgebung sollte sich vorab von der E-Commerce-Richtlinie der EU inspirieren lassen.

8. Zivilrechtliche Haftung

8.1 Vorbemerkungen

Neben dem Strafrecht prägt auch das Zivilrecht massgeblich die Verantwortlichkeitsordnung, welche die Tätigkeit und die Investitionsentscheide von Internet-Providern bestimmt. Die öffentliche Empörung über die Verbreitung strafbarer Inhalte (z.B. Pornographie, Rassendiskriminierung, Gewaltdarstellung) lässt allerdings zivilrechtliche Verantwortlichkeitsursachen, wie etwa die Verletzung des Immaterialgüter-, Wettbewerbs- und Persönlichkeitsrechts, in den Hintergrund treten.

Doch zeigt die Rechtsprechung im Ausland, dass sich zivilrechtliche Klagen gegen Hosting- und Access-Provider häufen, und die zivilrechtliche Haftung an Bedeutung gewinnt. Wenn die strafrechtliche Verantwortlichkeit von Internet-Providern untersucht wird, können zivilrechtliche Verantwortlichkeitsursachen im Interesse der Kohärenz nicht unberücksichtigt bleiben. Gemeinsamkeiten und Unterschieden ist dabei gleichermassen Rechnung zu tragen.

Die Expertenkommission befasste sich im Rahmen ihrer primär auf die strafrechtliche Verantwortlichkeit ausgerichteten Arbeiten auch mit der Frage einer Änderung der zivilrechtlichen Haftungsbestimmungen. Ausgehend vom Begleitbericht zum Entwurf eines Bundesgesetzes über den elektronischen Geschäftsverkehr [192], wonach kein Bedarf nach einer Regelung der Haftung von Providern besteht [193], erwog sie *zum einen* die grundsätzliche Notwendigkeit einer Änderung im Zivilrecht. *Zum anderen* erörterte sie die Zweckmässigkeit einer gleichzeitigen Anpassung von Straf- und Zivilrecht im Vergleich zu einer zeitlich gestaffelten Änderung in den beiden Rechtsbereichen.

[192] Begleitbericht vom 17. Januar 2001 zum Entwurf eines Bundesgesetzes über den elektronischen Geschäftsverkehr (Teilrevision des Obligationenrechts und des Bundesgesetzes gegen den unlauteren Wettbewerb), <http://www.ofj.admin.ch/themen/e-commerce/vn-ber-b-d.pdf>.

[193] A.a.O., S. 9: „Ebenfalls wesentlich von der internationalen Rechtsentwicklung hängen auch allfällige Anpassungen des Immaterialgüterrechts sowie der straf- und zivilrechtlichen Verantwortlichkeit der Provider ab. Ein unmittelbarer Handlungsbedarf besteht diesbezüglich nicht. Sachgerechte Lösungen lassen sich auf der Grundlage des geltenden Rechts finden."

Die Expertenkommission hat ungeachtet des grenzüberschreitenden Charakters des Informationsflusses im Internet von einer Behandlung der Probleme des *internationalen Privatrechts* abgesehen. Eine Prüfung dieser Fragen wäre nach ihrer Ansicht über ihren Auftrag hinausgegangen; dieser verlangt eine Stellungnahme zur inhaltlichen Ausgestaltung namentlich der strafrechtlichen Verantwortlichkeit von Internet-Providern.

Die Straftatbestände in *zivilrechtlichen Spezialerlassen*, namentlich im Urheberrechtsgesetz (URG, SR 231.1), im Markenschutzgesetz (MSchG, SR 232.11) sowie im Bundesgesetz über den unlauteren Wettbewerb (UWG, SR 241) werden bei der strafrechtlichen Fragestellung behandelt (siehe oben Ziff. 6.12)

8.2 Ausservertragliche Haftung

8.21 Haftungsgrundlagen

Die schweizerische Rechtsordnung kennt keine spezifischen Haftungsnormen, welche die deliktische Verantwortlichkeit für Rechtsverletzungen im Zusammenhang mit der Nutzung des Internet regeln. Zu deren Beurteilung muss daher auf die *allgemeinen Bestimmungen des Obligationenrechts* (OR, SR 220) zur Haftung aus unerlaubter Handlung (namentlich bei Persönlichkeitsverletzungen) oder auf *spezialgesetzliche Haftungsnormen* zurückgegriffen werden (hier v.a. Art. 62 URG, Art. 55 MSchG, Art. 9 UWG). Die vermögensrechtlichen Ansprüche richten sich allerdings auch aufgrund dieser Spezialgesetze nach den Bestimmungen des Obligationenrechts [194].

8.22 Haftung von Access- und Hosting-Providern

Die Ausgangslage der Diskussion zur zivilrechtlichen Haftung von Access- und Hosting-Providern ist vergleichbar mit jener im Strafrecht: Die Identifizierung und Ermittlung der für eine Rechtsverletzung unmittelbar verantwortlichen Person erweist sich bei einer über das Internet begangenen Rechtsgutsverletzung in tatsächlicher Hinsicht bisweilen als unmöglich oder erfordert einen unverhältnismässigen Aufwand.

Wird der Verantwortliche identifiziert, so kann seine Verfolgung dennoch aussichtslos erscheinen. So beispielsweise, wenn er sich im Ausland aufhält oder über keine ausreichenden finanziellen Mittel verfügt, die als Haftungssubstrat für eine Schadenersatzklage dienen könnten. Für den Rechtsinhaber stellt sich daher die

[194] Die *Unterlassungs- und Beseitigungsklagen* sind gegen jedes objektiv rechtswidrige Verhalten gegeben. Ein Verschulden ist nicht erforderlich, ebenso wenig der Nachweis eines Schadens. Nach Massgabe von Art. 41 OR erfordert die *Schadenersatzklage* den Nachweis eines Schadens, der Widerrechtlichkeit des Verhaltens, des Kausalzusammenhangs zwischen schädigendem Verhalten und Schadenseintritt sowie des Verschuldens der rechtswidrig handelnden Person. Der *Genugtuungsanspruch* setzt demgegenüber neben der Rechtswidrigkeit und dem Kausalzusammenhang eine Persönlichkeitsverletzung von gewisser Schwere voraus. Der Anspruch auf *Gewinnherausgabe* gemäss Art. 423 OR besteht nach traditioneller Rechtsprechung unabhängig von einem Verschulden.

Frage, ob er Dritte für die Rechtsgutsverletzung in Anspruch nehmen kann. Dabei fallen auch die am Kommunikationsvorgang beteiligten Access- und Hosting-Provider in Betracht.

Ansatzpunkt für eine Inanspruchnahme solcher Beteiligter bietet Art. 50 OR, auf den in Art. 28a ZGB sowie in den jeweiligen Spezialgesetzen verwiesen wird. Im Sinne dieser Vorschrift ist jede Person für Schadenersatzklagen passivlegitimiert, die an einer Verletzung oder Gefährdung eines Rechtsgutes (als Anstifter oder Gehilfe) mitwirkt. Eine gemeinsame Absprache ist nicht vorausgesetzt. Es genügt, wenn die Beteiligten erkennen müssen, dass ihr Handeln oder Unterlassen geeignet ist, die Rechtsgutverletzung schuldhaft herbeizuführen.

8.221 Verschuldensabhängige Ansprüche

Allfällige verschuldensabhängige Schadenersatzansprüche gegen Access- oder Hosting-Provider werden in vielen Fällen von der Beurteilung von Fahrlässigkeitsvorwürfen abhängen, die sich im Falle einer Unterlassung [195] mit Handlungspflichten überschneiden; letztere werden unter dem Gesichtspunkt der Rechtswidrigkeit geprüft. Die diesbezüglichen Sorgfaltspflichten der Access- und Hosting-Provider sind für die Schweiz noch *nicht geklärt* [196]*.* In Bezug auf den Access-Provider ist offen, ob und gegebenenfalls wie weit die Kenntnis der von ihm zugänglich gemachten Inhalte verlangt werden kann. Beim Hosting-Provider steht in Frage, ob und gegebenenfalls in welchem Umfang ihn Kontroll- und Überwachungspflichten treffen, im Falle von deren Unterlassung er haftbar gemacht werden kann.

In der Literatur wird mehrheitlich hervorgehoben, dass Sorgfaltspflichten nur im Rahmen des *Zumutbaren und Möglichen* bestehen. Bei blosser Bereitstellung der technischen Infrastruktur für den Datentransport oder für den Netzzugang wird dem Dienstanbieter regelmässig keine Kenntnisnahme und Kontrolle der vermittelten Inhalte zugemutet (was die Verneinung einer Verschuldenshaftung der Netzwerkbetreiber und Access-Provider für fremde, rechtsverletzende Inhalte bedeutet). Dagegen wird die Zumutbarkeit der Kenntnisnahme und Prüfung von Fremdinhalten auf Rechtswidrigkeit durch den Hosting-Provider unterschiedlich beurteilt. Entweder wird von einer eingeschränkten Pflicht zur Kenntnisnahme von Fremdinhalten ausgegangen, oder es wird eine eingeschränkte inhaltliche Überprüfungspflicht angenommen.

Im Ergebnis tendiert die Lehre dahin, die *Haftung der Hosting-Provider zu begrenzen*, wobei danach differenziert wird, ob der Hosting-Provider weitere Aufgaben, wie etwa die Betreuung von Websites oder der Moderation von Newsgroups, übernimmt.

---

[195] Es ist umstritten, ob in Bezug auf die Tätigkeit des Hosting-Providers die Verletzungshandlung als positives Tun oder als Unterlassen zu werten sei.

[196] Siehe zum Meinungsstand in der Schweiz WEBER (Bibl.), S. 507 ff. (Access-Provider) und 515 ff. (Hosting-Provider), m.w.H.; PHILIPPE GILLIERON, La résponsabilité des fournisseurs d'accès et d'hébergement, ZSR NF Bd. 121/I, S. 387 ff., insbes. S. 430 ff. Siehe zum Meinungsstand in Europa ANDREA SCHMOLL: Die deliktische Haftung der Internet-Service-Provider: Eine rechtsvergleichende Untersuchung zu Deutschland, Frankreich, England und den USA, Frankfurt am Main 2001.

8.222 Verschuldensunabhängige Ansprüche

Der Anspruch auf Beseitigung oder Unterlassung setzt nur einen rechtswidrigen Eingriff in fremde Rechte voraus, erfordert also kein Verschulden. Für einen Beseitigungsanspruch genügt demnach, dass eine adäquat kausale Mitwirkung an der Rechtsverletzung und eine (zumutbare) Verhinderungsmöglichkeit gegeben sind. Folglich könnten Begehren auf Sperrung und/oder Löschung gegen Hosting- und Access-Provider durchgesetzt werden, wenngleich nur soweit, als die Sperrung oder Löschung technisch möglich und zumutbar ist. Bei der Beurteilung der Zumutbarkeit wird mit dem Schrifttum und der Rechtsprechung in Europa der *technische Aufwand ins Verhältnis zur Möglichkeit einer Umgehung* der Massnahme zu setzen sein.

Es stellt sich allerdings die *Frage*, ob jeder, der eine Teilursache in einer auf eine Rechtsverletzung hinauslaufenden Kausalkette setzt, passivlegitimiert und zur Beseitigung bzw. Verhinderung der Rechtsgutverletzung verpflichtet ist. Es findet sich daher auch in Bezug auf Unterlassungs- und Beseitigungsklagen das Postulat einer Beschränkung der Verantwortlichkeit für Access- und Hosting-Provider. Das wird zum Teil unter dem Stichwort der Adäquanz zu erreichen versucht. In Deutschland wird in diesem Zusammenhang auch auf die aus dem Verwaltungsrecht bekannte Figur des „Störers“ (vgl. oben Ziff. 5.12) zurückgegriffen. In der Schweiz hat diese Frage soweit ersichtlich bislang keine eingehende Erörterung erfahren.

8.23 Gesetzgeberischer Handlungsbedarf

Aus dem oben Gesagten geht hervor, dass die haftungsrechtliche Situation für Hosting- und Access-Provider in der Schweiz *unklar* ist, was sich negativ auf Investitionsentscheide dieser Wirtschaftsteilnehmer auswirken könnte. Auch wenn zu erwarten ist, dass die Rechtsprechung in der Schweiz über die Auslegung der allgemeinen Haftungsbestimmungen zu vertretbaren Lösungen gelangt, dürfte die Herausbildung von Leitregeln Jahre in Anspruch nehmen. Das Interesse an einer raschen Verwirklichung von Rechtssicherheit spricht daher dafür, dass die offenen Rechtsfragen vom Gesetzgeber beantwortet werden. Eine Klärung könnte entweder im Rahmen des *Bundesgesetzes über den elektronischen Geschäftsverkehr* oder im Zuge der Arbeiten zum *Bundesgesetz über die Revision und Vereinheitlichung des Haftpflichtrechts* (Haftpflichtgesetz) herbeigeführt werden [197].

Die Globalität des Internet verlangt nach *international vereinheitlichten Regeln* für die Verantwortlichkeit von Internet-Providern. Harmonisierungsbestrebungen, welche international eine unter zivil- und strafrechtlichen Gesichtspunkten kohärente Verantwortlichkeitsregelung herbeiführen, bestehen nicht. Es ist auch nicht binnen einer vertretbaren Zeitspanne mit einer internationalen Lösung zu rechnen. Dementsprechend rechtfertigt es sich vorderhand, den *nationalen Weg* zu beschreiten. Auch bei einer nationalen Regelung kann sich die Schweiz jedoch der

[197] Der Verfahrensstand beider Revisionsvorhaben ist unterschiedlich: In Bezug auf das Bundesgesetz über den *elektronischen Geschäftsverkehr* hat der Bundesrat das EJPD am 9. Dezember 2002 mit der Ausarbeitung einer Botschaft beauftragt. Vom Ergebnis des Vernehmlassungsverfahrens zum Vorentwurf eines Bundesgesetzes über die *Revision und Vereinheitlichung des Haftpflichtrechts* wird er im Laufe des Jahres 2003 Kenntnis nehmen. Diesem unterschiedlichen Projektstand wird im Zeitpunkt des Entscheids, in welches Vorhaben eine Regelung der Haftung von Hosting- und Access-Providern aufzunehmen ist, Rechnung zu tragen sein.

internationalen Dimension der Problemstellung nicht ganz verschliessen. Entsprechend sind die Lösungsansätze und Erfahrungen im Ausland zu berücksichtigen (vgl. oben Kapitel 4).

Die Art. 12 bis 15 der *E-Commerce-Richtlinie der EU* [198] können dabei einen ersten Ausgangspunkt für eine nationale Regelung bilden. Die ersten Erfahrungen mit dieser Richtlinie zeigen jedoch, dass speziell in Bezug auf Beseitigungs- und Unterlassungsansprüche ergänzende Regeln zu erlassen sind, welche die Fragen der Sperrungs- und Löschungsverpflichtungen gestützt auf das Zivilrecht klären. Schliesslich ist auch der Haftung für Links Beachtung zu schenken.

8.24 Koordination mit dem Strafrecht

Strafrechtliche Verantwortlichkeit und zivilrechtliche Haftung weisen im Zusammenhang mit der Netzwerkkriminalität verschiedene *Berührungspunkte* auf. Mit dem von der Expertenkommission vorgeschlagenen strafrechtlichen Lösungsansatz (vgl. unten Kapitel 9) werden Wertungen hinsichtlich der Verantwortlichkeit von Hosting- und Access-Providern vorgenommen, die jedenfalls auch für die verschuldensabhängigen Schadenersatzansprüche des Zivilrechts massgeblich sind. Dies betrifft zunächst die Beurteilung von allfälligen Kontroll- bzw. Überwachungspflichten. Sodann können Straftatbestände Schutznormen darstellen, die im Falle eines reinen Vermögensschadens die Rechtswidrigkeit begründen [199]. Darüber hinaus sind auch spezialgesetzlich geregelte, zivilrechtliche Verletzungstatbestände mit strafrechtlichen Sanktionen bewehrt. Hier stellt sich ganz konkret die Frage der Anwendung des Medienstrafrechts bzw. der nunmehr vorgeschlagenen Regelung auf Handlungen mittels elektronischer Kommunikationsnetze.

Die *strukturellen Unterschiede* zwischen beiden Rechtsbereichen müssen jedoch ebenfalls beachtet werden: Die Fahrlässigkeit spielt im Rahmen des Strafrechts im Zusammenhang mit den hier in Frage stehenden Delikten kaum eine Rolle. Insbesondere setzt die strafrechtliche Gehilfenschaft, welche als Basis zur Begründung einer möglichen Verantwortlichkeit der Internet-Provider für die von ihnen transportierten oder gespeicherten Informationen Dritter, immer wieder stark in den Vordergrund gerückt wird, den Vorsatz voraus. Die zivilrechtliche Gehilfenschaft gemäss Art. 50 OR ist jedoch auch fahrlässig möglich. Zu beachten ist ferner, dass der zivilrechtliche Verschuldensbegriff ein objektivierter ist. Dies hat zur Folge, dass insbesondere die Frage der Zumutbarkeit von allfälligen Gegenmassnahmen der Provider im Zivilrecht nach allgemeinen Massstäben und nicht nach den individuellen Voraussetzungen der einzelnen Provider geprüft wird. Vor allem geht die Frage nach der zivilrechtlichen Verantwortlichkeit im Zusammenhang mit den verschuldensunabhängigen zivilrechtlichen Ansprüchen auf Beseitigung und

---

[198] Richtlinie 2000/31/EG des Europäischen Parlaments und des Rates über den elektronischen Geschäftsverkehr vom 8.6.2000 (sog. „E-Commerce-Richtlinie“, vgl. oben Kapitel 4).

[199] Nach bundesgerichtlicher Rechtsprechung (siehe etwa BGE 119 II 127 E. 3) und herrschender Lehre liegt der Haftungsnorm des Art. 41 OR die objektive Widerrechtlichkeitstheorie zugrunde. Danach ist eine Schadenszufügung widerrechtlich, wenn sie gegen eine allgemeine gesetzliche Pflicht verstösst, indem entweder ein absolutes Recht des Geschädigten beeinträchtigt (Erfolgsunrecht) oder eine reine Vermögensschädigung durch Verstoss gegen eine einschlägige Schutznorm bewirkt wird (Verhaltensunrecht).

Unterlassung über die das Verschulden voraussetzende strafrechtliche Fragestellung hinaus.

Eine *Querschnittsregelung*, welche sowohl das Straf- als auch das Zivilrecht umfasst, erweist sich angesichts der Differenzen ebenso wenig als zwingend wie ein zeitlich paralleles Vorgehen. Die vertieft zu führende dogmatische Auseinandersetzung bei der Ausarbeitung eines konkreten Lösungsvorschlags im Bereich der zivilrechtlichen Haftung, der an Art. 50 OR ansetzen müsste, spricht vielmehr für getrenntes Vorgehen in den beiden Rechtsbereichen.

8.3 Vertragliche Haftung von Access- und Hosting-Providern

Die Beurteilung der vertraglichen Haftung von Internet-Providern [200] weist nur in eingeschränktem Masse einen Zusammenhang mit der strafrechtlichen Fragestellung auf: Ein solcher besteht namentlich dann, wenn ein Internet-Provider angesichts einer möglichen strafrechtlichen Verantwortlichkeit aus eigener Veranlassung oder in Befolgung einer von Strafverfolgungsbehörden erlassenen Sperr- oder anderen Massnahmeverfügung vertraglich geschuldete Leistungen nicht oder nicht gehörig erbringen kann. Sachgerechte Lösungen lassen sich in diesen Fällen allerdings auf der Grundlage vertraglicher Abreden und des geltenden Rechts (Art. 97 OR) finden [201]. Insbesondere wenn die Leistungsstörung etwa auf einem hoheitlichen Akt (z.B. einer Sperrverfügung) beruht, ist sie nicht vom Schuldner zu vertreten. Anders wäre insbesondere zu entscheiden, wenn dem Provider als Schuldner der Vorwurf gemacht werden könnte, übliche und zumutbare technische Massnahmen unterlassen zu haben, die eine Sperrung des betreffenden Informationsmaterials ohne Beeinträchtigung seiner Leistungspflichten ermöglicht hätten.

Soweit Berührungspunkte zwischen der Thematik der vertraglichen Haftung und der strafrechtlichen Fragestellung bestehen, erfordern sie nach Ansicht der Expertenkommission keine Intervention des Gesetzgebers im Obligationenrecht.

8.4 Schlussfolgerungen der Expertenkommission

Die Expertenkommission erkennt für die Frage der ausservertraglichen Haftung von Internetdienste-Anbietern, namentlich von Access- und Hosting-Providern, die Notwendigkeit einer Klärung durch den Gesetzgeber. Einer vertieften Auseinandersetzung bedarf dabei die Frage der Passivlegitimation von Access- und Hosting-Providern bei Unterlassungs- und Beseitigungsklagen.

Nach Ansicht der Expertenkommission könnten diese Fragen entweder im Rahmen des *Bundesgesetzes über den elektronischen Geschäftsverkehr* oder im Zuge der Arbeiten zum *Bundesgesetz über die Revision und Vereinheitlichung des*

---

[200] Siehe zur vertraglichen Haftung im allgemeinen WEBER (Bibl.), S. 511 ff. (Access-Provider) und 521 ff. (Hosting-Provider), m.w.H.

[201] MARKUS H. BERNI: Die zivil- und strafrechtliche Verantwortung des ISP, in: Hans Rudolf Trüeb (Hrsg.), Aktuelle Rechtsfragen des E-Commerce, Zürich 2001, S. 117 ff., 134, weist eine Haftung unter Berufung auf Art. 20 OR generell zurück.

Haftpflichtrechts (Haftpflichtgesetz) einer positiven Regelung zugeführt werden. Dabei sollte die E-Commerce-Richtlinie der EU Ausgangspunkt bilden; eine nationale schweizerische Regelung hat freilich auch diejenigen wesentlichen Fragen zu beantworten, welche in der EU-Richtlinie dem Gesetzgeber der Mitgliedstaaten vorbehalten worden sind.

9. Vorschläge der Expertenkommission

Vorgeschlagener Gesetzestext (Änderung des Strafgesetzbuches)

(neuer Titel) 6. Strafbare Handlungen in elektronischen Kommunikationsnetzen und in Medien

(neu) Art. 27 StGB ***Strafbare Handlungen in elektronischen Kommunikationsnetzen***

1. Wird eine strafbare Handlung mittels Übertragung, Bereitstellen oder Bereithalten von Informationen in einem elektronischen Kommunikationsnetz begangen, so gelten unter Vorbehalt der nachfolgenden Bestimmungen die allgemeinen Regeln.

2. Ist der Täter Autor oder Redaktor im Sinne von Art. 27bis, so richtet sich die Strafbarkeit nach dieser Bestimmung.

3. Wer fremde Informationen zur Nutzung in einem elektronischen Kommunikationsnetz automatisiert bereithält, macht sich unter den Voraussetzungen von Art. 322bis Ziff. 1 strafbar. Das Bereithalten eines Verzeichnisses, in welches fremde Informationen automatisiert aufgenommen werden, gilt als Bereithalten fremder Informationen.

4. Wer lediglich den Zugang zu einem elektronischen Kommunikationsnetz vermittelt, ist nicht strafbar. Eine automatische und kurzzeitige Speicherung fremder Informationen infolge Nutzerabfrage gilt als Zugangsvermittlung.

(neu) Art. 27bis StGB ***Strafbare Handlungen in Medien***

[1] Wird eine strafbare Handlung durch Veröffentlichung in einem Medium begangen und erschöpft sie sich in dieser Veröffentlichung, so ist, unter Vorbehalt der nachfolgenden Bestimmungen, der Autor allein strafbar.

[2] Kann der Autor nicht ermittelt oder in der Schweiz nicht vor Gericht gestellt werden, so ist der verantwortliche Redaktor nach Artikel 322bis Ziff. 2 strafbar. Fehlt ein verantwortlicher Redaktor, so ist jene Person nach Artikel 322bis Ziff. 2 strafbar, die für die Veröffentlichung verantwortlich ist.

[3] Hat die Veröffentlichung ohne Wissen oder gegen den Willen des Autors stattgefunden, so ist der Redaktor oder, wenn ein solcher fehlt, die für die Veröffentlichung verantwortliche Person als Täter strafbar.

[4] Die wahrheitsgetreue Berichterstattung über öffentliche Verhandlungen und amtliche Mitteilungen einer Behörde ist straflos.

Art. 27bis StGB wird unverändert zu (neu) Art. 27ter StGB *Quellenschutz*

(neu) Art. 322bis StGB *Nichtverhindern strafbarer Handlungen in elektronischen Kommunikationsnetzen und in Medien*

(neu) 1. Wer in einem elektronischen Kommunikationsnetz fremde Informationen automatisiert bereithält, mittels deren, wie er sicher weiss, eine strafbare Handlung begangen wird, und es unterlässt, die Nutzung dieser Informationen zu verhindern, obwohl es ihm technisch möglich und zumutbar ist, wird mit Gefängnis oder Busse bestraft.

Wer in einem elektronischen Kommunikationsnetz fremde Informationen automatisiert bereithält, mittels deren eine strafbare Handlung begangen wird, und es unterlässt, von Dritten an ihn gerichtete und bei ihm eingegangene Hinweise auf solche Informationen an die Strafverfolgungsbehörden weiterzuleiten, wird mit Gefängnis oder Busse bestraft.

Handelt es sich bei der strafbaren Handlung im Sinne der Abs. 1 und 2 um ein Antragsdelikt, so wird die Tat nur verfolgt, wenn ein Antrag auf Verfolgung der strafbaren Handlung vorliegt.

Ob mittels einer Information eine strafbare Handlung im Sinne der Abs. 1 und 2 begangen wird, beurteilt sich nach schweizerischem Recht.

Informationen im Sinne der Abs. 1 und 2 werden ungeachtet schweizerischer Strafhoheit gelöscht.

(abgeänderter Text von Art. 322bis) 2. Wer als Verantwortlicher nach Artikel 27bis Absätze 2 und 3 eine Veröffentlichung, durch die eine strafbare Handlung begangen wird, vorsätzlich nicht verhindert, wird mit Gefängnis oder Busse bestraft. Handelt der Täter fahrlässig, so ist die Strafe Haft oder Busse.

(neu) Art. 340ter StGB *Bei strafbaren Handlungen in elektronischen Kommunikationsnetzen*

1 Der Bundesgerichtsbarkeit unterstehen zudem strafbare Handlungen mittels elektronischer Kommunikationsnetze, wenn:
a. mehrere Kantone von der strafbaren Handlung betroffen sind und kein eindeutiger Schwerpunkt in einem Kanton besteht; oder
b. ein koordiniertes Ermittlungsverfahren in mehreren Kantonen notwendig ist.

2 Die Bundesanwaltschaft kann ausserdem ein Ermittlungsverfahren eröffnen, wenn eine zuständige kantonale Strafverfolgungsbehörde sie um Übernahme des Verfahrens ersucht.

3 Die Eröffnung des Ermittlungsverfahrens gemäss Absatz 2 begründet Bundesgerichtsbarkeit.

Nötige Anpassungen aufgrund obiger Vorschläge

Art. 347 StGB

[1] Bei einer strafbaren Handlung im Inland nach Artikel 27bis sind die Behörden des Ortes zuständig, …

Art. 18bis Bundesstrafrechtspflege (BStP, SR 312.0)

[1] Der Bundesanwalt kann eine Bundesstrafsache nach Artikel 340 Ziffer 2, Artikel 340bis und Artikel 340ter des Strafgesetzbuches nach Abschluss der Voruntersuchung der kantonalen Behörde zur Beurteilung übertragen. Er führt in diesem Fall die Anklage vor dem kantonalen Gericht.
[2] (unverändert)
[3] (unverändert)

Art. 26 Strafgerichtsgesetz (SGG, noch nicht in Kraft)

Die Strafkammer beurteilt:
a. Strafsachen, die nach den Artikeln 340, 340bis und 340ter des Strafgesetzbuches der Bundesstrafgerichtsbarkeit unterstehen, soweit der Bundesanwalt die Untersuchung und Beurteilung nicht den kantonalen Behörden übertragen hat;
b. …

9.1 Regelungskonzept der Expertenkommission und Kommentar zur vorgeschlagenen Neuregelung

9.11 Allgemeines zur Regelung der Verantwortlichkeit

Die zunehmende Durchlässigkeit unter den verschiedenen elektronischen Kommunikationsnetzen und der schnelle technische Wandel in der Informations- und Netzwerktechnologie legen es nahe, sich bei der Eingrenzung des Regelungsbereiches der Netzwerkkriminalität nicht auf die Begriffe „Internet“ und die TCP/IP-basierte Datenübertragung festzulegen 202.

Eine konsistente Regelung der Internet-Sachverhalte muss ausserdem die sich überschneidenden Bereiche der Kommunikations-, Informations- und Mediendienste erfassen, sich folglich auf die Kommunikationsträger und -inhalte beziehen. Für eine solche gesetzliche Regelung bieten sich verschiedene *Lösungsansätze* an (siehe unten Ziff. 9.12) 203.

9.12 Horizontalregelung oder bereichsspezifische Regelung?

9.121 Horizontalregelung für alle Rechtsgebiete

Der Gesetzgeber könnte in einem separaten Erlass eine Haftungs- bzw. Strafbarkeitsregelung für alle Beteiligten festlegen. Diese wäre gleichermassen für das Strafrecht, das Haftpflichtrecht, das Urheberrecht, das Wettbewerbsrecht usw. verbindlich. Einen solchen Weg hat beispielsweise Deutschland mit dem *Teledienstegesetz* (TDG) vom 22. Juli 1997 204 eingeschlagen. Auch die *EU-Richtlinie über den elektronischen Geschäftsverkehr* 205 geht grundsätzlich von einer einheitlichen „Verantwortlichkeitsregelung“ aus. Eine Horizontalregelung könnte aber auch in einem bestehenden Gesetz untergebracht werden. In der Schweiz wurde etwa vorgeschlagen, eine alle Rechtsbereiche abdeckende Ausscheidung der Haftung bzw. Strafbarkeit im *Fernmeldegesetz* (FMG, SR 784.10) vorzunehmen.

Dem Vorteil einer Horizontalregelung, der darin bestehen soll, mit einem eigenständigen Gesetz alle öffentlich- und zivilrechtlichen Haftungs- sowie Strafbarkeitsfragen zu klären, stehen gewichtige Nachteile gegenüber. Insbesondere bietet ein solches „Gesetz neben dem Gesetz“ erhebliche Integrationsprobleme in das System der Haftungs- bzw. Strafbarkeitsvoraussetzungen der bestehenden Gesetze (StGB, OR).

---

202 Zur näheren Begründung, s. oben Ziff. 2.44.

203 Hierzu NIGGLI/SCHWARZENEGGER (Bibl.), S 63 und 66 ff.

204 Revidiert durch das Gesetz über die rechtlichen Rahmenbedingungen für den elektronischen Geschäftsverkehr (EGG), in Kraft seit 22.12.2001, vgl. BGBl. I 2001 S. 3721. Die Verantwortlichkeits-regelung findet sich in den §§ 8–11 TDG (neue Fassung) ; vgl. oben Kapitel 4, Ziff. 4.31.

205 Vgl. Art. 12 ff. E-Commerce-Richtlinie, vgl. oben Kapitel 4.

Im Verhältnis zum dortigen StGB ist in *Deutschland* beispielsweise strittig, wie die §§ 8 ff. TDG in den Stufenaufbau der Strafbarkeit einzuordnen seien 206. Mit Horizontalbegriffen wie „Kenntnis“ oder „Verantwortlichkeit“ wird sowohl im Zivilrecht als auch im Strafrecht vom vertrauten Begriffsinstrumentarium abgewichen, was zusätzliche Auslegungsprobleme hervorruft. Bei anderen Fragen, wie z.B. derjenigen nach der Strafbarkeit für Link-Verweise auf strafbare Inhalte, schuf die Horizontalregelung des deutschen Teledienstegesetzes (insbes. § 5 TDG a.F.) zusätzliche Verwirrung 207. Selbst wenn man sich an den Vorgaben der E-Commerce-Richtlinie orientiert, ist dies nicht notwendigerweise mit einer Horizontalregelung verbunden.

In *Frankreich* kam es im Jahr 2000 zu einer wichtigen Abänderung der Strafbarkeitsvoraussetzungen für Provider. In das Gesetz über die Kommunikationsfreiheit wurde in Art. 43-8 Abs. 1 das Prinzip der sogenannten eingeschränkten Verantwortlichkeit eingefügt. Diesem Prinzip zufolge ist der Hosting-Provider nur dann strafbar, wenn er nach einer richterlichen Notifikation nicht sofort den Zugang zur inkriminierten Webseite sperrt. Mit dieser Regelung scheint auch klar, dass jegliche Strafbarkeit von Access-Providern dahinfällt. Im Gesetzesentwurf war noch eine strengere Ergänzung von Art. 43-8 vorgesehen. Art. 43-8 Abs. 2 des Entwurfes hielt fest, dass eine Strafbarkeit auch dann entstehen könnte, wenn der Hosting-Provider von einem Nutzer informiert würde und darauf nicht reagiere. Dieser Satz wurde aber vom Conseil constitutionel mangels Bestimmtheit als verfassungswidrig erklärt. Er bezog sich dabei einzig auf die Voraussetzungen der Strafbarkeit, denn nach französischem Strafrecht setzt die Gehilfenschaft einen direkten Vorsatz voraus. Eine eventualvorsätzliche Begehung, die durch die Formulierung von Art. 43-8 Abs. 2 des Entwurfes erfasst worden wäre, gibt es im Rahmen der Vorsatzdelikte nicht 208. Ein erster Gesetzesvorschlag vom 14. Juni 2001 zur Umsetzung der E-Commerce-Richtlinie sah deswegen nur noch eine bereichsspezifische Haftungsbeschränkung für das Zivilrecht vor 209.

---

206 Eine Modifikation des Allgemeinen Teils des StGB durch ausserstrafrechtliche Erlasse ist bisher unbekannt, weshalb die vermeintliche Klarheit der Horizontalregelung zu neuen Problemen und völlig konträren Meinungen im strafrechtlichen Schrifttum geführt hat (Vorfilterlösung, tatbestandsmodifizierender Ansatz, Rechtfertigungsansatz, Schuldausschluss, Strafbefreiungsgrund, Nachfilterlösung). Vgl. dazu NIGGLI/SCHWARZENEGGER (Bibl.), S. 66 f.

207 Zusammenfassend CHRISTIAN SCHWARZENEGGER: Die strafrechtliche Beurteilung von Hyperlinks, in: Festschrift Rehbinder, München 2002, S. 723 ff. m.w.N.; selbst nach der klareren neuen Fassung des TDG setzt sich diese Desorientierung fort, s. etwa HENNING ROSENAU / LARS WITTECK, Der Castor-Transport und die Hakenkralle im Internet, JURA 2002, 781 ff.

208 Loi du 1er août 2000 relative à la communication (loi no 2000-719 du 1er août 2000, modifiant la loi no 86-1067 du 30 septembre 1986 relative à la liberté de communication, JO du 2 août 2000, 11903). Wortlaut von Artikel 43-8 dieses Gesetzes, vgl. oben Ziff. 4.33. Vgl. Conseil constitutionnel, Décision no 2000-433 DC du 27 juillet 2000, JO du 2 août 2000, 11922 ff., insbesondere 11926. Hierzu näher MOREILLON/DE COURTEN, (Bibl.), S.12 m.N.

209 Siehe Projet de loi sur la société de l'information, enregistré à la Présidence de l'Assemblée nationale le 14 juin 2001. Nach dem Regierungswechsel wurde dieses Gesetzgebungsvorhaben nicht weiterverfolgt. In der Zwischenzeit legte das Ministerium für Industrie am 15. Januar 2003 einen neuen Gesetzesentwurf (Projet de loi pour la confiance dans l´économie numérique) vor, der im Gesetz über die Kommunikationsfreiheit (loi n° 86-1067 du 30 septembre 1986 relative à la liberté de communication) zwei unabhängige Normen für die zivilrechtliche Haftung und die Strafbarkeit der Hosting-Provider vorsieht (neu Art. 43-8 bzw. Art. 43-9). Die Haftungsfreistellung und Straflosigkeit des Access-Providers für automatisierte Zugangsvermittlung wird neu im Code des postes et télécommunications verankert (neu Art. L. 32-3-3). In *Japan* wurde eine bereichsspezifische Regelung

Eine Horizontalregelung in einem eigenständigen „Internet-Verantwortlichkeitserlass“ erscheint der Expertenkommission vor diesem Hintergrund *nicht erstrebenswert*.

Im übrigen griffe eine Horizontalregelung im Fernmeldegesetz zu kurz, weil der Begriff des Fernmeldedienstes nur die Zugangsvermittlung zur Nutzung von Informationen (vgl. Art. 3 FMG) erfasst, nicht aber das Bereitstellen oder -halten zum Zwecke der fernmeldetechnischen Übertragung. Entsprechend blieben die strafrechtsdogmatischen Probleme im Zusammenhang mit dem Hosting wie bis anhin unklar, und die Rechtsunsicherheit bliebe bestehen. Ausserdem sieht Art. 2 FMG eine Ausnahme für Programme i.S. des Radio- und Fernsehgesetzes (RTVG, SR 784.40) vor, worunter wohl auch Internetradio und –fernsehen fielen. Schliesslich erstreckt sich das FMG nur auf Kommunikationsdienste, nicht aber auf Informations- und Mediendienste 210. Auch dieser Regelungskontext erscheint der Expertenkommission daher inadäquat.

9.122 Bereichsspezifische Regelung in den jeweiligen Rechtsgebieten

Die Expertenkommission tritt demnach für eine bereichsspezifische Lösung ein; dabei räumt sie der Anpassung des StGB erste Priorität ein. Dieser Ansatz ermöglicht einerseits die systemimmanente Anpassung der Strafbarkeitsvoraussetzungen, welche weder in den Tatbestandsaufbau noch in die herkömmliche fachspezifische Begrifflichkeit eingreift.

Das Strafrecht regelt mehrheitlich ganz andere Problemfelder als das Zivilrecht. Denn viele der netzwerkbezogenen Straftaten schützen Allgemeininteressen, bei denen keine Einzelpersonen als Geschädigte auftreten, und stellen schon die Gefahrschaffung für ein Rechtsgut unter Strafe. Andererseits steht dieser Ansatz einer dogmatisch stimmigen und die spezifischen Parteiinteressen berücksichtigenden Anpassung der zivilrechtlichen Haftungsvoraussetzungen nicht im Wege. Das Ziel, eine berechenbare und beständige Rechtslage in Kommunikationsnetzen zu schaffen, ist mit diesem schrittweisen Vorgehen eher zu erreichen.

9.13 Drei Eckpfeiler der neuen Regelung

- Über die Grenzen der Strafbarkeit von Infrastrukturanbietern für automatisiert ablaufende Prozesse soll im Bereich der elektronischen Kommunikationsnetze Klarheit geschaffen werden. Beschränkt sich die Beteiligung der Access-Provider auf die reine Zugangsvermittlung, soll diese straflos bleiben. Bei den Hosting-Providern ist zu differenzieren zwischen dem Regelfall der automatisiert ablaufenden Datentransfers, von denen sie nichts wissen, und den Fallkonstellationen, in denen sie nachträglich die (mögliche) Strafbarkeit solcher Handlungen erkennen. Im ersten Fall sind sie nicht strafbar, im zweiten Fall dagegen schon, falls sie nichts unternehmen. Darüber besteht international weitgehend Konsens.

---

eingeführt, s. Law concerning limitation of damages to specific telecommunications service provider and disclosure of sender information, passed on November 22, 2001.

210 NIGGLI/SCHWARZENEGGER (Bibl.), S. 68.

- Damit wird das Problem der „neutralen Handlungen“ sektoriell entschärft (vgl. hierzu oben Ziff. 6.3). Den Infrastrukturanbietern im Bereiche der elektronischen Kommunikationsnetze werden einheitliche und kalkulierbare strafrechtliche Rahmenbedingungen gesetzt.

- Die neue Regelung soll weiter präzise Abgrenzungskriterien zwischen Medien- und Netzwerkstrafrecht formulieren. Einerseits soll die bestehende Privilegierung für Massenmedien bei Kommunikation in Netzwerken beibehalten werden, andererseits sollen aber ausserhalb dieses Sonderstrafrechts für alle Sachverhalte klare Lösungen vorgezeichnet werden.

9.2 Kommentar zu (neu) Art. 27 StGB [211]

9.21 Titel des 6. Abschnitts: „Strafbare Handlungen in elektronischen Kommunikationsnetzen und in Medien“

Bei der Begriffsbildung hat sich die Expertenkommission von folgenden *Prämissen* leiten lassen:

- Die Spezialregelung der strafrechtlichen Verantwortlichkeit soll sich *nicht nur auf das Internet* beziehen (vgl. oben Kapitel 2, Ziff. 2.24, 2.4 – 2.6);
- sie ist insofern *technologieneutral*, als es keine Rolle spielt, ob die fraglichen Informationen über Leitungen oder drahtlos übertragen werden und welche Übertragungsinfrastruktur verwendet wird (Telefonleitungen, Stromleitungen usw.);
- die privilegierende Strafbarkeitsregelung *knüpft nicht an die Veröffentlichung* (Publikation) an [212]. Sie erfasst also grundsätzlich auch strafbare Inhalte in E-Mails.
- die privilegierende Strafbarkeitsregelung erfasst nicht nur Gedankenäusserungsdelikte, sondern *sämtliche* durch die Übermittlung, das Bereitstellen oder Bereithalten von Informationen in Telekommunikationsnetzen begangenen Straftaten;
- für die Regelung spielt es *keine Rolle*, ob die Informationen einseitig (wie z.B. im Rahmen traditioneller Radio- und Fernsehsendungen) oder interaktiv zugänglich sind, d.h. auf zweiseitigem Datenaustausch basieren (wie z.B. beim Telefongespräch oder dem Versenden und Empfangen elektronischer Post). Auch die Einweg-Kommunikation wird erfasst. Unter die vorgesehene Regelung fällt damit beispielsweise auch die Verbreitung von Radio- und

---

211 Die *Kommentierung* der vorgeschlagenen Neuregelung erstreckt sich über die Ziff. 9.2 (Art. 27 StGB), 9.3 (neu Art. 322bis StGB) und Ziff. 9.4 (neu Art. 340bis StGB) - „Art. 27 StGB“ bezeichnet den Art. 27 des StGB in der heute geltenden Fassung (also das Medienstrafrecht); wo auf unseren Revisionsentwurf Bezug genommen wird, ist dies mit „(neu) Art. 27 StGB“ gekennzeichnet. Bei den anderen vorgeschlagenen neuen Vorschriften wird analog verfahren.

212 So der bisherige Artikel 27 Absatz 1 StGB, welcher damit die Individualkommunikation ausschliesst. Das Merkmal der Veröffentlichung setzt nach der bundesgerichtlichen Rechtsprechung voraus, dass der fragliche Inhalt für die Veröffentlichung bestimmt ist und nicht nur an individuell festgelegte Personen abgegeben wird (BGE 125 IV 177, 183 f.).

Fernsehprogrammen über herkömmliche Kabelnetze oder künftig im Rahmen des digitalen Fernsehens (Digital Video Broadcasting, DVB) oder Radios (Digital Audio Broadcasting, DAB) [213].

Als *Klammerbegriff*, der alle erwähnten Bereiche umschreiben kann, kommen folgende drei Bezeichnungen in Frage:

9.211 Strafbare Handlungen „in einem Telekommunikationsnetz“

Dieser Begriff findet sich bislang im schweizerischen Recht nicht. *Ziel* ist es, folgende Phänomene zu erfassen, welche durch das FMG (möglicherweise) nicht abgedeckt sind:

- das Bereitstellen und Bereithalten von Informationen (nicht nur deren Übertragung [214]);
- das Erfassen von Programmen im Sinne des RTVG [215];
- das Erfassen von Informations- und Mediendiensten (nicht bloss von Kommunikationsdiensten).

Diese Terminologie hat *einerseits* den Nachteil, dass sie nicht an bestehende Definitionen anknüpft, was einen gewissen Argumentationsaufwand sowohl im Gesetzgebungsverfahren als auch bei der Rechtsanwendung notwendig machen dürfte. *Andererseits* ist der Begriff der Telekommunikation ursprünglich mit Individualkommunikation wie der Telegrafie oder der Telefonie verknüpft und wurde teilweise auch von einseitig übertragenen Radio- und Fernsehprogrammen abgegrenzt (Rundfunk einerseits und Telekommunikation anderseits werden in der Diskussion regelmässig als voneinander abgetrennte Gebiete verstanden). Dass der Begriff „Telekommunikationsnetze“ auch die Einwegkommunikation sowie die Massenkommunikation erfasst, ist zumindest nicht offensichtlich.

9.212 Strafbare Handlungen „mittels fernmeldetechnischer Übertragung oder Bereithaltung von Informationen“

Diese in enger Anlehnung an die Terminologie des Fernmeldegesetzes gehaltene Formulierung erfasst nicht nur das Übertragen, sondern auch das Bereithalten von Informationen, hat aber zwei Nachteile. Erstens ist sie sprachlich umständlich, und zweitens könnte sie Verwirrung stiften, weil der Begriff der Fernmeldetechnik oft mit Telefonie gleichgesetzt wird. Aus der Formulierung wird nicht deutlich, dass auch Radio- und Fernsehprogramme erfasst sind, welche Art. 2 FMG aus dem

---

[213] Es ist darauf hinzuweisen, dass im Bereiche der Einweg-Kommunikation gegenwärtig die Funktion des Hosting-Providers nicht existiert. Gleichwohl ist die Klärung der Strafbarkeitsvoraussetzungen auch hier gültig: Inhalteanbieter sollen grundsätzlich nach den allgemeinen Regeln behandelt, reine Informationsdurchleiter dagegen von der Strafbarkeit für die Informationen ausgenommen werden.

[214] Art. 2 FMG knüpft an die „fernmeldetechnische Übertragung“ von Informationen an.

[215] Sie sind gemäss Art. 2 vom FMG nicht erfasst.

Regelungsbereich des FMG ausschliesst. Die Erfassung von Radio- und Fernsehprogrammen müsste daher zusätzlich explizit geregelt werden [216].

9.213 Strafbare Handlungen „in elektronischen Kommunikationsnetzen“

Dieser Begriff ist sehr breit und bringt den Vorzug mit sich, dass er an eine bestehende Terminologie des EU-Rechts anknüpft. Eine *Definition* des Begriffs des elektronischen Kommunikationsnetzes findet sich in Art. 2 Bst. a der EU-Rahmenrichtlinie für elektronische Kommunikationsnetze und -dienste vom März 2002 [217]:

> „Elektronisches Kommunikationsnetz“: Übertragungssysteme und gegebenenfalls Vermittlungs- und Leitwegeinrichtungen sowie anderweitige Ressourcen, die die Übertragung von Signalen über Kabel, Funk, optische oder andere elektromagnetische Einrichtungen ermöglichen, einschliesslich Satellitennetze, feste (leitungs- und paketvermittelte, einschliesslich Internet) und mobile terrestrische Netze, Stromleitungssysteme, soweit sie zur Signalübertragung genutzt werden, Netze für Hör- und Fernsehfunk sowie Kabelfernsehnetze, unabhängig von der Art der übertragenen Informationen.“

Der letztgenannte Begriff fängt alle einzubeziehenden Netzwerkfunktionen am treffsichersten ein. Der Titel des 6. Abschnittes ist folglich zu ergänzen und lautet neu: „Strafbare Handlungen in elektronischen Kommunikationsnetzen und in Medien.“

Die Ungenauigkeit, die durch die Wendung „*in* elektronischen Kommunikationsnetzen“ entsteht, ist hinzunehmen. Denn der Titel soll eine begriffliche Klammer bilden sowohl für Straftaten, die mittels elektronischen Kommunikationsnetzen begangen werden, als auch für Mediendelikte, die sich in der Publikation erschöpfen müssen. Eine Präzisierung erfolgt in (neu) Art. 27 Ziff. 1, wo von „strafbaren Handlungen mittels Übertragung, Bereitstellen oder Bereithalten” gesprochen wird [218].

9.22 (neu) Art. 27 Ziff. 1 StGB (Content-Provider)

9.221 „Strafbare Handlung mittels …“.

Die Formulierung „strafbare Handlung mittels“ hat einen weiteren Bedeutungsgehalt als „strafbare Handlungen in“ und soll alle Taten erfassen, die mit der Übertragung,

---

[216] Dies gilt zumindest bis zur Totalrevision des RTVG, welche im Rahmen der Verbreitung auch eine Änderung von Art. 2 FMG bringen wird. Künftig soll für die Verbreitung von Radio- und Fernseh-programmen auf das Fernmelderecht abgestellt werden; vgl. die Botschaft des Bundesrates vom 18. Dezember 2002 zur Totalrevision des Radio- und Fernsehgesetzes, BBl 2003 1659f.

[217] Richtlinie 2002/21/EG des Europäischen Parlaments und des Rates vom 7. März 2002 über einen gemeinsamen Rechtsrahmen für elektronische Kommunikationsnetze und -dienste (Rahmenrichtlinie) Amtsblatt Nr. L 108 vom 24/04/2002 S. 33 ff.; abrufbar unter: www.europa.eu.int/smartapi/cgi/sga_doc?smartapi!celexapi!prod!CELEXnumdoc&lg=DE&numdoc=32002L0021&model=guichett (Stand: 9.4.2003).

[218] Die Straftaten spielen sich nur z.T. „im“ Netz ab. Möglich ist auch, dass das Netz bloss Mittel zum Zweck ist und gar nur am Rande eine Rolle spielt (z.B. Betrug).

Bereitstellung oder Bereithaltung von Informationen in elektronischen Kommunikationsnetzen zu tun haben. Die Regelung strebt mithin an, über denjenigen Bereich hinauszugehen, der üblicherweise als Paradebeispiel für Internet-Kriminalität angeführt wird, namentlich den Bereich der sog. Äusserungsdelikte (Gewaltdarstellungen, harte Pornographie, Rassendiskriminierung, Ehrverletzungen usw.).

Zwar soll dieser Bereich durchaus von der Regelung erfasst sein, doch soll deren Anwendungsbereich *nicht darauf beschränkt* bleiben. Vielmehr sollen z.B. die sog. Computerdelikte ebenfalls unter die Regelung fallen, also etwa das Verbreiten von Computerviren (Art. 144bis Ziff. 2 StGB). Von der Regelung erfasst werden sollen zudem alle "traditionellen" Delikte (z.B. Vermögensdelikte wie Betrug, Art. 146 StGB, oder der betrügerische Missbrauch einer Datenverarbeitungsanlage, Art. 147 StGB; aber auch die Delikte des Nebenstrafrechts, v.a. jene im Zusammenhang mit dem unlauteren Wettbewerb oder dem Markenschutz; vgl. die Liste oben in Ziff. 2.2).

9.222 Übertragung, Bereitstellen, Bereithalten

Von der Regelung des (neu) Art. 27 StGB werden *drei* aus netzwerkspezifischer Sicht *grundlegende Operationen* erfasst. Diese sind:

- Das Übertragen i.S. eines elektrischen, magnetischen, optischen oder anderen elektromagnetischen Sendens oder Empfangens von Informationen über Leitungen oder Funk.
- Das Bereitstellen i.S. eines Aufladens von Informationen auf ein öffentliches, durch elektronische Kommunikationsnetze zugängliches Speichermedium.
- Das Bereithalten i.S. eines Unterhaltens eines öffentlichen, durch elektronische Kommunikationsnetze zugänglichen Speichermediums, auf dem Informationen abgespeichert sind.

Das letzte Glied im Kommunikationsprozess, das *Abrufen*, wird in der Regel von einem *Nutzer* vorgenommen, der sich dadurch noch nicht strafbar macht (möglich ist dies aber bei Abspeicherung auf einem lokalen Medium, vgl. Art. 197 Ziff. 3bis StGB).

9.223 Informationen

„Informationen" ist ein breiter Begriff, der insbesondere auch Computerprogramme einschliesst [219]. Damit ist der Gesetzesvorschlag nicht auf „Äusserungsdelikte" im Internet beschränkt [220], sondern geht weiter: Er will auch eine Regelung der Verantwortlichkeit für die Computerkriminalität [221] und urheberstrafrechtliche Delikte [222] treffen.

---

[219] Vgl. die Legaldefinition in Art. 3 lit. a FMG: „Informationen: für Menschen, andere Lebewesen oder Maschinen bestimmte Zeichen, Signale, Schriftzeichen, Bilder, Laute und Darstellungen jeder anderen Art;"

[220] Z.B. Gewaltdarstellungen Art. 135, Pornographie Art. 197, Rassendiskriminierung Art. 261bis StGB.

[221] Z.B. Bereithalten von Computer-Viren, Art. 144bis StGB; betrügerische Angebote auf dem WWW, Art. 146 StGB.

[222] Z.B. Musikpiraterie, Art. 67 und 69 URG.

Die Expertenkommission hat auch den Begriff der *rechtswidrigen Inhalte* erwogen, ihn aber verworfen. Er deckt nicht den gesamten Bereich der zu erfassenden Informationen ab; so sind etwa im Falle von betrügerischen oder urheberstrafrechtswidrigen Angeboten auf dem WWW nicht diese Inhalte als solche rechtswidrig, sondern deren Verwendung. Zudem ist der Begriff der rechtswidrigen Inhalte in seiner Reichweite umstritten. Deshalb gebraucht der Entwurf konsequent den Terminus „Informationen“. Dieser wird ebenfalls im FMG sowie auch in der E-Commerce-Richtlinie verwendet. Darunter sind auch illegale Inhalte zu verstehen.

9.224 Geltung der allgemeinen Regeln

Der Vorschlag statuiert in (neu) Art. 27 Ziff. 1, dass grundsätzlich die allgemeinen Regeln auch für strafbare Handlungen in einem elektronischen Kommunikationsnetz gelten. Dies mag überflüssig erscheinen, ergibt sich aber aus der vorgeschlagenen Struktur der Strafbarkeit. Diese ist so angeordnet, dass Ausnahmen (elektronische Kommunikationsnetze; Medienstrafrecht) zu den allgemeinen Regeln statuiert werden. Die vorgeschlagene Regelungsstruktur ist *dreistufig-hierarchisch*:

- Grundsätzlich sollen die allgemeinen Regeln gelten.
- Gegenüber diesen allgemeinen Regeln wird ein Vorbehalt gemacht, soweit die strafbaren Handlungen in einem elektronischen Kommunikationsnetz begangen werden.
- Gegenüber den in (neu) Art. 27 StGB statuierten Regeln wird in (neu) Art. 27 Ziff. 2 StGB wiederum ein Vorbehalt zugunsten des bisherigen Medienstrafrechts gemacht, allerdings nur bezüglich Autoren und Redaktoren.

Diese dreistufige Struktur wird gewählt, weil die zu regelnden Sachverhalte (Netzwerkkriminalität) *einerseits* von der Struktur her stark an die Mediendelikte erinnern (notwendige Teilnahme einer Vielzahl von Beteiligten), *andererseits* aber die über das Medienstrafrecht bereits erfassten Sachverhalte ihrerseits auch über elektronische Kommunikationsnetze verwirklicht werden können (z.B. online-Publikation einer Tageszeitung); die beiden Bereiche überschneiden sich mithin. Die hierarchische dreistufige Regelung erlaubt, praktisch ohne Rückverweisung sämtliche Sachverhalte zu erfassen.

9.23 (neu) Art. 27 Ziff. 2 StGB (Abgrenzung zum Medienstrafrecht)

9.231 Verweisung auf das Medienstrafrecht nur für Autoren und Redaktoren

(Neu) Art. 27 Ziff. 2 StGB statuiert einen Vorbehalt zugunsten des Medienstrafrechtes, d.h (neu) Art. 27^{bis} StGB. Weil Sachverhalte, die unter das klassische Medienstrafrecht fallen, bei entsprechender Verwertung (Online-Publikation z.B. einer Tageszeitung) gleichzeitig auch in den Bereich der strafbaren Handlungen in elektronischen Kommunkationsnetzen fallen können, muss für das erst kürzlich revidierte Medienstrafrecht ein Vorbehalt angebracht werden. Dieser soll sicherstellen, dass das Medienstrafrecht nicht durch die neue Regelung unterlaufen wird. Dazu dient (neu) Art. 27 Ziff. 2 StGB.

Der Vorbehalt nennt allerdings nur die *Autoren und Redaktoren*. Namentlich für die – in der gegenwärtigen Regelung durch Art. 27 Abs. 2 StGB erfassten – „für die Veröffentlichung verantwortlichen Personen“ soll er dagegen nicht gelten. Dies deshalb, weil bei strafbaren Handlungen, die sich mittels automatisierter Prozesse in elektronischen Kommunikationsnetzen ereignen, gerade diese Gruppe von Personen – also die für die Veröffentlichung Verantwortlichen unter Ausschluss der Autoren und Redaktoren – der Neuregelung unterstellt werden sollen. Hingegen fallen andere Mitglieder der Redaktion und technisches Hilfspersonal (z.B. Kameraleute, Kabelträger usw.) weiterhin unter das Medienstrafrecht nach (neu) Art. 27bis StGB, weil sie mit der automatisierten Informationsübermittlung, -bereithaltung und -bereitstellung nichts zu tun haben. Der Gesetzestext von (neu) Art. 27 Ziff. 2 legt auch keine abweichende Auslegung nahe, insbesondere ist nicht die Rede von „ihrer“ Strafbarkeit.

Würde der Vorbehalt von (neu) Art. 27 Ziff. 2 auch diese Personengruppe erfassen, so könnten die Regelungen von (neu) Art. 27 Ziff. 3 und 4 StGB keine Allgemeingültigkeit beanspruchen. Vielmehr wäre im Schnittbereich von Medienstrafrecht und elektronischen Kommunikationsnetzen danach zu unterscheiden, ob es sich um ein Mediendelikt handelt - was zu einer Anwendung des Medienstrafrechtes führen würde - oder aber um ein „gewöhnliches“ Delikt, was zur Anwendung der Regelung von (neu) Art. 27 Ziff. 3 und 4 StGB führen würde.

Die Beschränkung des Vorbehaltes zugunsten des Medienstrafrechtes auf Autoren und Redaktoren gewährleistet demgegenüber, dass für diese durch die Einführung der neuen Bestimmungen grundsätzlich keine Änderung eintritt, während für Hosting- und Access-Provider spezifische Regelungen aufgestellt werden. Diesen beiden Personengruppen droht damit nicht mehr eine mögliche Strafbarkeit nach dem bisherigen Art. 322bis StGB (in der neuen Reihenfolge: Art. 322bis Ziff. 2 StGB); vielmehr unterstehen die Hosting-Provider der neuen Regelung von (neu) Art. 322bis Ziff. 1 StGB, während die automatisierte Zugangsvermittlung der Access-Provider gemäss (neu) Art. 27 Ziff. 4 StGB immer straflos bleibt.

Die vorgeschlagene Neuregelung der Strafbarkeit für Hosting-Provider geht einerseits weniger weit als die bisherige, weil fahrlässiges Handeln nicht mehr erfasst wird, ist aber andererseits auch deutlich schärfer, weil die strafrechtliche Verantwortung unabhängig davon greift, ob ein Autor oder Redaktor für die Veröffentlichung verantwortlich gemacht werden kann [223].

9.24 (neu) Art. 27 Ziff. 3 StGB (Hosting-Provider, Suchmaschinen)

9.241 Fremde Informationen

Die Regelung von (neu) Art. 27 Ziff. 3, Satz 1 StGB beschränkt ihren Anwendungsbereich auf “fremde Informationen“. Dies geschieht deshalb, weil das Bereithalten *eigener* Informationen, auch wenn es automatisiert erfolgt, nicht von der Privilegierung in (neu) Art. 27 Ziff. 3 StGB erfasst sein sollte.

[223] Vgl. oben Kapitel 6.

Fremd ist die Information, wenn der Täter sie weder selbst geschaffen noch sie sich zu eigen gemacht hat (z.B. indem er sie bewusst auswählt, verändert oder zusammenstellt), so dass auch ursprünglich fremde Informationen durch diese Handlungen als eigene qualifiziert werden müssen. Weil Suchmaschinen, soweit sie automatisiert arbeiten, im Kern solche Zusammenstellungen darstellen, wird für sie eine Sonderregelung getroffen (siehe dazu unten Ziff. 9.244).

Hält der Täter *eigene* Informationen bereit, so ist er nicht mehr bloss als Hosting-Provider zu qualifizieren, sondern untersteht den allgemeinen Regeln der Täterschaft nach (neu) Art. 27 Ziff. 1 StGB, evtl. als Autor oder Redaktor nach dem Medienstrafrecht (neu Art. 27bis Ziff. 2 StGB).

9.242 „automatisiert bereithalten“

Die Formulierung “automatisiert bereithalten“ bezeichnet – in Verbindung mit der Tatsache, dass es sich um fremde Informationen handelt, die bereitgehalten werden – im Wesentlichen das, was heute als “*Hosting*” bekannt ist. Wenn der Host fremde Informationen bereithält, ist daran zentral, dass es *automatisiert* geschieht.

Der Hosting-Provider räumt seinem Kunden ein bestimmtes Quantum an Speicherplatz auf seinen Rechnern ein, den der Kunde nutzen kann. Ist dem Kunden das Zugriffsrecht auf den entsprechenden Speicherplatz einmal eingeräumt, kann er diesen Speicherplatz nutzen, ohne dass der Hosting-Provider weiteres dazu tun müsste. Was immer der Kunde auf diesen Speicherplatz lädt, ist über eine entsprechende Adresse abrufbar. Hosting ist vergleichbar der Vermietung von Räumen: Sobald der Schlüssel übergeben wird, kann der Mieter sie nutzen.

Durch das Element der Automatisierung unterscheidet sich das Bereithalten von Informationen auch wesentlich von anderen Konstellationen. Zwar ist das Bereithalten der Informationen notwendig, damit der Täter seine Informationen überhaupt der Öffentlichkeit zugänglich machen kann. Weil er den Speicherplatz aber automatisiert (also analog einer Wohnung oder eines Geschäftsraumes) nutzt - d.h. Informationen auflädt, löscht, verändert usw.-, weiss der Hosting-Provider typischerweise gar nicht, was für Informationen sich auf seinen Rechnern befinden. Dieses Wissen kann er nur dadurch erlangen, dass er entweder auf eine Information spezifisch hingewiesen wird, oder dadurch, dass er präventiv selbst Kontrollen durchführt (in der Analogie zum Vermieter: die vermieteten Räumlichkeiten regelmässig selbst inspiziert).

9.243 Verweisung auf (neu) Art. 322bis Ziff. 1

Mit der Schaffung einer eigenständigen Strafnorm im Besonderen Teil des StGB folgt die Expertenkommission dem Regelungsmodell, das schon für die Strafbarkeit der Medienverantwortlichen in (neu) Art. 322bis Ziff. 2 StGB herangezogen wurde [224].

9.244 Verzeichnis, in welches fremde Informationen automatisiert aufgenommen werden (Suchmaschinen), (neu) Art. 27 Ziff. 3, Satz 2

Viele Nutzer beginnen ihre Web-Recherche bei einer *Suchmaschine* (sog. Search-Engines wie google.com, hotbot.com, altavista.com). Dabei handelt es sich um spezielle Web-Server, die eine Stichwortabfrage in einer Datenbank ermöglichen; diese Datenbank erfasst automatisiert bestehende Informationsangebote (Texte,

[224] Zu den Voraussetzungen der Strafbarkeit nach dieser Bestimmung, siehe unten Ziff.9.3.

Bilder, Musik, Multimediawerke usw.) und erschliesst sie per Hyperlink. Spider- oder Crawler-Programme suchen das WWW kontinuierlich ab, indexieren neue Webseiten nach Stichworten und legen diese mit den entsprechenden Hyperlinks in der Datenbank der Suchmaschine ab. Der Betreiber der Suchmaschine lässt diese Prozesse automatisiert ablaufen, hält aber den Index mit den Linkverweisungen auf seinem Server zum Abruf bereit.

(Neu) Art. 27 Ziff. 3 StGB stellt nun die Betreiber derartiger Suchmaschinen in strafrechtlicher Hinsicht den *Hosting-Providern* gleich. Diese Ergänzung ist notwendig, weil die Informationen, die der Index der Suchmaschine enthält [225], nicht mehr fremd sind. Es ist nicht irgendein Content-Provider, der seine Informationen auf dem Server des Suchmaschinenbetreibers bereitstellt, sondern der Betreiber der Suchmaschine selbst, der automatisiert eine Datenbank erstellt. Was in diesem Index steht, ist eigener Inhalt und wäre folglich nach (neu) Art. 27 Ziff. 1 StGB zu beurteilen.

Beispiel: Eine Abfrage nach den Suchbegriffen „Politiker X“ und „Arschloch“ führt zu einer Liste von Treffern. Einer davon enthält neben dem zum fremden Inhalt hinführenden Hyperlink den Satz: „Denn dieser Herr im teuren BMW ist nicht irgend ein kleines, mieses Arschloch, es ist der allseits beliebte Frauenheld Politiker X aus Y.“

Diese ehrverletzende Aussage kann als strafbares Verhalten des Suchmaschinenbetreibers interpretiert werden, da er sie selbständig in sein Verzeichnis aufgenommen hat. Nur schon für den Hyperlink, der auf fremde Webseiten weiterführt, kann – je nach Tatbestandsfassung der Strafnormen des Besonderen Teils StGB – eine Strafbarkeit des Link-Setzers bejaht werden (als eigenständiger Haupttäter oder als Gehilfe) [226]. In vergleichbarer Weise kommt eine Strafbarkeit in Betracht, wenn der Betreiber einer Suchmaschine automatisiert Bilder indexiert, die im Verzeichnis als kleine Bilddatei abgespeichert sind (siehe z.B. http://images.google.de).

Trotz dieser Unterschiede zur Funktion des Hosting-Providers ist *eine rechtliche Gleichbehandlung* mit letzterem angezeigt. Auch der Betreiber einer Suchmaschine unterhält eine sozialadäquate, ja letzlich gesellschaftlich erwünschte Infrastruktur. Die Suche und Indexierung des Webs läuft – ähnlich wie beim Hosting-Provider – automatisiert ab. Würde man die Strafbarkeit nach den allgemeinen Regeln bestimmen, träten die bekannten Probleme auf: Es könnte eine Kontrollpflicht zur Überprüfung der indexierten Informationen postuliert werden, bei deren Verletzung eine Strafbarkeit wegen Unterlassung drohte. Dies würde das effiziente Betreiben einer Suchmaschine letzlich verhindern.

Mit der vorgeschlagenen Neuregelung sollen die Grenzen der Strafbarkeit des Betreibers einer Suchmaschine klar definiert werden. Bei sicherem Wissen über strafrechtlich relevante Informationen in seinem elektronischen Verzeichnis soll er wie der Hosting-Provider den Zugriff verunmöglichen müssen. Bei Hinweisen auf

---

[225] Also nicht die verlinkten Informationen auf externen Rechnern.

[226] Näher dazu CHRISTIAN SCHWARZENEGGER/MARCEL ALEXANDER NIGGLI, Über die Strafbarkeit des Hyperlink-Setzers. Zum Urteil des Bezirksgerichts Zürichs vom 10. September 2002. medialex 2003, S. 27 ff.

derartige Informationen hat er ausserdem die Pflicht, diese an die Strafverfolgungsbehörden weiterzuleiten (vgl. zu den Einzelheiten die Kommentierung von (neu) Art. 322bis Ziff. 1 StGB). Hält er sich an diese Vorgaben, bleibt seine Tätigkeit straflos.

Nicht unter diese Strafbarkeitsbeschränkung fallen dagegen Anbieter von *nicht*-automatisiert ausgewählten und zusammengestellten Linklisten, wie die bekannten Web-Directories von Yahoo oder auch Google (www.yahoo.com oder http://directory.google.com u.ä). Wenn Mitarbeiter eines Diensteanbieters bestimmte Webinhalte gezielt in ein Verzeichnis aufnehmen, erfolgt dies mit Vorsatz, zumindest Eventualvorsatz. Ein solches Verhalten soll gerade nicht privilegiert werden. Genausowenig soll dies für eine Person gelten, die bewusst per Hyperlink auf fremde Informationen verweist, die den objektiven Tatbestand einer Strafnorm erfüllen. Hier wie dort ist nach den allgemeinen Regeln zu urteilen.

9.25 (neu) Art. 27 Ziff. 4 StGB (Access-Provider, kurzzeitige Zwischenspeicherung)

9.251 Gründe für die Straflosigkeit bei reiner Zugangsvermittlung in elektronischen Kommunikationsnetzen

Wie oben in Kapitel 6 (siehe Ziff. 6.2 und 6.3 a.E.) erläutert, ist bei Anwendung der allgemeinen Regeln des StGB nicht auszuschliessen, dass der Access-Provider als Gehilfe zur Haupttat des Content-Providers betrachtet wird. Gleiches gilt für den Sonderbereich der Mediendelikte, wenn man den Access-Provider als eine für die Veröffentlichung verantwortliche Person i.S. des geltenden Art. 27 Abs. 2 StGB begreift. In der Lehre des In- und Auslandes hat sich zu Recht die Auffassung durchgesetzt, dass für die automatisierte Durchleitung und Zugangsvermittlung keine Strafbarkeit entstehen kann 227. Dies beruht auf *verschiedenen Überlegungen*:

- Betrachtet man die Hauptrolle des Access-Providers genauer, fällt auf, dass seine hauptsächliche Tätigkeit in der *Unterstützung seiner Kunden* – der Nutzer – besteht. Diese benützen die verschiedenen Internetdienste zur Kommunikation oder Informationsbeschaffung und benötigen zu diesem Zweck einen Netzzugang. Die aktive Hilfe des Access-Providers bei der Errichtung eines momentanen Netzzugangs ist aber kein strafrechtlich relevantes Verhalten, weil die Handlung des Nutzers selbst straffrei ist. Dies gilt selbst dann, wenn der Nutzer auf Webseiten zugreift, auf welchen inkriminierte Informationen abgelegt sind.

- Eine bloss indirekte Funktion erfüllt der Access-Provider dagegen im Zusammenhang mit dem Bereitstellen illegaler Informationen durch den Content-Provider. Geht es beispielsweise um die Verbreitung einer rassendiskriminerenden Äusserung, so müssen – dem Informationsfluss folgend – als erste Helfer der Access-Provider *des Content-Providers* und sein Hosting-Provider angesehen werden. Nächster in der Reihe wäre dann der Network-Provider, der die Anbindung des Hosting-Providers an das Internet gewährleistet.

227 Siehe nur Art. 12 der E-Commerce-Richtlinie.

Weitere Helfer wären die Betreiber der Router oder Gateways, und schliesslich kämen wieder lokale Netzwerkdienstleister in Betracht. Vgl. zu den verschiedenen Provider-Typen die Grafik oben in Ziff. 2.31.

Erst am Ende dieses langen Weges ist die Unterstützung der Informationsverbreitung des Content-Providers durch den Access-Provider *des Nutzers* anzusiedeln. Bevor die Strafbarkeit dieses Akteurs erwogen wird, müsste jene der weiter vorne in der Kettengehilfenschaft stehenden Beteiligten nachgewiesen werden. Die Frage wird aber nicht einmal aufgeworfen, weil die Mitwirkung dieser Beteiligten ganz selbstverständlich als *sozialadäquat* angesehen wird.

- Voraussetzung solcher Überlegungen ist zudem, dass die Tat des Content-Providers überhaupt noch im Gange, d.h. nicht vollendet bzw. beendet ist. Es handelt sich hierbei um die Frage nach der Dauer der verschiedenen Äusserungs- und Verbreitungsdelikte, denn eine Förderung der Haupttat ist generell nur *vor* der Vollendung bzw. Beendigung möglich. Geht man – wie bei abstrakten Gefährdungsdelikten per definitionem (vgl. die Tabelle oben in Kapitel 6, Ziff. 6.12) – davon aus, dass die Äusserung schon im Moment der ersten Bereitstellung durch den Content-Provider vollendet und beendet ist, wäre jede spätere Zugangsvermittlung nicht mehr als Gehilfenschaft zu werten. Eine Strafbarkeit des Access-Providers wäre in solchen Fällen gar nicht denkbar.

- Da im Zusammenhang mit dem Bereitstellen illegaler Informationen durch den Content-Provider an kein aktives Tun des Access-Providers angeknüpft werden kann, müsste die Zuschreibung strafrechtlicher Verantwortung mit dem Unterlassen von technischen Sperrmassnahmen begründet werden. Anerkennt man, dass es überhaupt eine Gehilfenschaft durch Unterlassen geben kann, müsste man eine *Garantenstellung* des Access-Providers nachweisen.

  Weil das Vorverhalten des Access-Providers weder pflichtwidrig noch spezifisch gefahrerhöhend ist, scheidet eine Garantenstellung aus Ingerenz aus. Auch eine Garantenstellung aus Kontrolle über eine Gefahrenquelle lässt sich bezüglich des Access-Providers nicht konstruieren, da sonst die ganze Internet-Infrastruktur als Gefahrenherd betrachtet werden müsste, für den ein Access-Provider immer verantwortlich wäre.

- Die häufig gegenüber den Access-Providern geforderten Sperrmassnahmen haben im Grunde gar nichts mit Strafverfolgung zu tun. Sie gehören in den verwaltungsrechtlichen Bereich der Gefahrenabwehr (vgl. oben Kapitel 7). Damit eine Strafbarkeit durch Gehilfenschaft zur Verbreitung entstehen könnte, müsste im Einzelfall nachgewiesen werden, dass eine konkrete Datenübertragung direkt über die Infrastruktur des ins Auge gefassten Access-Providers stattfand. Mit den Sperrmassnahmen wird aber ein ganz anderes Ziel verfolgt: Prävention. Die Kunden des Access-Providers sollen nicht (mehr) auf die inkriminierten Informationen zugreifen können. Mangels eines konkreten Förderungsbeitrags des Access-Providers, fehlt es deshalb schon an der objektiven Voraussetzung einer Strafbarkeit wegen Teilnahme.

- Auch der Anwendungsbereich des Medienstrafrechts wird mehrheitlich so verstanden, dass Access-Provider nicht zu den für eine Veröffentlichung

verantwortlichen Personen zu zählen seien (vgl. oben Ziff. 6.2), so dass keine Strafbarkeit aus Art. 322bis StGB entstehen kann.

Diese Argumente sprechen klar dagegen, dem Access-Provider eine strafrechtliche Verantwortung zuzuschreiben. Dies ist denn auch der Standard, wie er von der Europäischen Union, den USA und anderen Ländern gesetzlich fixiert wurde und wie ihn auch das Ministerkomitee des Europarates empfiehlt. Wegen der grundsätzlichen Bedeutung der elektronischen Kommunikationsnetze in einer modernen Informationsgesellschaft drängt es sich auf, die Straflosigkeit der automatisierten Zugangsdienstleistung in elektronischen Kommunikationsnetzen im StGB explizit festzuhalten. Diesem Zweck dient (neu) Art. 27 Ziff. 4 StGB.

9.252 Zur Formulierung von (neu) Art. 27 Ziff. 4, Satz 1 StGB

Für eine *Definition der Zugangsvermittlung* kann auf die oben in Ziff. 2.314 gemachten Ausführungen verwiesen werden. Unter diese Bestimmung fällt nur, wer *ausschliesslich* den Zugang zum Internet ermöglicht. Ist ein Access-Provider aktiv an der Bereitstellung oder Bereithaltung von illegalen Informationen beteiligt, etwa indem er an den strafbaren Handlungen des Content-Providers als Mittäter, Anstifter oder Gehilfe beteiligt ist, oder handelt es sich dabei gar um eigene Informationen, so fällt er unter (neu) Art. 27 Ziff. 1 StGB (Strafbarkeit nach den allgemeinen Regeln). Die Strafbefreiung hängt also nicht von einem Status, sondern von der konkreten Funktion ab, die ein Access-Provider im einzelnen Kommunikationsvorgang einnimmt.

Eine Strafbefreiung, wie sie (neu) Art. 27 Ziff. 4 StGB vorsieht, ist in verschiedenen Normen anzutreffen. Zum Teil wird der Begriff „nicht strafbar“ verwendet 228, zum Teil das Adjektiv „straflos“ 229, was aber in der Regel eine Rechtfertigung indiziert. Als Beispiel sei Art. 32, 2. Teilsatz StGB genannt: „Die Tat […],die das Gesetz für erlaubt oder straflos erklärt, ist kein Verbrechen oder Vergehen.“ 230 Die gewählte Formulierung („nicht strafbar“) ist vorzuziehen, weil sie die strafrechtsdogmatische Einordnung als Tatbestandsausschluss vorzeichnet.

9.253 Automatische und kurzzeitige Speicherung fremder Informationen, (neu) Art. 27 Ziff. 4, Satz 2 StGB

Nach dieser Bestimmung ist die automatische kurzzeitige Zwischenspeicherung von fremden Informationen als Zugangsvermittlung i.S. von Art. 27 Ziff. 4, Satz 1 StGB zu verstehen, soweit sie durch eine Nutzerabfrage veranlasst wird. Entgegen der EU-Richtlinie 231 wird in der vorgeschlagenen Regelung nicht zwischen der technisch bedingten Zwischenspeicherung während eines spezifischen Datentransports 232

---

228 So z.B. in Art. 100 Ziff. 4 SVG (dringliche Dienstfahrt); Art. 53 Binnenschiffahrtsgesetz [SR 747.01] (dringliche Dienstfahrt); Art. 19b BetmG (Vorbereitung des eigenen Konsums/unentgeltliche Abgabe zum gemeinsamen Konsum bei geringen Mengen).

229 Unter anderem bei den Rechtfertigungsgründen (so z.B. in Art. 33 Abs. 2, 2. Satz; Art. 34 Ziff. 1 und Ziff. 2; Art. 119, strafloser Schwangerschaftsabbruch; Art. 260bis Abs. 2 StGB).

230 Zur Bedeutung, siehe TRECHSEL (Bibl.), Art. 33 N 17: „… so bleibt er «straflos», was prozessual einen *Freispruch* bedeutet, BGE 73 IV 261, 101 IV 121.“

231 Art. 12 Abs. 2 und Art. 13 der E-Commerce-Richtlinie.

232 Z.B. die Zwischenspeicherung eines an einen bestimmten Nutzer adressierten E-Mails auf dem Mailserver des Access-Providers.

und dem sog. *Proxy-Caching* unterschieden. Letzteres meint ebenfalls eine kurzzeitige Zwischenspeicherung durch den Access-Provider, die jedoch nicht einem einzelnen Datentransfer dient, sondern bei häufig abgerufenen Web-Inhalten einen effizienteren Datenabruf für alle Kunden des Access-Providers ermöglicht.

Programmgesteuerte Prozesse sorgen für eine dem Nutzerverhalten angepasste Zwischenspeicherung der meistbesuchten Webseiten auf einem Proxy-Server des Access-Providers. Auf diesem bleiben sie für eine gewisse Zeit bereitgehalten, fallen aber automatisch wieder aus dem Speicher, wenn sie veraltet sind oder nicht mehr abgefragt werden. Beide Varianten können unter den Begriff der automatischen und kurzzeitigen Speicherung fremder Informationen eingeordnet werden, wobei die Grenzziehung zwischen kurzzeitiger Zwischenspeicherung und einem längeren Bereithalten der Rechtsprechung überlassen bleibt.

Diese *flexible Lösung* ist einer expliziten Regelung vorzuziehen, weil eine Abgrenzung in generell-abstrakter Form in einem sich ständig wandelnden technischen Umfeld kaum gelingt. So ist auch in Deutschland trotz expliziter Regelung kaum geklärt, welcher Maximalzeitraum für eine solche Zwischenspeicherung zu gewähren sei, oder welches die beim Proxy-Caching „weithin anerkannten und verwendeten Industriestandards“ seien (vgl. § 10 TDG n.F.). Ausserdem ist wegen der grösseren Datenübertragungskapazitäten der Gebrauch von Proxy-Servern in der Zwischenzeit stark zurückgegangen.

Das sogenannte „*Mirroring*“ wird von der vorgeschlagenen Regelung nicht erfasst. Wenn also ein Anbieter ein bestimmtes Internet-Angebot durch aktive Handlungen auf einen anderen Server überspielt 233 - etwa um die Zugriffszeiten auf einen besonders entfernten oder besonders belasteten Server zu verkürzen -, wird er dadurch zum Content-Provider im Sinne von (neu) Art. 27 Ziff. 1 StGB. In diesen Fällen handelt es sich gerade nicht um eine automatische, durch Nutzerabfrage bedingte Zwischenspeicherung, sondern diese beruht auf einer *bewussten Auswahl*.

Geschieht die Spiegelung dagegen automatisiert, so unterliegt der „Spiegelnde“ der Verantwortlichkeit nach (neu) Art. 27 Ziff. 3 StGB. Dies ist insbesondere bedeutsam im Bereich der sogenannten „Newsgroups“, die häufig automatisiert und tale quale auf den lokalen News-Server überspielt werden.

9.3 Kommentar zu (neu) Art. 322bis Ziff. 1

9.31 Absatz 1

9.311 Allgemeines

Abs. 1 regelt die *Strafbarkeit des Hosting-Providers*, d.h. desjenigen, der seinen Kunden, den Content-Providern, einen Internet-Server zur Verfügung stellt, auf dem

233 Also „spiegelt“, deswegen: „Mirroring“.

diese eigene Dateien [234] anbieten können. Am Vorgang der Abspeicherung der Informationen auf den Webseiten ist der Hosting-Provider, auf dessen Internet-Server dies geschieht, gewöhnlich nicht beteiligt. Vielmehr handelt es sich dabei um automatisierte Programmabläufe, die allein der Content-Provider veranlasst und kontrolliert.

Auf dieser technischen Grundlage wäre an sich die Strafbarkeit des Hosting-Providers nach den allgemeinen Regeln zu beurteilen. Wenn etwa ein Content-Provider auf seiner Webseite kinderpornographisches Material anbietet oder betrügerische Angebote macht, stellt sich die Frage, ob der Hosting-Provider in einer der dem Strafrecht bekannten Beteiligungsformen daran mitwirkt. Die Antwort auf diese Frage ist in verschiedener Hinsicht unklar. Zunächst ist zu klären, ob überhaupt ein aktives Tun vorliegt. Der Vertrag, den der Hosting-Provider mit dem Content-Provider schliesst (worin man ein aktives Tun sehen könnte), ist bezüglich der Inhalte, die der Content-Provider später auf den Internet-Server des Hosting-Providers aufladen wird, eine *Art Blanko-Vertrag*: Sein Gegenstand ist nur die Pflicht, dem Kunden (Content-Provider) Speicherplatz auf dem Internet-Server zu überlassen und die Voraussetzungen dafür zu schaffen, dass dieser die von ihm ausgewählten Inhalte aufschalten und nach seinen Wünschen gestalten kann. Der Kunde hat seinerseits dafür ein Entgelt zu entrichten. Die Inhalte selber sind nicht Gegenstand des Vertrages, mit Ausnahme einer allfälligen Klausel, dass widerrechtliche Inhalte nicht aufgeschaltet werden dürfen. An den Vertragsschluss kann eine strafrechtliche Haftung also nicht anknüpfen.

Hat der Content-Provider einmal seine Inhalte aufgeladen, beschränkt sich der *Beitrag des Hosting-Providers* darauf, die Internet-Server, deren Speicherplatz er vermietet hat, zu betreiben. Ob darin ein aktives Tun erblickt werden kann, ist fraglich [235]. Zudem hängt die nähere Bestimmung des Tatbeitrages des Hosting-Providers entscheidend davon ab, wie im entsprechenden Tatbestand (den der Content-Provider als Täter verwirklicht) die Tathandlung umschrieben ist. Gerade bei Tathandlungen wie „überlassen“ und insbesondere „zugänglich machen“ (Art. 135, 197 Ziff. 3 StGB) ist die Unterscheidung von Tun und Unterlassen unsicher. Selbst wenn man im Einzelfall von einem aktiven Tun ausgehen kann, ist dieser Tatbeitrag weiter daraufhin zu bewerten, ob er täterschaftlicher oder nur gehilfenschaftlicher Natur ist.

Auch in diesem Punkt sind die Ergebnisse wenig klar, zumal hier noch das Problem der sog. *Gehilfenschaft durch alltägliche Handlungen* hineinspielt: Die genannten Tathandlungen verwischen die traditionelle Unterscheidung zwischen täterschaftlicher und gehilfenschaftlicher Begehungsweise in weitem Ausmass, und zwar zugunsten ersterer. Deshalb wäre über weite Strecken eine mittäterschaftliche Haftung anzunehmen, was jedenfalls im Ergebnis der Sache wenig angemessen erscheint.

Dazu kommt, dass die Einstufung als Täterschaft die Frage übergeht, ob man sich (auch) durch die Erbringung von alltäglichen Dienstleistungen, sofern diese eine

---

[234] Gemeint sind hier und im Folgenden via Internet abrufbare Dateien. Dabei handelt es sich überwiegend um Webseiten (daneben aber auch um Dateien, die über andere Internet-Dienste, z.B. FTP, abrufbar gehalten werden).

[235] Vgl. die Hinweise oben Ziff. 6.3.

vorsätzliche Haupttat fördern, als Gehilfe strafbar machen kann. Das Bundesgericht hat diese Frage in seiner bisherigen Rechtsprechung bejaht, sie aber immer nur fallweise und nicht generell und damit auch nicht abschliessend beantwortet [236]. Stuft man den Tatbeitrag des Hosting-Providers als täterschaftlich ein, kann sich diese Frage gar nicht mehr stellen. Das würde zwar zu einem klaren Ergebnis führen, verkürzt aber die sachliche Problematik, so dass eine solche Lösung aus diesem Grund ausscheiden muss. Wer hingegen die Leistung des Hosting-Providers als Gehilfenschaft einstuft, steht vor der nicht leicht zu beantwortenden Frage der Gehilfenschaft durch übliche Geschäftstätigkeit (hierzu oben Ziff. 6.3).

Scheidet ein aktives Tun aus, erhebt sich die Frage, ob der Hosting-Provider allenfalls aus Unterlassen mit begehungsgleicher Strafe belegt werden könnte. Auch in diesem Bereich ist die richtige und angemessene Lösung wenig klar. Eine *Garantenstellung* kann nach anerkannter Rechtsprechung und Lehre aus einem vorausgehenden gefährdenden Tun entstehen (Ingerenz). Wer in voraussehbarer Weise durch sein Handeln für Rechtsgüter Dritter eine Gefahr schafft, ist verpflichtet, alles zu unternehmen, damit sich diese Gefahr nicht in einer Rechtsgutsverletzung verwirklicht. Das Tun des Hosting-Providers liegt darin, dass er Interessierten Speicherplatz zur Verfügung stellt. Das ist wiederum eine völlig alltägliche und für sich legale Handlung, die keinerlei besondere Gefahr schafft.

Die Gefahr bzw. die strafbare Handlung resultiert erst aus der *missbräuchlichen Verwendung dieses Speicherplatzes* durch einen Dritten (Content-Provider), der vorsätzlich und rechtswidrig mittels der ins Netz gestellten Informationen eine Straftat begeht. Dabei verletzt er auch den mit dem Hosting-Provider geschlossenen Vertrag, weil dieser in der Regel das Angebot strafrechtlich relevanter Informationen in den Allgemeinen Geschäftsbedingungen verbietet.

Abhilfe könnte eine Klärung der offenen Fragen durch das Bundesgericht bringen. Das würde, bis alle relevanten Punkte die Stufe des Bundesgerichts erreicht hätten, mehrere Jahre dauern. Zudem besteht keinerlei Garantie, dass die höchste Instanz auch tatsächlich damit befasst wird; vielmehr hängt dies zunächst allein von der Praxis der Strafverfolgungsbehörden (Anklageerhebung) ab, die sich nicht voraussagen lässt. Eine weitere Unwägbarkeit liegt in der Reaktion der Verfahrensbeteiligten auf die Urteile der erst- und zweitinstanzlichen Gerichte (Ergreifung von Rechtsmitteln).

Aus diesen Gründen hat sich die Expertenkommission entschlossen, die Entscheidung über das Ausmass der Strafbarkeit eines Hosting-Providers nicht der Praxis zu überlassen, sondern sie *gesetzlich zu regeln*, und zwar unter *Ausschluss der allgemeinen Regeln von Täterschaft und Teilnahme*. Dabei bietet sich die Parallele zum bisherigen Medienstrafrecht deshalb an, weil hier Modifikationen dieser allgemeinen Regeln bereits gesetzlich vorgesehen sind (vgl. Art. 27 Abs. 2, 322bis StGB). Dies gilt auch, weil in einem Teilbereich Identität der Problemlagen besteht: Online-Versionen von Printmedien sind in der Sache dem gleichen Regime zu unterstellen, dem die Printmedien bereits jetzt unterstehen; das gilt jedenfalls für den Autor und den Redaktor. Im Übrigen ist jedoch zu beachten, dass diese Parallelität Grenzen hat. Die vorgeschlagene Norm ist in mehrfacher Hinsicht nicht

[236] Vgl. oben Ziff. 6.3.

einfach das Spiegelbild von Art. 322bis StGB in elektronischen Kommunikationsnetzen:

- Sie ist *weiter gefasst*, indem sie nicht nur auf Mediendelikte i.S. der bundesgerichtlichen Rechtsprechung zu Art. 27 StGB anwendbar ist. Es fallen auch diejenigen Äusserungsdelikte darunter, deren Qualifizierung als Mediendelikte das Bundesgericht ablehnt, wie z.B. Art. 135, 197 Ziff. 2 und 3 oder 261bis Abs. 4 StGB. Sie geht zudem weit über den Kreis jener Delikte hinaus, deren Qualifizierung als Mediendelikte überhaupt in Betracht kommt: Jede Straftat, bei deren Begehung das Mittel elektronischer Kommunikationsnetze im Spiel ist, fällt im Ausgangspunkt unter (neu) Art. 27 StGB und damit auch unter (neu) Art. 322bis Ziff. 1 StGB.

- Im Medienstrafrecht ist eine strafrechtliche Haftung des verantwortlichen Redaktors bzw. der für die Veröffentlichung verantwortlichen Person an die Voraussetzung geknüpft, dass der Autor nicht ermittelt oder in der Schweiz nicht vor Gericht gestellt werden kann. Dieser Ausschluss der Strafbarkeit gilt nicht bei Straftaten in elektronischen Kommunikationsnetzen: Auch wenn der Autor und/oder Content-Provider ermittelt oder in der Schweiz vor Gericht gestellt werden können, *bleibt die Strafbarkeit des Hosting-Providers nach (neu) Art. 322bis Ziff. 1 StGB möglich*.

- Die *Rolle des verantwortlichen Redaktors*, wie sie Art. 27 Abs. 2 StGB kennt und Art. 322 Abs. 2 StGB (Auskunftspflicht) strafrechtlich absichert, existiert in elektronischen Kommunikationsnetzen nicht zwingend. Wo sie aber besteht, richtet sich die Strafbarkeit des verantwortlichen Redaktors (wie auch des Autors) nach dem Medienstrafrecht ((neu) Art. 27 Ziff. 2 StGB).

- Die *fahrlässige Begehung* wird *nicht* unter Strafe gestellt.

9.312 Einzelheiten

9.312.1 Systematik

Nach dem neuen Konzept ist der Begriff der elektronischen Kommunikationsnetze, soweit er im vorliegenden Zusammenhang von Bedeutung ist, *umfassender als derjenige der Medien*. Deshalb wird die Vorschrift über strafbare Handlungen in elektronischen Kommunikationsnetzen in Art. 27 ff. StGB an den Anfang der ganzen Regelung gestellt ((neu) Art. 27 StGB); die „alte“ medienstrafrechtliche Strafnorm erscheint nun als (neu) Art. 27bis StGB. Die gleiche Umstellung erfolgt in der Annexstrafnorm von Art. 322bis StGB: Die ursprünglich im einzigen Absatz dieser Bestimmung untergebrachte Nichtverhinderung einer strafbaren Veröffentlichung wird zu Ziff. 2, Ziff. 1 regelt neu die Nichtverhinderung der Nutzung fremder „strafbarer“ Informationen in elektronischen Kommunikationsnetzen.

9.312.2 Verhältnis zur Strafbarkeit des Content-Providers

Der Content-Provider entspricht unter dem Gesichtpunkt seiner Tätigkeit zum Teil dem *Autor* im Medienstrafrecht, und zwar soweit, wie er selber geistiger Urheber der von ihm auf dem Internet-Server seines Hosting-Providers veröffentlichten Daten

(Texte, Bilder, etc.) ist. Unter dieser Voraussetzung richtet sich seine Strafbarkeit nach dem Medienstrafrecht (neu) Art. 27 Ziff. 2 StGB); das bedeutet, dass dessen Exklusivitätsregeln zur Anwendung kommen, diese gelten aber gemäss der ausdrücklichen Anordnung in (neu) Art. 27 Ziff. 2 StGB nur für den Autor (und für den Redaktor). Für den Hosting-Provider (der als solcher nie Autor oder Redaktor ist, sondern – auf den Medienbereich übertragen – allenfalls die Funktion der für die Veröffentlichung verantwortlichen Person innehat), gelten sie nicht. Seine Strafbarkeit richtet sich in diesem Fall nach (neu) Art. 322bis Ziff. 1 StGB.

Ist der Content-Provider nicht Autor, weil er etwa nur Bilder von Dritten übernimmt (und sie damit zu seinen eigenen macht), oder ist er zwar Autor, aber handelt es sich nicht um ein Mediendelikt im Sinne des geltenden Art. 27 Abs. 1 StGB, so gelten die allgemeinen Regeln (neu) Art. 27 Ziff. 1 StGB). Für den Hosting-Provider ändert dies nichts: Auch in diesem Fall haftet er nach (neu) Art. 322bis Ziff. 1 StGB.

Im Bereich der elektronischen Kommunikationsnetze steht also die strafrechtliche Haftung des Hosting-Providers nicht unter dem Vorbehalt, dass ein primär Haftender fehlt. Die Begründung dafür liegt letztlich in den Unterschieden zwischen der für eine Veröffentlichung verantwortlichen Person und einem Hosting-Provider: Während jene immerhin noch einen Bezug zu den publizierten Inhalten aufweist, indem sie überwachen muss und einschreiten kann [237], fehlt es bei dieser daran: Die Aufschaltung der Inhalte erfolgt automatisiert durch den Content-Provider, und sein Hosting-Provider kommt mit den Inhalten gar nicht in kognitiven Kontakt. Zudem geht die medienstrafrechtliche Zuordnung der Verantwortung vom Regelfall eines Unternehmens aus, innerhalb dessen nach Ausfall eines verantwortlichen Autors und Redaktors die für die Veröffentlichung verantwortliche Person zur Rechenschaft gezogen wird. Auch diese Voraussetzung ist im Verhältnis von Content- und Hosting-Provider nicht erfüllt.

Die gegenüber dem Medienstrafrecht leicht modifizierte Regelung führt für Hosting-Provider insofern zu einer *Verschärfung*, als ihnen die Strafbarkeit eines Autors oder Redaktors nicht zwingend Straflosigkeit verschafft. Auf der andern Seite liegt in der neuen Bestimmung auch eine Entlastung, weil die Hosting-Provider nicht der in Art. 322bis Satz 2 StGB vorgesehenen Fahrlässigkeitshaftung unterliegen.

9.312.3 Täterkreis

(neu) Art. 322bis Ziff. 1 StGB stellt ein *echtes Sonderdelikt* dar: Täter kann nur sein, wer fremde Informationen automatisiert in einem elektronischen Kommunikationsnetz bereithält; wer dies nicht tut, fällt zum vornherein aus dem Kreis der möglichen Täter. Mit dieser Umschreibung sind die Hosting-Provider erfasst, auf deren Webservern die Kunden (Content-Provider) Informationen aufschalten, ohne dass jene darauf noch einen Einfluss hätten. Dieser Vorgang läuft vielmehr automatisiert ab und hängt in jeder Hinsicht (Form und Inhalt der Information, deren Änderung oder Löschung, Zeitpunkt der Aufschaltung) allein vom Content-Provider ab. Darin ist eingeschlossen, dass es sich um *fremde* Informationen handelt, d.h. um solche, die nach Form und Inhalt allein auf den Content-Provider zurückgehen. Nimmt der Hosting-Provider auf die Information selber Einfluss, werden solche Informationen zu

[237] BGE 128 IV 53, 67 E. 5c; ZELLER (Bibl.), N. 55

eigenen mit der Folge, dass er nicht mehr dem Regime von (neu) Art. 322bis Ziff. 1 StGB untersteht, sondern der Regelung von (neu) Art. 27 Ziff. 1 StGB.

Um den möglichen Täterkreis auf den ersten Blick klar zu stellen, wird die Tätereigenschaft (Bereithalter von Informationen in einem elektronischen Kommunikationsnetz zu sein) an den Anfang der Bestimmung gerückt. Damit die Eingangsnorm von (neu) Art. 27 Ziff. 3 StGB, die auf (neu) Art. 322bis Ziff. 1 StGB verweist, und diese Norm in ihrem Wortlaut möglichst deckungsgleich sind, wird auch hier der Begriff „automatisiert“ eingefügt.

Ist der Hosting-Provider als *juristische Person* organisiert, trifft die Sondereigenschaft zunächst nur die juristische Person als solche, aber nicht die natürlichen Personen, die verantwortlich für sie handeln. Die Übertragung der strafbarkeitsbegründenden Pflichtenstellung auf die handelnden natürlichen Personen brauchte an sich eine explizite gesetzliche Regelung, wie sie das geltende StGB (nur) für die Straftaten des 2. Titels (Strafbare Handlungen gegen das Vermögen) kennt (Art. 172 StGB). Mit Blick auf die Regelung der Vertretungsverhältnisse im neuen Allgemeinen Teil des StGB, der in Art. 29 eine solche Norm schafft, die für sämtliche Straftaten gilt, hat sich die Expertenkommission indessen dazu entschlossen, von einer derartigen Sondernorm abzusehen. Sollte sich das Inkrafttreten des neuen Allgemeinen Teils verzögern, wäre diese Entscheidung nochmals zu überdenken.

9.312.4 Tathandlung

(neu) Art. 322bis Ziff. 1 StGB verankert eine *Unterlassungs*strafbarkeit: Der Vorwurf an den Hosting-Provider geht dahin, dass er nicht eingeschritten ist gegen die Nutzung einer Datei, die z.B. rassendiskriminierende oder gewaltverherrlichende Inhalte aufweist. Dieses Einschreiten bestünde darin, den Zugang zu der Webseite zu *sperren* (hingegen kommt eine an den Content-Provider gerichtete Aufforderung, die Inhalte unverzüglich zu entfernen, nicht in Betracht, weil darin eine Begünstigungshandlung [Art. 305 StGB] liegen könnte). Der Wortlaut der Bestimmung erwähnt ausdrücklich, dass dies nur gilt, soweit es ihm *technisch möglich* und *zumutbar* ist, eine Voraussetzung, die bei Unterlassungsdelikten anerkannte Selbstverständlichkeit darstellt [238], die aber um der Klarheit willen hier dennoch wiederholt wird.

9.312.5 Gegenstand der Unterlassung

Dieser besteht nicht in der Verhinderung einer strafbaren Handlung als solcher. Wenn der Content-Provider einmal einen strafrechtlich relevanten Inhalt aufgeschaltet hat, lässt sich diese Handlung nicht dadurch aus der Welt schaffen, dass der Hosting-Provider den Zugang zur Datei sperrt. Dies trifft jedenfalls nicht zu bei Gedankenäusserungsdelikten, deren Unrecht in der Äusserung als solcher liegt, vgl. die bereits genannten Beispiele von Art. 135 oder 261, aber auch 173 ff., 197 oder 259 StGB (Öffentliche Aufforderung zu Verbrechen oder zu Gewalttätigkeit). Gleiches gilt für andere Delikte, mit dem Unterschied, dass hier die Konstellation vorstellbar ist, dass die Zugangssperre die Vollendung der Straftat verhindert und es

[238] Vgl. KURT SEELMANN, in Niggli/Wiprächtiger, Basler Kommentar, N 62, 92 zu Art. 1; GÜNTER STRATENWERTH, Schweizerisches Strafrecht, Allgemeiner Teil I, 2. Aufl., Bern 1996, § 14 N 37.

beim Versuch bleibt, z.B. wenn der Zugang zu einer Webseite mit arglistig täuschenden Inhalten gesperrt wird.

Das Unrecht, das der Content-Provider verwirklicht hat, bleibt bestehen. Aber die *Wirkungen* dieser strafbaren Handlung lassen sich durch eine Zugangssperre beschränken, indem die Nutzer des Internet nicht mehr auf die Datei zugreifen können. Ob sie sich ihrerseits durch die Nutzung strafbar machen (würden), ist ohne Belang (durch den blossen Zugriff in der Regel noch nicht, wohl aber ausnahmsweise durch das anschliessende Abspeichern der Seite, vgl. Art. 197 Ziff. 3^{bis} StGB).

Damit ist auch der *rechtspolitische Zweck* der Inpflichtnahme der Hosting-Provider erfüllt. Man kann von ihnen nicht verlangen, Straftaten ihrer Kunden, d.h. der Content-Provider, welche diese durch die Publikation auf dem Internet-Server begangen haben, zu verhindern; denn sie haben ja auf den Vorgang der Aufschaltung der konkreten Inhalte keinen Einfluss. Aber man kann sie – und darin liegt ja das eigentliche gesetzgeberische Ziel – sehr wohl dazu anhalten, solche *Straftaten in ihren Folgen zu begrenzen*, indem sie die Kenntnisnahme der entsprechenden Inhalte verunmöglichen.

Darin liegt gegenüber der Variante, den Hosting-Provider für seine Beteiligung an der Tat des Content-Provider haften zu lassen, eine Änderung der Stossrichtung. Nach den allgemeinen Regeln von Täterschaft und Teilnahme geht es für den Hosting-Provider stets um die Frage, ob und wie er am Delikt des Content-Providers beteiligt ist. *Sofern* er sich strafbar macht, dann leitet sich seine Strafbarkeit aus dem Unrecht ab, das jener verwirklicht. Die vorgeschlagene Norm verschiebt den Vorwurf. Unrechtskern ist nicht die Beteiligung am Hauptdelikt, auch nicht durch eine allfällige Unterlassung, sondern das Untätigbleiben mit Blick auf die Nutzung durch Dritte. Das Unrecht der Haupttat, begangen durch den Content-Provider, stellt den Hintergrund dar, vor dem eine solche Regelung erst sinnvoll wird. Bedeutung erlangt dieses Unrecht ja erst dadurch, dass Dritte es zur Kenntnis nehmen, etwa rassendiskriminierende Äusserungen lesen oder sich Gewaltdarstellungen ansehen. Insofern bleibt bei der vorgeschlagenen Lösung die Verbindung mit der Haupttat durchaus erhalten.

Damit verwirklicht die neue Bestimmung zwei Ziele zugleich: Sie nimmt der Diskussion um die richtige Erfassung der Beteiligung des Hosting-Providers an der Haupttat des Content-Providers die Schärfe und sogar die praktische Bedeutung, und sie erlaubt es, die Wirkungen dieser Haupttat (vgl. die eben genannten Beispiele) auf die Nutzer der entsprechenden Datei einzudämmen.

Die dargelegte Modifikation des Unrechts hat also *zwei Hauptgründe*. Die Unmöglichkeit, die Begehung von Internet-basierten Delikten durch den Content-Provider zu verhindern, sowie die Möglichkeit, die Nutzung der Informationen durch Dritte strafrechtlich abgesichert zu verhindern.

Dazu kommt als *dritter wichtiger Grund* die Regelung des Strafanwendungsrechts (Art. 3 ff. StGB): Danach begeht der Content-Provider seine Tat dort, wo er den Abspeicherungsbefehl betätigt, der automatisiert zur Übermittlung der inkriminierten Daten an den Hosting-Provider führt. Ist dies im Ausland geschehen, so entfällt nach der bundesgerichtlichen Rechtsprechung die schweizerische Strafhoheit über

Teilnehmer der Tat; als solcher kommt der Hosting-Provider in Frage (über den im Ausland handelnden Content-Provider als Täter entfällt die Strafhoheit ohnehin, oben Ziff. 6.43). Dieses Problem umgeht die vorgeschlagene Lösung einer täterschaftlichen Unterlassungshaftung des Hosting-Providers, sofern dieser seinen Sitz in der Schweiz hat (ist dies nicht der Fall, besteht auch nach der hier neu vorgeschlagenen Regelung keine schweizerische Strafhoheit).

9.312.6 Voraussetzung der Pflicht zum Einschreiten

Verlangt wird, dass mittels der fremden Informationen eine strafbare Handlung begangen wird. Diese, begangen vom Content-Provider, ist in ihren Erscheinungsformen nicht begrenzt, sondern kann verschiedenster Art sein. Phänomenologisch lassen sich *zwei Gruppen* unterscheiden:

Zum einen kommen hier diejenigen Straftaten in Betracht, die dem Ruf nach einer verstärkten strafrechtlichen Erfassung der „Internetkriminalität“ Pate gestanden haben, wie Gewaltdarstellungen (Art. 135 StGB), Pornographie (Art. 197 StGB) oder Rassendiskriminierung (Art. 261bis StGB).

Zum andern gehören zum Kreis möglicher strafbarer Handlungen aber sämtliche Straftaten, zu deren Begehung der Einsatz elektronischer Kommunikationsmittel denkbar ist, z.B. täuschende Angaben für einen Betrug ebenso wie erhebliche Drohungen für eine Erpressung oder das urheberrechtswidrige Anbieten oder Verbreiten von Werkexemplaren (Art. 67 Abs. 1 lit. f URG) oder von einem Vervielfältigungsexemplar eines Tonträgers (Art. 69 Abs. 1 lit. f URG).

Entscheidend ist nur, dass die *fremden Informationen das Mittel zur Begehung* der strafbaren Handlung bilden („mittels“). Sie braucht sich in der Veröffentlichung nicht zu erschöpfen, sondern kann darüber hinaus die Erfüllung weiterer Tatbestandsmerkmale erfordern, z.B. eines Vermögensschadens beim Betrug. Das bedeutet, dass die strafbare Handlung, wie sie (neu) Art. 322bis Ziff. 1 Abs. 1 StGB voraussetzt, im Moment des Entstehens der Handlungspflicht des Hosting-Providers nicht vollendet sein muss, ein Versuch genügt.

Auf der andern Seite müssen die Informationen bereits Teil von strafrechtlich relevantem Unrecht bilden. Tun sie das nicht, sondern dienen sie z.B. erst der Vorbereitung eines Betruges, kann die Eingriffspflicht noch nicht entstehen. Denn erst die Verknüpfung von Strafunrecht mit der Benutzung eines Internet-Servers lässt die spezifische Pflicht des Hosting-Providers entstehen, weil Hintergrund der Regelung ja der Gedanke der Teilnahme am Internet-basierten Delikt bildet. Fehlt es (noch) an strafbarem Unrecht, ist der Tatbestand von (neu) Art. 322bis Ziff. 1 Abs. 1 StGB nicht erfüllt (woraus sich mit Blick auf Abs. 2 der neuen Bestimmung zugleich ergibt, dass Hinweise auf Handlungen, die nicht strafbar sind, nicht weiter geleitet werden müssen).

Die Beschränkung auf *fremde* Informationen hat ihren Grund darin, dass nur diesbezüglich die spezifische Situation vorliegt, die eine Sonderregelung für den Hosting-Provider rechtfertigt. Nur unter der Voraussetzung, dass er mit dem Inhalt der Information nichts zu tun hat, dass sie also für ihn fremd ist, treten die oben beschriebenen Schwierigkeiten der adäquaten Erfassung seiner Beteiligung an der Haupttat auf. Handelt es sich hingegen um eigene Informationen des Hosting-

Providers, so ist er in dieser Hinsicht eben nicht mehr Hosting-, sondern Content-Provider und fällt unter (neu) Art. 27 Ziff. 1 StGB.

Mit dem Begriff der *strafbaren Handlung* ist (nur) die Verwirklichung von strafrechtlich relevantem, d.h. tatbestandsmässig-rechtswidrigem Unrecht gemeint. Ob der Täter (Content-Provider) schuldhaft handelt, ist ohne Belang. Das ergibt sich schon aus der Praktikabilitätsüberlegung, dass man der Information nicht ansieht, ob sie von einem (nicht) schuldfähigen Täter stammt. Zudem wäre es auch bei der Erfassung des Hosting-Providers als Teilnehmer gleichgültig, ob er schuldhaft handelt (limitierte Akzessorietät). Und drittens ist auch das Anliegen, die Kenntnisnahme der inkriminierten Information durch Nutzer möglichst zu verhindern, jenseits der Frage der Schuldfähigkeit des Hosting-Providers.

9.312.7 Subjektiver Tatbestand

Im subjektiven Tatbestand verlangt die neue Bestimmung zunächst *Vorsatz* i.S.v. Art. 18 Abs. 2 StGB hinsichtlich aller objektiven Tatumstände; dazu gehört grundsätzlich auch der Eventualvorsatz. Daraus ergeben sich mit Blick auf (neu) Art. 322bis Ziff. 1 Abs. 1 StGB *zwei Schwierigkeiten*:

- Der Eventualvorsatz hat in der Praxis die Ausdeutung erfahren, dass eventualvorsätzlich (auch) derjenige handelt, von dem man sagen muss, dass sich ihm „der Erfolg seines Verhaltens als so wahrscheinlich aufdrängte, dass sein Verhalten vernünftigerweise nur als Inkaufnahme dieses Erfolges ausgelegt werden kann“ [239]. Wie immer man sich zu dieser Formel stellen mag, im hier interessierenden Bereich der Strafbarkeit der Hosting-Provider könnte sie dazu führen, dass ihnen auf dem Umweg über den Eventualvorsatz eine positive Kontrollpflicht auferlegt wird:

  Erhält der Hosting-Provider einen Hinweis auf eine Datei auf seinem Internet-Server mit angeblich strafrechtlich relevantem Inhalt und ignoriert er diesen Hinweis, dann stellt sich im anschliessenden Strafverfahren die Frage nach seinem Vorsatz (die praktisch relevanten Delikte sind nur vorsätzlich begehbar), vorausgesetzt, es handelt sich objektiv tatsächlich um eine strafbare Handlung. Je nachdem, wie glaubwürdig der Hinweisende ist und wie oft er den (sich im Ergebnis als zutreffend herausstellenden) Hinweis angebracht hat, kommt man im Einzelfall nicht um den Schluss herum, dass sich das Verhalten des Hosting-Providers nicht anders begreifen lässt denn als Inkaufnahme der Tatsache, dass mittels fremder Information auf seinem Internet-Server eine strafbare Handlung begangen wird. Um zu verhindern, in den Bereich des Eventualvorsatzes zu geraten, müsste der Hosting-Provider somit jedenfalls den glaubwürdigen und insistent vorgebrachten Hinweisen nachgehen; das ist gleichbedeutend mit der Etablierung einer positiven Kontrollpflicht.

  Nun geht es nicht darum, Hosting-Provider von einer Strafbarkeit auszunehmen, die sie an sich verdient hätten, und sie ungerechtfertigterweise zu privilegieren. Aber man hat sich die *Folgen* einer solchen Regelung vor Augen zu führen. Sie lägen darin, ein Kontrollsystem einzurichten, um den eingehenden Hinweisen selber nachgehen zu können. Das allein würde die hier vorgeschlagene Regelung

[239] BGE 109 IV 140.

noch nicht rechtfertigen.

Macht man sich indessen klar, dass die Glaubwürdigkeit des Hinweisenden dem Hinweis kaum je zu entnehmen ist und die hartnäckige Wiederholung eines Hinweises ebenfalls kein verlässlicher Gradmesser für seine Richtigkeit darstellt, dann wird deutlich, dass sich das System ad absurdum führen lässt, wenn man sich mit dem Eventualvorsatz hinsichtlich der strafbaren Handlung begnügt: Faktisch hätte der Hosting-Provider *jedem* Hinweis nachzugehen. Gehen solche Hinweise zahlreich ein, werden damit Ressourcen in einem Ausmass gebunden, das man angesichts der weit überwiegenden Zahl von legalen Nutzungen des Internet nicht mehr als angemessen bezeichnen könnte.

Überdies ist zu befürchten, dass die Hinweise als Mittel benutzt würden, rein privatrechtliche Streitigkeiten, wie sie beispielsweise bei Verletzungen des URG typisch sind, auf die Ebene des Strafrechts zu heben: durch einen entsprechenden Hinweis würde der Hosting-Provider verpflichtet, die Nutzung einer bei ihm gehosteten Datei mit angeblich URG-widrigen Inhalten (ohne dass dies bereits gerichtlich festgestellt wäre) zu unterbinden. Diesen Überlegungen käme noch verstärkte Bedeutung zu, wenn der Eventualvorsatz nicht nur bei Vorliegen von Hinweisen an den Hosting-Provider bejaht würde, sondern bereits aufgrund des allgemein bekannten Umstandes, dass die Hosting-Dienstleistungen auch zur Begehung von strafbaren Handlungen missbraucht werden. Um unter diesen Voraussetzungen der Strafbarkeit zu entgehen, müsste der Hosting-Provider die von seinen Kunden gespeicherten Inhalte präventiv kontrollieren [240].

- Die *zweite Schwierigkeit* liegt in der Natur einiger Tatbestände begründet, um die es im Kontext elektronischer Kommunikationsnetze häufig geht. Gewaltdarstellungen (Art. 135 StGB), Pornographie (Art. 197 StGB) oder Rassendiskriminierung (Art. 261bis StGB) verkörpern Unrechtsbeschreibungen, die normative Merkmale enthalten. Deren Bedeutung erschliesst sich nicht einfach aus einem alltäglichen und allgemein vorhandenen Vorverständnis, sondern erfordert eine Wertung.

  Was eine „grausame“ Gewalttätigkeit ist, ob deren bildliche Darstellung „schutzwürdigen kulturellen oder wissenschaftlichen Wert“ hat, ob sie die „elementare“ Würde des Menschen „in schwerer Weise“ verletzt (Art. 135 StGB), was „pornographische“ Schriften i.S.v. Art. 197 StGB sind, ob eine Ideologie auf die „systematische“ Herabsetzung gerichtet ist, ob eine Person wegen ihrer Religion „in einer gegen die Menschenwürde verstossenden Weise“ herabgesetzt wird (Art. 261bis StGB), all dies ist für den Betrachter häufig nicht eindeutig festzustellen.

  Der vorsichtige Hosting-Provider würde allerdings nicht auf die gerichtliche Bestätigung warten, dass etwa die Gewalttätigkeit „grausam“ ist, sondern er würde den Zugang zu der entsprechenden Datei schon dann sperren, wenn dies nach menschlichem Ermessen zumindest nicht mit Sicherheit auszuschliessen

[240] Vgl. NIGGLI/RIKLIN/STRATENWERTH, Die strafrechtliche Verantwortlichkeit von Internet-Providern, medialex, Sonderausgabe 1/2000, insb. S. 31f.

ist. Das führt zu einer Art von privater Zensur, an der einer demokratisch verfassten Gesellschaft nicht gelegen sein kann.

Aus diesen Gründen schlägt der Entwurf vor, dass die Strafbarkeit des Hosting-Providers auf die Fälle beschränkt wird, in denen er *sicheres Wissen um die Strafbarkeit* der beanstandeten Datei hat; alle andern Fälle vorsätzlichen Handelns sind hingegen nicht tatbestandsmässig. Die Hauptbedeutung dieser Begrenzung liegt darin, dass der Eventualvorsatz als strafbarkeitsbegründend ausgeschlossen wird; er zeichnet sich – auf der Wissensseite – dadurch aus, dass der Täter es bloss für möglich hält, aber nicht sicher weiss, dass der Inhalt der beanstandeten Datei ein bestimmtes tatbestandsmässiges Unrecht darstellt. Kaum praktische Bedeutung dürfte die mit der Beschränkung auf das sichere Wissen weiter verbundene Ausgrenzung der sog. Eventualabsicht (eine Spielart des direkten Vorsatzes) haben, deren Eigenart darin liegt, dass der Täter die Unrechtsverwirklichung zwar erstrebt, ihr Eintreten aber nicht für sicher, sondern bloss für möglich hält [241].

Ein sicheres Wissen um die Strafbarkeit der beanstandeten Handlung ergibt sich regelmässig nicht bereits aus dem blossen Hinweis, eine bestimmte Datei enthalte strafrechtlich relevante Information. Es kann sich aber daraus ergeben, dass dem Hosting-Provider nicht nur ein Hinweis auf die Datei zugeleitet wird, sondern der Inhalt der Datei selber [242]. Springt etwa dessen rassendiskriminierender Charakter in die Augen, dann ist es nahe liegend, dass der Hosting-Provider damit das für die Strafbarkeit nach (neu) Art. 322bis Ziff. 1 Abs. 1 StGB nötige sichere Wissen um die Strafbarkeit der entsprechenden Handlung erlangt hat (obwohl von der Offensichtlichkeit der Strafbarkeit nicht per se auf sein sicheres Wissen geschlossen werden kann).

Eine *Minderheit in der Expertenkommission* wollte die Erlangung des sicheren Wissens an die Voraussetzung knüpfen, dass dem Hosting-Provider ein Hinweis *aus zuverlässiger Quelle* (z.B. von Seiten der Strafverfolgungsbehörden) zugegangen sein muss und Hinweise beliebiger Privatpersonen nicht genügen. Grund für diese zusätzliche Beschränkung bildete die Überlegung, dass der Hosting-Provider nicht gezwungen sein solle, die Rechtswidrigkeit eines Inhalts selber zu beurteilen. Im Bereich der freien Kommunikation seien Grenzfälle an der Tagesordnung, und der Hosting-Provider könne im Zeitpunkt der Beurteilung nicht wissen, ob ein Gericht später zur Ansicht komme, die Widerrechtlichkeit der Datei sei offensichtlich. Ob etwas ins Auge springe, hänge nämlich von der Optik des Betrachters ab. Ein vorsichtiger Provider werde aus der Befürchtung heraus, sich strafbar zu machen, im Zweifelsfall den Zugang zur beanstandeten Datei sperren. Es bestehe deshalb eine erhebliche Gefahr, dass die Hosting-Provider auch rechtmässige Inhalte sperren würden. Dies widerspreche dem fundamentalen Grundsatz der freien Kommunikation in einer demokratischen Gesellschaft. Zudem setze es den Hosting-Provider dem Risiko aus, vom Content-Provider zivilrechtlich belangt zu werden, wenn sich eine Sperrung nachträglich als unnötig herausstellt.

---

[241] Vgl. TRECHSEL/NOLL (Bibl.), S. 98.

[242] Dabei muss hier offen bleiben, inwiefern sich derjenige, der dem Hosting-Provider den Inhalt der Datei selber zusendet, um ihn darauf aufmerksam zu machen, selber strafbar macht (z.B. Zugänglich-Machen oder Überlassen von harter Pornographie, Art. 197 Ziff. 3 StGB). Das Bundesgericht hat in einem strukturell ähnlich gelagerten Fall unter Hinweis auf das erlaubte Risiko dem Transport von Betäubungsmitteln (Art. 19 Ziff. 1 Abs. 3 BetmG) mit dem (verwirklichten) Ziel, diese zu vernichten, strafwürdiges Unrecht abgesprochen (BGE 117 IV 58).

Die *Mehrheit der Kommission* ist dieser Auffassung nicht gefolgt. Sie hat sich *gegen ein weiteres Zurückschneiden der Strafbarkeit* ausgesprochen, und zwar aus folgenden *Gründen*:

Erstens ist durch das Erfordernis des sicheren Wissens um die Strafbarkeit der Handlung die Verantwortung im Vergleich zum Normalfall des Eventualvorsatzes bereits reduziert. *Zweitens* ist – sollten die Zweifelsfälle tatsächlich die Norm bilden – durch die Voraussetzung sicheren Wissens dafür gesorgt, dass solches beim Hosting-Provider nicht entsteht: Wenn die Strafbarkeit des Inhalts einer Darstellung objektiv zweifelhaft erscheint, so ist sie das regelmässig auch für ihn, und dann hält er die Strafbarkeit der Handlung allenfalls für möglich, nicht aber für gewiss, wie es Abs. 1 erfordern würde.

Drittens fand die Kommissionsmehrheit es nicht sachgemäss, das sichere Wissen mit der Voraussetzung zu verknüpfen, dass der Hinweis aus zuverlässiger Quelle, z.B. von einer Strafverfolgungsbehörde, stammt. Das zeigt sich auf der einen Seite daran, dass auch ein Hinweis aus dieser Quelle falsch sein kann; dann fehlt es am objektiven Tatbestandsmerkmal einer „strafbaren Handlung“ (was eine Haftung für die vollendete Tat zum vornherein ausschliesst). Merkt dies der Hosting-Provider, dann hat er (zu Recht) kein sicheres Wissen um die Strafbarkeit. Auf der andern Seite kann sicheres Wissen im Einzelfall auch dann vorliegen, wenn der Hinweis von einer Privatperson kommt. Wollte man den Hinweis aus zuverlässiger Quelle nur als notwendige, nicht aber hinreichende Bedingung für die Entstehung sicheren Wissens verstehen [243], so bleibt offen, welche weiteren Erfordernisse dafür noch nötig sind.

An dieser Schwierigkeit wird – *viertens* – deutlich, dass sich das Konzept „Hinweis aus zuverlässiger Quelle“ mit dem Erfordernis des sicheren Wissens nicht verträgt. Sein Dreh- und Angelpunkt ist nicht die Qualität des Wissens des Hosting-Providers, sondern die *Quelle*, aus welcher der Hinweis stammt: die Tatsache, dass er von einer zuverlässigen Quelle, z.B. einer Strafverfolgungsbehörde, und nicht von einer Privatperson kommt. Dann aber geht es, genau besehen, gar nicht um einen blossen *Hinweis* dieser Behörde, sondern um eine *Anordnung* dieser Behörde.

Der Vorschlag der Minderheit läuft darauf hinaus, den Hosting-Provider dann zu bestrafen, wenn er einer Sperrverfügung der Strafverfolgungsbehörden nicht Folge leistet. Das bedeutet in der Sache die Streichung von (neu) Art. 322bis Ziff. 1 Abs. 1 StGB. Denn die Missachtung einer solchen Verfügung ist bereits nach geltendem Recht strafbar, und zwar unter den Voraussetzungen von Art. 292 StGB.

Aus diesen Gründen hält die *Mehrheit der Kommission* dafür, dass die vorgeschlagene Regelung der Sache angemessen ist und den Hosting-Providern die *Wahrnehmung von Eigenverantwortung* im beschriebenen Ausmass durchaus zugemutet werden kann.

Die Beschränkung auf das sichere Wissen bezieht sich einzig auf das Tatbestandsmerkmal der Strafbarkeit der entsprechenden Handlung („strafbare“ Handlung). Das StGB formuliert dies andernorts mit der Wendung „wider besseres

[243] Dies aus der Überlegung heraus, dass die Strafverfolgungsbehörde von ihrem Auftrag her notwendig der Belastungsperspektive verpflichtet ist, was in der Tendenz zu einer Einengung der Kommunikationsfreiheit führt.

Wissen“, z.B. in den Art. 128bis, 174 oder 303 f. StGB (oder „wissentlich“ [244]), so dass Abs. 1 den Wortlaut hätte: „Wer in einem elektronischen Kommunikationsnetz fremde Informationen automatisiert bereithält, mittels deren eine strafbare Handlung begangen wird (Art. 27 Ziff. 2), und es wider besseres Wissen unterlässt, …“.

Die adverbiale Verwendung des Begriffs hat bislang in der Praxis nicht zu Schwierigkeiten geführt, ist doch klar, dass sich die „wider besseres Wissen“ erfolgende Beschuldigung etwa bei der Verleumdung (Art. 174 StGB) nicht auf die Tathandlung der Beschuldigung als solche bezieht, sondern auf deren Wahrheit [245]. Um noch präziser zu sein, zieht die Kommissionsmehrheit indessen den (sachlich gleichbedeutenden) Einschub „… wie er sicher weiss …“ vor. Damit wird auch in sprachlicher Hinsicht deutlich gemacht, dass Bezugspunkt des sicheren Wissens einzig die Strafbarkeit der Handlung ist.

Eine *Fahrlässigkeitshaftung wird nicht eingeführt*. Sie würde schon dem Ausgangspunkt der Regelung widersprechen, die zu einem Teil die dogmatisch schwierig zu lösende Frage obsolet machen will, in welcher Beteiligungsform der Hosting-Provider an der Tat des Content-Provider mitwirkt; als solche Taten kommen praktisch nur Vorsatzdelikte in Betracht. Dazu kommt, dass eben dargelegt wurde, aus welchen Gründen ein Eventualvorsatz des Hosting-Providers hinsichtlich der Strafbarkeit der beanstandeten Handlung nicht zu genügen vermag; diese Entscheidung würde konterkariert, wenn man zugleich eine Fahrlässigkeitshaftung statuieren würde.

Schliesslich basiert die Unterscheidung auf dem unterschiedlichen Grad der automatisierten Mitwirkung: Ein Redaktor hat die (strafbare) Information regelmässig vor sich und kennt sie oder sollte sie zumindest kennen. Beide Voraussetzungen sind im Fall des Hosting-Providers nicht erfüllt: Weder hat er die Information vor sich noch kann er sie im Moment ihrer Aufschaltung kennen, sondern erst, wenn er darauf aufmerksam gemacht wird.

9.312.8 Strafdrohung

Die neue Bestimmung droht Gefängnis oder Busse an und befindet sich damit im Einklang mit Art. 322bis StGB. Weil der Hintergrund von (neu) Art. 322bis Ziff. 1 Abs. 1 StGB die positivierte Teilnahme an der Straftat des Content-Providers bildet, ist sicher zu stellen, dass die Strafdrohungen in beiden Fällen nicht allzu stark divergieren. Ein Blick auf die Delikte, bei denen die Nichtintervention des Hosting-Providers zu einer Strafbarkeit führen könnte, zeigt, dass diese Übereinstimmung fast durchgehend besteht; insbesondere drohen auch die Art. 135, 197 und 261bis StGB Gefängnis oder Busse an.

Nur in *Ausnahmefällen*, die aufs Ganze gesehen aber nicht ins Gewicht fallen, ist die abstrakte Strafobergrenze der durch den Content-Provider begangenen Tat höher, z.B. bei Art. 273 StGB (schwere Fälle von wirtschaftlichem Nachrichtendienst), während die Art. 258 (Schreckung der Bevölkerung) und 259 StGB (Öffentliche

[244] V.a. bei Gefährdungsdelikten, vgl. Art. 221 Abs. 2, 223 Ziff. 1 Abs. 1, 227 Ziff. 1 Abs. 1, 228 Ziff. 1 Abs. 4, 229 Abs. 1, 230 Ziff. 1 Abs. 3, 237 Ziff. 1, 238 Abs. 1 StGB.

[245] Vgl. GÜNTER STRATENWERTH, Schweizerisches Strafrecht, Besonderer Teil I I, 5. Aufl., Bern 1995, § 11 N 58.

Aufforderung zu Verbrechen oder zur Gewalttätigkeit) als Obergrenze statt drei Jahre Gefängnis drei Jahre Zuchthaus vorsehen (welche Unterscheidung mit dem revidierten StGB dahin fällt, vgl. dessen Art. 10).

Soweit mit der Androhung nur von Busse die Untergrenze von (neu) Art. 322bis Ziff. 1 Abs. 1 StGB tiefer liegt als diejenige der Straftat des Content-Providers, die mit Gefängnis allein bedroht sein kann, ist auch dieses Ergebnis sachgerecht, weil es in der Sache um eine Gehilfenschaft des Hosting-Providers geht und in diesem Fall bereits Art. 25 i.V.m. Art. 65 Abs. 4 StGB erlaubt, statt auf Gefängnis auf (Haft oder) Busse zu erkennen.

9.32 Absatz 2

9.321 Allgemeines

(neu) Art. 322bis Ziff. 1 Abs. 1 StGB verlangt sicheres Wissen um die Strafbarkeit der Handlung. Daraus ergibt sich die Frage, was mit demjenigen Hosting-Provider zu geschehen hat, der solches sichere Wissen nicht erlangt, etwa weil die Hinweise, die bei ihm eingehen, nur die URL-Adresse der beanstandeten Webseite enthalten, doch keine weiteren Informationen. Bleibt der Hosting-Provider in einem solchen Fall passiv, vermag er das für Abs. 1 nötige Wissen nie zu erlangen. Dieser Preis für die berechtigterweise enge Fassung von Abs. 1 wäre zu hoch. Deshalb muss die Beschränkung der Haftung in Abs. 1 in dieser Hinsicht (wieder) ausgeglichen werden.

Das ist die Funktion von (neu) Art. 322bis Ziff. 1 Abs. 2 StGB.
Angesichts dieser Stossrichtung wäre nahe liegend, Abs. 2 als Vereitelungsvariante zu konzipieren, wie sie etwa vom Tatbestand der Vereitelung einer Blutprobe (Art. 91 Abs. 3 SVG) her bekannt ist. Der Entwurf verzichtet aus *verschiedenen Gründen* darauf:

- Eine Vereitelungsfassung der Norm müsste lauten: „Der gleichen Strafdrohung untersteht, wer die Erlangung des nach Abs. 1 verlangten Wissens vereitelt“. Damit wäre jedoch zweifelsfrei nur derjenige Täter erfasst, der durch aktives Tun verhindert, an ihn gerichtete Hinweise zur Kenntnis zu nehmen, bildlich gesprochen: derjenige, der eine Mauer um sich baut, damit die Information nicht an ihn herankommt. Dieser ist aber nicht das Problem. Problematisch ist vielmehr die Konstellation, in welcher der Hosting-Provider sich nicht aktiv abschottet, sondern einfach untätig bleibt, und die Hinweise ihn nicht erreichen [246] oder er ihnen nicht nachgeht, d.h. die Information keine Wirkung entfalten kann. Es ist also vor allem die *Unterlassung*, die Abs. 2 erfassen muss.

- Deshalb müsste man die Vereitelungsfassung um den Zusatz ergänzen: „… oder wer die Nichterlangung zulässt“. Gleichbedeutend wäre „Der gleichen Strafdrohung untersteht, wer bewirkt oder zulässt, dass er das nach Abs. 1 nötige Wissen nicht erlangt“. Abgesehen von der unschönen und sehr technischen

[246] Mit einem Bild: Derjenige, der keine Mauer bauen muss, weil die Information schon in der Ausgangssituation auch ohne Mauer nicht an ihn herankommt, etwa weil zwischen ihm und „draussen“ ein Graben liegt.

Formulierung hat diese Variante einen gravierenden Nachteil: Sie führt wiederum zu einer positiven Kontrollpflicht des Hosting-Providers. Wenn aber schon die Regelung von Abs. 1 mit der Beschränkung auf sicheres Wissen eine solche Kontrollpflicht auszuschliessen anstrebt, so muss dies erst recht gelten für die Regelung von Abs. 2, die auf einen Ausgleich der Defizite von Abs. 1 abzielt.

Ein solcher Ausgleich kann nicht darin bestehen, eine Kontrollpflicht nun doch einzuführen, nachdem man sie im vorgehenden Absatz noch abgelehnt hat. Abgesehen davon, würde eine Kontrollpflicht, sofern man sie im Grundsatz bejahen wollte, die Frage aufwerfen, in welchem Ausmass Hosting-Provider verpflichtet sind, ihre Internet-Server nach Informationen rechtswidriger Art zu durchforsten. Diese Frage lässt sich abstrakt nicht beantworten, so dass die Einführung der Unterlassungshaftung zu grosser Rechtsunsicherheit führen würde, der mit der Neuerung gerade begegnet werden sollte.

- Angesichts dieser Überlegungen bliebe nichts anderes übrig, als der um die Unterlassungsvariante ergänzten Vereitelungsfassung einen Zusatz beizufügen; dieser könnte etwa folgenden Inhalt haben: „Eine Pflicht, in einem Telekommunikationsnetz ohne Hinweise Dritter nach Informationen im Sinne von Abs. 1 zu forschen, besteht nicht“. Doch ist man auch damit das Kontrollproblem nicht los. Denn damit wäre explizit gesagt, dass eine Pflicht zur Nachforschung besteht, wenn Hinweise Dritter eingehen. Eben zur Vermeidung einer solchen Pflicht beschränkt Abs. 1 den subjektiven Tatbestand hinsichtlich der Strafbarkeit der Handlung auf sicheres Wissen.

  Diese Entscheidung würde auch dann unterlaufen, wenn eine Pflicht zur Nachforschung erst aufgrund eingehender Hinweise Dritter entstünde. Liesse man den Zusatz „ohne Hinweise Dritter“ beiseite, gerät man in einen Widerspruch zu Satz 1, der ja explizit festhält, dass auch derjenige den Tatbestand erfüllt, der „zulässt“, dass er das nach Abs. 1 nötige Wissen nicht erlangt. Abgesehen davon wäre eine derartige Pflichteingrenzung ein Unikum, das im StGB nirgendwo sonst vorkommt.

Aus diesem Grund hat sich der Entwurf zu einem *radikalen Schritt* entschlossen. Statt den Ausgleich der Beschränkung der Strafbarkeit nach Abs. 1 auf sicheres Wissen um die strafbare Handlung in einer wie auch immer formulierten Vereitelungslösung zu suchen, wird dem Hosting-Provider die *positive Pflicht* auferlegt, Hinweise über (angeblich) strafbare Handlungen auf seinem Internet-Server an die Strafverfolgungsbehörden weiter zu leiten. Damit ist auch gewährleistet, dass die Beurteilung der Strafbarkeit – unter Vorbehalt von Abs. 1 – durch die dazu berufene Behörde und nicht durch eine Privatperson erfolgt; dazu besteht umso mehr Anlass, als zahlreiche Tatbestände, die hier praktische Bedeutung erlangen können – etwa Art. 135, 197 oder 261bis StGB –, normative Auslegungsspielräume bieten; deren Ausfüllung muss gerade in Zweifelsfällen den kompetenten Stellen vorbehalten sein.

9.322 Einzelheiten

9.322.1 Täterkreis

Abs. 2 stimmt hinsichtlich des Täterkreises mit Abs. 1 überein: Auch hier kommt als Täter nur in Betracht, wer in einem elektronischen Kommunikationsnetz fremde Informationen automatisiert bereithält, d.h. der Hosting-Provider. Damit erhält die Bestimmung die gleiche Struktur wie Abs. 1; was dort zum Täterkreis ausgeführt wird, gilt auch für Abs. 2.

9.322.2 Tathandlung

Auch bei Abs. 2 handelt es sich um ein *echtes Unterlassungsdelikt*: Der Hosting-Provider unterlässt die Weiterleitung von Hinweisen auf Informationen (auf seinem Internet-Server), mittels deren eine strafbare Handlung begangen wird, d.h., er bringt solche Hinweise den Strafverfolgungsbehörden nicht zur Kenntnis. Auch hier ist die Möglichkeit und Zumutbarkeit der Weiterleitung natürlich vorausgesetzt. Der Vorentwurf verzichtet darauf, für die Weiterleitung eine *Frist* anzusetzen; eine solche ergibt sich im Einzelfall aus den Möglichkeiten des Hosting-Providers sowie aus Zumutbarkeitsüberlegungen. Auch die *Form* der Weiterleitung ist nicht geregelt; in Frage kommen sämtliche Formen der Kommunikation, die den Inhalt des Hinweises zuverlässig den Strafverfolgungsbehörden zur Kenntnis bringen.

Schliesslich ist im Gesetzestext offen gelassen, an welche Strafverfolgungsbehörde im Einzelfall die Information weiterzuleiten ist. Die Präzisierung, sie sei an die „zuständige“ Strafverfolgungsbehörde weiterzuleiten, wäre eine Leerformel: Wenn damit gemeint ist, sie an die für die Verfolgung der Tat des Content-Providers zuständige Behörde weiter zu leiten, spricht dagegen, dass der Hosting-Provider kaum je weiss, wer dafür zuständig ist; sollte hingegen damit gemeint sein, dass sie an die für die Entgegennahme der Information zuständige Strafverfolgungsbehörde weiterzuleiten sei, stellt dies eine Selbstverständlichkeit dar, deren Erwähnung überflüssig ist. Entscheidend unter dem Gesichtspunkt des Normzwecks von Abs. 2 ist, dass die Information überhaupt Strafverfolgungsbehörden zur Kenntnis gebracht wird und nicht, von ihnen unerkannt, auf dem Internet-Server liegen bleibt. In der Praxis werden sich zudem allseits akzeptierte Meldewege einspielen.

Näher zu umschreiben sind die *Hinweise*, deren unterlassene Weiterleitung dem Hosting-Provider vorgeworfen wird:

- Zunächst sind mit den „Hinweisen“ Informationen gemeint, die an den Hosting-Provider *gerichtet* sind. Das ist in zweierlei Hinsicht zu präzisieren: Die Weiterleitungspflicht wird nur ausgelöst durch individuell an den Hosting-Provider gerichtete Meldungen, nicht aber durch allgemein zugängliche Informationen etwa aus Presse, Radio oder Fernsehen. Sie wird nur ausgelöst, wenn die Information gerade um dieser Information willen an ihn gerichtet ist. Hat er etwa eine Zeitung abonniert (dann ist *sie* an ihn gerichtet!), der er Hinweise auf einen strafbaren Inhalt auf seinem Internet-Server entnimmt, genügt dies nicht, weil es am spezifischen Zusammenhang zwischen Information und Meldevorgang fehlt. Dasselbe gilt für das Beispiel eines vom Hosting-Provider abonnierten online-newsletters.

- Es genügt jedoch nicht, dass die Hinweise lediglich „an ihn gerichtet“ sind. Entscheidend ist nicht, ob sie mit der Zielbestimmung „Hosting-Provider“ abgesendet wurden, sondern ob sie bei ihm *eingetroffen* sind und ihn *tatsächlich erreicht* haben. Deshalb spricht der vorliegende Entwurf von „bei ihm eingegangenen“ Hinweisen. Hingegen empfiehlt sich nicht, dies so zu formulieren, dass ihm die Hinweise „zur Kenntnis gebracht“ worden sind. Damit fände ein subjektives Moment Eingang in die Umschreibung der objektiven Tatbestandsmerkmale. Dass der Hosting-Provider die Hinweise zur Kenntnis nehmen muss, um vorsätzlich zu handeln, ist eine Frage des subjektiven Tatbestandes und deshalb dort zu behandeln.

  Theoretisch lässt sich der Eingang solcher Hinweise, soweit es um elektronische Kommunikation geht, auf zwei Wegen verhindern: Indem dagegen eine Schranke errichtet wird (vgl. das bereits genannte Beispiel der Abschottung durch „Mauerbau“), oder indem keine Möglichkeit elektronischer Kontaktnahme besteht (Beispiel der Abschottung durch „vorbestehenden Graben“). Praktisch dürften diese Befürchtungen wenig Gewicht haben, da Hosting-Provider auf Kommunikation angewiesen sind und entsprechende – offen gehaltene – Kanäle eingerichtet haben.

- Die Haftung des Hosting-Providers ist *beschränkt auf den Fall von Hinweisen „Dritter“.* Diese Präzisierung hat einerseits wiederum den Zweck, sicherzustellen, dass allgemein zugängliche Informationen aus Radio oder Fernsehen die Weiterleitungspflicht nicht auslösen. Sie soll andererseits aber erneut verdeutlichen, dass der Hosting-Provider nicht selber nach Hinweisen soll suchen müssen. Das bedeutet, dass der Hosting-Provider Hinweise auf strafbare Handlungen, die er zufälligerweise *selber* entdeckt (d.h.: Hinweise, die nicht von Dritten stammen), gemäss Abs. 2 nicht weiter leiten muss, sofern er deren Strafbarkeit nur für möglich, aber nicht für gewiss hält; ist er sich hingegen in der Frage der Strafbarkeit der Handlung sicher, hat er den Zugang zu der Datei zu sperren, andernfalls er nach Abs. 1 haftet.

- Weiterleitungspflichtig ist der Hosting-Provider nur bezüglich der Hinweise auf Dateien, die er selber hostet. Ein Hinweis an Provider A, die Datei xy sei pornographisch, muss nicht weiter geleitet werden, wenn nicht Provider A, sondern Provider B die beanstandete Datei hostet. Anders zu entscheiden, führt zu einer sektoriell begrenzten („Internetdelikte“) allgemeinen Anzeigepflicht (ohne dass diese einen Bezug zur eigenen Tätigkeit des Hosting-Providers hätte). Diese Lösung ergibt sich zudem aus der Überlegung, dass auch (neu) Art. 322bis Ziff. 1 Abs. 2 StGB in einem Teilbereich und gewissermassen in der „zweiten Ableitung“ eine positivierte Norm der Beteiligung (an der Tat des Content-Provider) statuiert; beteiligt ist der Hosting-Provider aber natürlich nur an derjenigen Tat, die auf seinem eigenen Internet-Server begangen wird.

- *Gegenstand der Hinweise* sind vom Hosting-Provider automatisiert bereit gehaltene Informationen, mittels deren eine strafbare Handlung begangen wird. In diesem Punkt entspricht Abs. 2 vollständig Abs. 1; das dort Ausgeführte gilt auch hier.

  Ein vorsichtiger Hosting-Provider wird unter dem Regime von (neu) Art. 322bis Ziff. 1 Abs. 2 StGB *sämtliche eingehenden Hinweise* an die Strafverfolgungsbehörden

weiter leiten. Damit entgeht er der Unrechtsverwirklichung der neuen Bestimmung sofern der Hinweis nicht selber schon Informationen enthält, die bei ihm das sichere Wissen um die Strafbarkeit der beanstandeten Handlung erzeugen. Ist dies hingegen der Fall, und leitet er trotzdem bloss weiter, dann erfüllt er (neu) Art. 322bis Ziff. 1 Abs. 1 StGB. Verzichtet er umgekehrt auf die Weiterleitung eines blossen Hinweises („Webseite xy enthält Gewaltdarstellungen"), so ist (neu) Art. 322bis Ziff. 1 Abs. 2 StGB dann nicht erfüllt, wenn die Darstellungen objektiv nicht tatbestandsmässig i.S.v. Art. 135 StGB sind und der Hosting-Provider dies weiss (andernfalls untauglicher Versuch).

9.322.3 Subjektiver Tatbestand

Wiederum ist *Vorsatz* verlangt, wobei hier bezüglich aller Tatbestandsmerkmale auch Eventualvorsatz genügt: Wer es ernsthaft für möglich hält und billigend in Kauf nimmt, dass Gegenstand eines Hinweises tatsächlich eine von ihm gehostete Datei mit strafrechtlich relevantem Inhalt bildet (womit er die entsprechende Information „bereithält" i.S.v. Abs. 2), und trotzdem nicht weiterleitet, macht sich nach (neu) Art. 322bis Ziff. 1 Abs. 2 StGB strafbar.

Dasselbe muss dann gelten, wenn ein Hosting-Provider die eingehenden Hinweise systematisch nicht zur Kenntnis nehmen sollte. Ist eine gewisse Häufung von Hinweisen von verschiedenen Seiten eingetreten, wird man ein solches Tun kaum mehr anders auslegen können denn als Inkaufnahme des Umstandes, dass sich unter den Hinweisen auch solche befinden, die tatsächlich strafrechtlich relevante Dateien betreffen. Der Vorwurf an ihn lautet dann aber nicht, dass er dies nicht überprüft (keine Kontrollpflicht!), sondern dass er trotz dieser nahe liegenden Möglichkeit nicht weiter geleitet habe. Ist der Hosting-Provider hingegen der richtigen Meinung, der Hinweis treffe zwar zu, aber es handle sich nicht um eine bei ihm, sondern beim Konkurrenten XY gehostete Datei, so entfällt der Vorsatz und damit die Strafbarkeit nach Abs. 2, wenn er nicht weiterleitet.

9.322.4 Strafdrohung

Auch Abs. 2 droht *Gefängnis oder Busse* an. Auf den ersten Blick mag dies für die blosse Nichterfüllung einer Weiterleitungspflicht streng erscheinen. Wenn man sich aber klar macht, dass die Bestimmung wie Abs. 1 die Beteiligung des Hosting-Providers an der Haupttat im Rücken hat und die – ihrerseits aus anderen Gründen notwendige – Beschränkung auf sicheres Wissen in Abs. 1 ausgleichen soll, wird die Strafdrohung plausibel.

9.33 Absatz 3

9.331 Grundsatz

Die vorgeschlagene Fassung von Abs. 2 kann dazu führen, dass ein Hosting-Provider einen in der Sache zutreffenden Hinweis auf eine strafbare Handlung im Sinne von Abs. 1 nicht weiterleitet, der Täter dieser strafbaren Handlung aber nicht verfolgt, geschweige denn bestraft wird; dies weil es am notwendigen Strafantrag fehlt (z.B. bei der Ehrverletzung, Art. 173 ff. StGB, oder bei Verletzungen des

Urheberrechts, Art. 67 ff. URG). Eine vergleichbare Konstellation tritt bei der Hehlerei auf (Art. 160 StGB). Wenn dort die Vortat ein Antragsdelikt darstellt, das jedoch mangels Strafantrag keine Strafverfolgung nach sich zieht, sieht Ziff. 1 Abs. 3 von Art. 160 StGB vor, dass auch die Hehlerei nicht verfolgt wird.

Die Expertenkommission schlägt für (neu) Art. 322bis Ziff. 1 StGB eine *analoge Regelung* vor: Soweit es sich bei der strafbaren Handlung um ein bloss auf Antrag strafbares Delikt handelt und ein Antrag nicht vorliegt, wird auch kein Verfahren gegen den Hosting-Provider eingeleitet. Anders zu entscheiden, kann zur paradoxen Situation führen, dass etwa bei einer Ehrverletzung der mutmasslich Verletzte die Tat nicht verfolgt haben will, der Hosting-Provider, bei dem ein Hinweis auf die Tat eingeht, aber doch zum Weiterleiten verpflichtet wäre.

Unterlässt er dies, müsste gegen ihn ein Verfahren wegen Verdachts der Verletzung von (neu) Art. 322bis Ziff. 1 Abs. 2 StGB eingeleitet werden. In diesem Verfahren müsste die mutmassliche Ehrverletzung öffentlich zur Sprache kommen, obwohl doch der Verletzte gerade dies nicht will und deswegen auf die Stellung eines Strafantrages verzichtet hat. Zudem ist Abs. 3 auch vor dem Hintergrund der Tatsache sinnvoll, dass es mit (neu) Art. 322bis Ziff. 1 StGB letztlich um die Erfassung des Beitrages des Hosting-Providers zur strafbaren Handlung des Content-Providers, d.h. zur „Haupttat“, geht.

Dieser Tatbeitrag stellt von seinem Charakter her und jenseits von spezifischen Tathandlungsbeschreibungen eine Gehilfenhandlung dar. Sofern aber kein Strafantrag gegen den Haupttäter vorliegt, bedeutet dies, dass auch keiner gegen den Gehilfen vorliegt. Denn würde ein Strafantrag gegen den Gehilfen bestehen, wäre davon auch der Haupttäter erfasst (Art. 30 Abs. 1 StGB). Auch aus diesem Grund empfiehlt sich die vorgeschlagene Regelung. Nur der Klarheit halber sei beigefügt, dass damit (neu) Art. 322bis Ziff. 1 Abs. 1 und 2 StGB nicht zum Antragsdelikt wird. Abs. 3 statuiert bloss dort eine Verfolgungssperre, wo *die strafbare Handlung* i.S.v. Abs. 1 und 2 ein Antragsdelikt ist, aber mangels Antrag nicht verfolgt wird.

9.332 Unsicherheit über den Strafantrag

Wenn ein Hinweis auf ein Antragsdelikt bei ihm eingeht, wird der Hosting-Provider häufig nicht wissen, ob ein Antrag vorliegt; weiss er gar nicht, dass es sich um ein Antragsdelikt handelt, wird er den Hinweis ohnehin weiterleiten. Es ist ihm deshalb zu empfehlen, die Meldungen *unabhängig vom Antragserfordernis* weiterzuleiten. Denn liegt ein Antrag vor, geht der Hosting-Provider aber irrtümlich davon aus, er fehle, betrifft dieser Irrtum nicht seinen Vorsatz, sondern eine Prozessvoraussetzung, und er ist damit unerheblich. Daran wird die Funktion von Abs. 3 nochmals klar: Die Bestimmung richtet sich nicht direkt an den Hosting-Provider, indem sie den Umfang seiner Weiterleitungspflicht einschränken würde. Sie soll vielmehr das stossende Ergebnis verhindern, dass der Hosting-Provider wegen unterlassener Weiterleitung eines Hinweises nach Abs. 2 bestraft wird, obwohl derjenige, der von der angeblich strafbaren Handlung betroffen ist, deren Verfolgung und damit auch Bestrafung ablehnt.

9.333 Antragsloses Antragsdelikt

Abs. 3 bezieht sich nicht nur auf Abs. 2, sondern auch auf Abs. 1: Selbst wenn der Hosting-Provider sicher weiss, dass mit den fremden Informationen eine strafbare Handlung begangen wird, findet keine Strafverfolgung statt, wenn es sich bei der strafbaren Handlung um ein antragsloses Antragsdelikt handelt. Denn hier gilt das zu Abs. 2 Ausgeführte analog: Die Nutzung einer Information zu verhindern, mittels deren eine strafbare Handlung begangen wird, ist sinnlos, wenn der durch die strafbare Handlung angeblich Verletzte deren Verfolgung und Bestrafung nicht will. Andernfalls müsste der Hosting-Provider sogar dann bestraft werden, wenn ihn der in seiner Ehre Verletzte selber auf die Datei aufmerksam macht und zugleich kundtut, dass ihm an einer Verfolgung nichts gelegen ist. Umgekehrt formuliert: Wenn der Verletzte die Nutzung der Information mit strafrechtlicher Absicherung verhindert haben will, hat er Strafantrag zu stellen.

9.34 Absatz 4

9.341 Grundsätzliches

Die Kommunikation über das Internet nimmt keine Rücksicht auf nationalstaatliche Grenzen. Daraus ergeben sich Schwierigkeiten im Strafanwendungsrecht (Art. 3 ff. StGB). Eine erste Schwierigkeit hat die geltende Regelung gelöst: Teilnahmehandlungen gelten nach der Rechtsprechung des Bundesgerichts als am Ort der Haupttat begangen. Liegt dieser im Ausland, wäre diese – soweit es um eine Teilnahmehandlung des Hosting-Providers geht und nicht eine täterschaftliche Beteiligung vorliegt – in der Schweiz grundsätzlich nicht strafbar.

Dieses Problem umgeht der vorliegende Entwurf, indem er konstruktiv die Strafbarkeit des Hosting-Providers von derjenigen des Content-Providers teilweise abkoppelt. Bei einer Haupttat im Ausland und einem Hosting-Provider in der Schweiz sind somit (neu) Art. 322^{bis} Ziff. 1 Abs. 1 und 2 StGB anwendbar; ist auch der Hosting-Provider im Ausland, fehlt es an der schweizerischen Strafhoheit.

9.342 Strafbarkeit des Delikts

Allerdings bleibt vorerst offen, nach welchem Recht zu entscheiden ist, ob eine *strafbare* Handlung vorliegt. Im Privatrecht beurteilt sich die Frage des anwendbaren Rechts nach den Regeln, wie sie im Internationalen Privatrecht (Art. 13 ff. IPRG sowie jeweilige sachspezifische Sonderbestimmungen) verankert sind. Im Strafrecht sucht man vergeblich nach einer solchen Regelungsart. Explizite gesetzliche Bestimmungen, die im internationalen Verhältnis eine Anweisung dafür geben würden, nach welchem Recht die Strafbarkeit der strafbaren Handlung zu beurteilen sind, fehlen. Die Art. 3 ff. StGB sind nicht anwendbar, weil sie (mit Ausnahme von Art. 5, 6 und 6^{bis} je Ziff. 1 Satz 2) die internationale Zuständigkeit und nicht das anwendbare Recht normieren.

Parallele Strukturen im geltenden Strafrecht, in denen die gleiche Frage entscheidwesentlich würde, sind nicht ersichtlich: Das StGB enthält keine Norm darüber, nach welchem Recht die Strafbarkeit einer Handlung zu beurteilen wäre, die

Teil des objektiven Tatbestandes bildet. Im „Normalfall“ der Gehilfenschaft stellt sich diese Frage dann nicht, wenn die Haupttat im Ausland begangen wurde; dann gilt auch die Gehilfenschaft als im Ausland begangen; damit fehlt es an der schweizerischen Strafhoheit, so dass sich die Frage des anwendbaren Rechts gar nicht stellen kann. Die Konstellation, in der bei einer Gehilfenhandlung darüber nachgedacht werden müsste, nach welchem Recht die Strafbarkeit der im Ausland begangenen Haupttat zu beurteilen sei, gibt es deshalb nicht.

Im Ergebnis ist jedoch klar, dass die Frage der Strafbarkeit des Delikts nach *schweizerischem Recht* beurteilt werden muss. Andernfalls gibt man den Vorzug preis, um dessentwillen der Vorentwurf die selbständige Strafbarkeit des Hosting-Providers eingeführt hat: Die neue Norm will nicht nur die umstrittenen Teilnahmefragen gesetzlich regeln, sondern auch verhindern, dass die „strafbare“ Information weiterhin von einem schweizerischen Server abgerufen werden kann. Dabei ist klar, dass ein Interesse an solcher Verhinderung nur insoweit besteht, als die Datei nach *schweizerischem* Recht strafbare Informationen enthält, da es um *dessen* Durchsetzung geht. Fraglich ist nur, ob dafür eine explizite gesetzliche Regelung notwendig ist [247].

9.343 Gründe für ausdrückliche Normierung

Für eine explizite Lösung spricht die Überlegung, dass es sich bei (neu) Art. 322bis Ziff. 1 StGB funktionell um eine Teilnahmebestimmung handelt. Die Teilnahme folgt dem Schicksal der Haupttat; für deren Beurteilung sind ausländische Behörden zuständig und ist ausländisches Recht anwendbar. Dazu kommt, dass die neue Bestimmung auf das Prinzip der doppelten Strafbarkeit insoweit verzichtet, als es um die Beurteilung der Strafbarkeit der strafbaren Handlung geht. Der Zugriff auf den Hosting-Provider soll auch in denjenigen Fällen möglich sein, in denen die beanstandete Handlung nach dem Recht des Ortes ihrer Ausführung nicht strafbar ist. Von praktischer Bedeutung könnten hier v.a. Äusserungen aus dem amerikanischen oder australischen Rechtskreis sein, die nach schweizerischem Recht als rassendiskriminierend gelten. Soweit in diesen beiden Modifikationen Abweichungen gegenüber den allgemeinen Regeln liegen, sprechen sie dafür, die Frage des anwendbaren Rechts ausdrücklich zu normieren.

9.344 Funktion des neuen Absatzes

Dass auch ohne die vorgeschlagene Sonderbestimmung nach schweizerischem Recht zu beurteilen wäre, ob die beanstandete Handlung strafbar ist, lässt sich mit dem Hinweis auf die internationale Zuständigkeit der Schweiz in solchen Fällen begründen. Wenn die Unterlassung des Hosting-Providers unstreitig unter schweizerische Strafhoheit fällt, dann muss sie auch nach schweizerischem Recht beurteilt werden. Belege dafür, dass der schweizerische Gesetzgeber diese Auffassung vertritt, finden sich in den erwähnten Ausnahmebestimmungen von Art.

---

[247] Aus der Sonderregelung bei der Geldwäscherei für den Fall, dass die Vortat im Ausland begangen wurde (Art. 305bis Ziff. 3 StGB), lässt sich nichts herleiten. Sie betrifft eine Spezialkonstellation der Einziehungsvereitelung (ohne Ziff. 3 würde Straflosigkeit eintreten, weil der 17. Titel nur die schweizerische Rechtspflege schützt, bei Vortaten im Ausland aber die ausländische geschützt würde), die mit (neu) Art. 322bis Ziff. 1 StGB nichts zu tun hat (dem Hosting-Provider wird in der Sache nicht die Vereitelung einer Einziehung bzw. Sperrung vorgeworfen, sondern dass er es unterlassen hat, durch Sperrung des Zugangs zur beanstandeten Datei deren Nutzung zu verhindern).

5, 6 und 6bis StGB, je Ziff. 1 Satz 2. Zu erwähnen, dass das Gesetz des Begehungsortes anzuwenden sei, wenn es für den Täter das mildere ist, ergibt nur einen Sinn vor dem Hintergrund der Tatsache, dass an sich das schweizerische Gesetz anzuwenden wäre.

Dass das schweizerische Gesetz anzuwenden ist, folgt für die Art. 3-7 StGB daraus, dass über die Tat schweizerische Gerichtshoheit besteht. Unausgesprochene, aber (nach den Art. 3-7 StGB) im Regelfall zwingende Folge internationaler Zuständigkeit ist somit nach schweizerischer Auffassung die Anwendung schweizerischen Sachrechts. So gesehen wäre der neue Abs. 4 nur eine *Klarstellung*.

(neu) Art. 322bis Ziff. 1 Abs. 4 StGB soll allfällige Diskussionen über das anwendbare Recht zum vornherein überflüssig machen. Gesetzestechnisch kann die neue Bestimmung, jedoch nicht in der materiellen Strafbestimmung selber untergebracht werden (d.h. in neu Art. 322bis Ziff. 1 Abs. 1 und 2 StGB), weil die strafbaren Handlungen, die hier in Betracht kommen, nicht zum vornherein auf eine einzige oder nur wenige begrenzt wären. Vielmehr müsste jede Straftat erwähnt werden, von der sich denken lässt, dass sie mit Hilfe oder mittels elektronischer Kommunikationsnetze begangen werden kann. Das trifft für *sämtliche* Straftaten zu; deshalb wird der gleiche Regelungsgehalt in einem separaten Absatz umschrieben.

Wie immer man bei Fehlen einer Regelung entscheiden würde: Die explizite Aussage, dass sich die Strafbarkeit des Delikts nach schweizerischem Recht beurteilt (wobei klar ist, dass es dabei um die Anwendung des Sachrechts geht und nicht des Zuständigkeitsrechts [248]), beseitigt allfällige Zweifel. Das erscheint nicht überflüssig auf einem Gebiet, dessen Regeln des internationalen Rechtsanwendungsrechts nicht sehr entwickelt sind, weil es ihrer bislang kaum bedurfte.

9.35 Absatz 5

Gemäss Abs. 5 werden Informationen im Sinne der Abs. 1 und 2, d.h. solche, mittels deren eine strafbare Handlung begangen wird, gelöscht. Hier stellt sich zunächst die Frage, ob eine solche Bestimmung überhaupt nötig ist, oder ob sich die Löschungsbefugnis nicht ohnehin aus der Anwendung der allgemeinen Regeln der Einziehung ergeben würde.

9.351 Löschung im Fall von Abs. 1

9.351.1 Grundsätzliches

Sedes materiae des Einziehungsrechts im vorliegenden Zusammenhang sind die Sicherungseinziehung nach Art. 58 StGB sowie allfällige besondere

[248] Andernfalls gerät man in einen Zirkel: Abs. 4 verwiese auf Art. 3 ff. StGB, schweizerische Strafhoheit läge vor, weil der Sitz des Hosting-Providers sich in der Schweiz befindet; deshalb wäre (neu) Art. 322bis Ziff. 1 StGB anwendbar. Die Frage, nach welchem Recht über die Strafbarkeit der strafbaren Handlung entschieden werden muss, würde sich nach Abs. 4 beantworten, dieser wiederum verwiese auf Art. 3 ff. StGB, usw.

Einziehungsbestimmungen bei einzelnen Straftaten. Wird in einem Strafverfahren z.B. wegen harter Pornographie (Art. 197 Ziff. 3 StGB) der Beschuldigte verurteilt, und finden sich pornographische Daten auf der Festplatte seines Computers, kann diese Festplatte nach den Sonderbestimmungen von Art. 197 Ziff. 3 und 3bis je Abs. 2 StGB eingezogen werden. Da bei der Einziehung der Grundsatz der Verhältnismässigkeit zu beachten ist [249], bedeutet dies indessen nicht, dass der Verurteilte seine Festplatte nicht wieder zurück erhält. Vielmehr hat die Vollzugsbehörde die inkriminierten Daten zu löschen und den Gegenstand in dieser Form dem Berechtigten auszuhändigen; dies jedenfalls dann, wenn nicht erneuter deliktischer Gebrauch wahrscheinlich ist. Gegenstand der Einziehung bleibt jedoch ein (körperlicher) Gegenstand im Sinne von Art. 58 StGB; dieser wird aber durch die Löschung so verändert, dass seine Gefährlichkeit entfällt [250].

Sollen bei einem Hosting-Provider, der nach (neu) Art. 322bis Ziff. 1 Abs. 1 StGB verurteilt worden ist, die „strafbaren Informationen“ gelöscht werden, so wäre an sich sein Internet-Server einzuziehen, auf dem sich diese Informationen befinden. Dieser Lösung steht jedoch entgegen, dass sie in der Regel unverhältnismässig sein dürfte. Denn auf diese Weise werden sämtliche andern Kunden des Hosting-Providers, deren Informationen auf dem einzuziehenden Server abgespeichert sind, tangiert; ebenso ist die praktische Durchführbarkeit dieser Anordnung fraglich. Deshalb liegt die Alternative darin, beim Hosting-Provider direkt auf den Internet- Server zu greifen und die „strafbaren“ Informationen zu löschen, sofern er nicht selber der vorausgehenden Aufforderung zur Löschung nachkommt.

Ob auf diesen Fall Art. 58 StGB analog anwendbar ist, erscheint zweifelhaft. Objekt der Einziehung wären Daten bzw. Informationen, aber diese stellen keine Gegenstände i.S.v. Art. 58 StGB dar [251]. Zudem kann nicht real eingezogen werden, sondern es fällt allein eine Löschung in Betracht. Aus diesen Gründen hat sich der Vorentwurf für eine explizite Lösung der Frage entschieden.

9.351.2 Materiellrechtliche Natur der Löschung

Die Löschung der Informationen als Pendant zur Einziehung ist, wie diese, materiellrechtlicher Natur. Sie wird vom Gericht im Urteil angeordnet. Abs. 5 verkörpert nicht eine prozessuale Bestimmung analog der Beschlagnahme, mittels deren die Strafverfolgungsbehörden die Informationen vorläufig sperren könnten. Eine solche ist der Prozessgesetzgebung vorbehalten, d.h. derzeit noch den Kantonen. Diese sind zur Umsetzung des materiellen Bundesstrafrechts verpflichtet und haben ihm genügende prozessuale Instrumente bereit zu stellen. Im Vordergrund steht hier eine Sperrverfügung der Strafverfolgungsbehörden; diese hat

---

[249] BAUMANN, in NiggliWiprächtiger, Basler Kommentar, Basel 2003, Art. 58 N 14. Das gilt auch für die speziellen Einziehungsbestimmungen in Art. 135 Abs. 2 und 197 Ziff. 3 Abs. 2 und Ziff. 3bis Abs. 2 : AEBERSOLD, in Niggli/Wiprächtiger, Basler Kommentar, Basel 2003, Art. 135 N 35; unklar SCHWAIBOLD/MENG, in Niggli/Wiprächtiger, Basler Kommentar, Basel 2003, Art. 197 N 61.

[250] Ob auch bei Art. 197 Ziff. 3 und 3bis je Abs. 2 StGB die oder einzelne weitere Voraussetzungen von Art. 58 StGB erfüllt sein müssen, kann hier auf sich beruhen.

[251] Nach SCHMID (Bibl.), N 22 zu Art. 58 können unkörperliche Werte wie „Forderungen, Guthaben und immaterielle Güter wie Patente, Urherberrechte etc. tendenziell nicht gemäss StGB 58 eingezogen werden“; eine Ausnahme will SCHMID für Daten machen (a.a.O., FN. 57). Aber die Ausnahme wird nicht begründet und der Vollzug der Einziehung in diesen Fällen nicht näher erläutert. TRECHSEL (Bibl.), N 5 zu Art. 58) erwähnt das Löschen eines Programms auf einer Festplatte.

sich – als prozessuale Zwangsmassnahme – auf entsprechende kantonale Bestimmungen zu stützen.

Im Rahmen des Vorentwurfes für eine Schweizerische Strafprozessordnung wird zu diskutieren sein, ob eine ausdrückliche Regelung für die „Beschlagnahme“ von Daten in Form einer (Zugangs-)Sperre einschliesslich eines Veränderungsverbots aufgenommen werden soll [252]. Auch die Cybercrime-Konvention verlangt in ihrem prozessualen Teil (Art. 19 Ziff. 3 lit. d), dass die Gesetzgebung den zuständigen Behörden Instrumente in die Hand gibt, um den Zugang zu bestimmten Daten zu sperren.

9.351.3 Löschung bei Freispruch

Die Löschung der Informationen wird vom Gericht dann angeordnet, wenn es zu einer Verurteilung kommt. Inwiefern eine Löschung auch im Falle eines Freispruchs oder bei prozessualer Erledigung der Sache in Betracht fällt, ist für das Verfahren gegen den Hosting-Provider und jenes gegen den Content-Provider gesondert zu prüfen:

- Scheitert eine Verurteilung des Hosting-Providers beispielsweise daran, dass sich ihm kein sicheres Wissen um die Strafbarkeit der Information, sondern nur allenfalls Eventualvorsatz nachweisen lässt, stellt sich die Frage, ob die „strafbaren“ Informationen in diesem Verfahren dennoch gelöscht werden können. Art. 58 StGB statuiert die Einziehung „ohne Rücksicht auf die Strafbarkeit einer Person“; dasselbe gilt für die Spezialbestimmung des neuen Abs. 5.

  Das bedeutet zweierlei: *Erstens* stehen allfällige Schuldausschliessungsgründe beim Hosting-Provider, der tatbestandsmässig und rechtswidrig gehandelt hat, der Löschung nicht entgegen. *Zweitens* – für den vorliegenden Zusammenhang bedeutsamer – ist eine Löschung auch dann zulässig, wenn nicht der Angeschuldigte, sondern ein Dritter die einziehungsbegründende Straftat begangen hat. Auch in diesem Fall können die Informationen, mittels deren eine strafbare Handlung begangen wird, auf dem Internet-Server des Hosting-Providers gelöscht werden [253].

  Wird also der Hosting-Provider von der Anklage der Verwirklichung von (neu) Art. 322bis Ziff. 1 Abs. 1 StGB freigesprochen, hat dies nicht zwingend zur Folge, dass die beanstandeten Informationen nicht von seinem Server entfernt werden könnten: Sofern im Urteil festgestellt ist, dass es sich dabei um eine (von einem Dritten, d.h. hier vom Content-Provider, begangene) tatbestandsmässige und rechtswidrige Tat handelt, kann das Gericht auf die Löschung dieser

[252] Nach Art. 273 ff. VE StPO sind Objekte der Beschlagnahme „Gegenstände und Vermögenswerte“.

[253] Vgl. BGE 124 IV 121: X. war Empfänger von rassendiskriminierenden Zeitschriften und CDs. Das kantonale Obergericht sprach ihn mangels Erfüllung des subjektiven Tatbestandes vom Vorwurf frei, Art. 261bis StGB verletzt zu haben, zog aber die Zeitschriften und CDs ein. Das Bundesgericht bestätigte die Einziehung mit der Überlegung, der unbekannt gebliebene Absender (aus den USA) habe die objektiven und subjektiven Merkmale von Art. 261bis Abs. 1 StGB verwirklicht, und da Art. 58 StGB die Einziehung „alors même qu’aucune personne déterminée n’est punissable“ erlaubt, komme es weder darauf an, dass die Personen, die das Material verbreitet hatten, nicht identifiziert oder in der Schweiz verfolgt werden konnten, noch darauf, dass X. nicht selber Täter oder Teilnehmer der Tat gewesen sei (vgl. a.a.O., S. 126).

Informationen erkennen. Die spezifische Gefährlichkeit der Informationen, die Art. 58 StGB für die Gegenstände eigens erwähnt, ist in solchen Fällen nur dann nicht weiter zu prüfen, wenn es um eine strafbare Handlung geht, die eine spezifische Einziehungsbestimmung kennt (also bei den Art. 135 Abs. 2, 197 Ziff. 3 Abs. 2 und Ziff. 3bis Abs. 2 StGB).

- Diese Lösung erfährt allerdings eine Einschränkung: Das Bundesgericht hat vor kurzem klargestellt (die Frage war in der Lehre umstritten [254]), dass eine Einziehung von in der Schweiz liegenden Vermögenswerten nach Art. 59 StGB nur dann möglich ist, wenn über die Tat, aus der diese Werte hervorgegangen sind, schweizerische Gerichtsbarkeit besteht [255]. Angesichts der Argumentation im zitierten Bundesgerichtsentscheid dürfte dies auch für die hier interessierende Sicherungseinziehung gelten [256]. Fehlt es somit an der schweizerischen Strafhoheit über die Tat des Content-Providers, würde nach den allgemeinen Regeln die Möglichkeit entfallen, bei einem Freispruch des Hosting-Providers die rechtswidrigen Informationen zu löschen. Dasselbe gilt für ein selbständiges [257] Einziehungs- bzw. Löschungsverfahren gegen den Hosting-Provider.

- Aus diesem Grund hat sich die Expertenkommission entschlossen, die Löschung „ungeachtet schweizerischer Strafhoheit“ zu ermöglichen. Es wäre eine rechtspolitisch unbefriedigende Situation, wenn zwar in dem den Hosting-Provider freisprechenden Urteil festgestellt würde, ein Content-Provider habe einen tatbestandsmässig-rechtswidrigen Inhalt auf dessen Server geladen, eine Löschung der entsprechenden Informationen sei jedoch nicht möglich, weil über die Tat des Content-Providers keine schweizerische Strafhoheit bestehe. Denn es liegt der Spezialregelung von (neu) Art. 322bis Ziff. 1 StGB nicht nur an der näheren Bestimmung der Strafbarkeit des Hosting-Providers, sondern auch an der Bereitstellung einer Handhabe, um die Nutzung der Information zu verhindern.

  Das bedeutet, dass mit dieser Lösung die Diskussion um den Begriff des Erfolges in Art. 7 StGB bzw. die Deliktsnatur (Erfolgs-/Tätigkeitsdelikte) der jeweiligen Straftaten ein Stück weit entschärft wird: Sie ist nur noch insofern von Belang, als es um die Frage geht, ob der Content-Provider schweizerischer Strafhoheit untersteht. Hingegen ist sie nicht (mehr) relevant in Bezug auf die Ergebnisse, die seine Straftat zeitigt, weil als Anknüpfungspunkt nur noch darauf abgestellt wird, ob diese Ergebnisse bei einem Provider mit Sitz in der Schweiz gehostet werden.

  Kurz: Es kommt für die Löschung nicht darauf an, ob über die Tat des Content-Providers schweizerische Strafhoheit vorliegt. Auch wenn das nicht der Fall ist, werden die Informationen auf dem Internet-Server des Hosting-Providers gelöscht. Dafür sind *zwei Arten von Verfahren* denkbar: Entweder wird gegen den Hosting-Provider wegen des Verdachts der Verletzung von neu Abs. 1

---

[254] Nachweise bei SCHMID (Bibl.), N 31 zu Art. 58.

[255] BGE 128 IV 145.

[256] Die Art. 3-7 StGB stellten Anwendungsregeln des StGB dar, als dessen Teil Art. 59 anzusehen sei (S. 151). – Inwiefern darin ein Widerspruch zu BGE 124 IV 241 liegt, ist unklar. Dieser Entscheid übergeht die Frage und äussert sich nicht dazu, ob die durch den Absender der Zeitschriften und CDs begangene Rassendiskriminierung als in der Schweiz begangen zu gelten hat.

[257] Dazu SCHMID (Bibl.), N 80 zu Art. 58.

bereits ein Verfahren geführt, in dessen Rahmen unabhängig vom Verfahrensausgang die Löschung angeordnet werden kann. Oder es wird, wenn kein Verdacht auf Verletzung von Abs. 1 vorliegt, ein selbständiges Löschungsverfahren eingeleitet. Sofern das Gericht zum Schluss kommt, ein bestimmter Inhalt sei tatbestandsmässig-rechtswidrig, ordnet es dessen Löschung an.

Ein entsprechendes Löschungsverfahren ist vorläufig durch das kantonale Strafprozessrecht zu gewährleisten (z.B. § 106a f. der Zürcher StPO) [258], wobei der Gerichtsstand – falls sich aus (neu) Art. 340ter StGB keine Bundeszuständigkeit ergibt – sinnvollerweise dem Ort der Verbreitung, d.h. am Standort des Host-Servers, zuzuweisen ist (vgl. die ähnliche Regelung bei Mediendelikten, Art. 347 Abs. 2 StGB). Auf eine explizite Bestimmung der örtlichen Zuständigkeit für dieses eigenständige Löschungsverfahren kann verzichtet werden [259].

9.352 Löschung im Fall von Abs. 2

Auch dort, wo ein Strafverfahren nach Abs. 2 eingeleitet worden ist, weil ein Hosting-Provider einen Hinweis nicht weitergeleitet hat, ist die Löschung ein notwendiges Mittel zur Entfernung der rechtswidrigen Informationen. Sie ist aus denselben Überlegungen ausdrücklich erwähnt, die zur Löschung im Fall von Abs. 1 angestellt worden sind. Insbesondere ist bei einem Freispruch des Hosting-Providers die Situation zu vermeiden, dass sich im Verfahren zwar die Feststellung treffen lässt, der Hinweis beziehe sich auf eine Information, mittels deren eine strafbare Handlung begangen wird (was gemäss Abs. 4 nach schweizerischem Recht zu beurteilen ist), über welche indessen keine schweizerische Strafhoheit besteht, so dass sie auf dem Internet-Server des Hosting-Providers nicht gelöscht werden könnte.

Dazu kommt im Fall von Abs. 2, selbst wenn am Ende des Verfahrens eine Verurteilung steht, dass unsicher ist, ob der Konnex zwischen der Tathandlung (Unterlassen der Weiterleitung des Hinweises) und den („strafbaren“) Informationen genügend eng ist: Kann man von den Informationen sagen, sie hätten „zur Begehung einer strafbaren Handlung gedient“? Diese Unsicherheiten verlieren mit der expliziten Regelung in Abs. 5 ihre Bedeutung: Die Informationen, auf die der Hosting-Provider hingewiesen wird (und deren unterlassene Weiterleitung ihm allenfalls zum Vorwurf gemacht wird) können gelöscht werden, sofern sich im Verfahren ergibt, dass mit ihnen eine strafbare Handlung begangen wird.

---

[258] Bei der Ausarbeitung der Eidgenössischen Strafprozessordnung ist diesem Sonderverfahren entsprechend Rechnung zu tragen (vgl. Art. 45 VE bezüglich eigenständige Einziehungsverfahren).

[259] Auch der Gerichtsstand für selbständige Einziehungsverfahren (Art. 58 f. StGB) wird im Gesetz nicht näher definiert, vgl. SCHMID (Bibl.) Art. 58 N 81; Art. 59 N 139 „Art. 346 ff. StGB nicht anwendbar“.

9.4 Kommentar zu (neu) Art. 340ter StGB

9.41 Problemlage

In mehreren Fällen von Netzwerkkriminalität hat sich gezeigt, dass die generelle Zuständigkeit der kantonalen Behörden für die meisten der interessierenden Straftatbestände nicht zu einer effektiven Strafverfolgung geführt hat. In einer Grossaktion („Genesis“) gegen Kunden eines internetbasierten Kinderpornographieanbieters im Herbst 2002 wurde deutlich, dass dem Bundesamt für Polizei die rechtlichen Grundlagen für eigene Ermittlungen oder eine verbindliche Koordination der kantonalen Ermittlungsverfahren fehlten. Dies führte u.a. zu *Verzögerungen* in der Erhebung der Adressen von Tatverdächtigen bei den Kreditkartenunternehmen und zu einer schlecht abgestimmten *Informationspolitik*. Auch im internationalen Vergleich war das Vorgehen der Schweizer Behörden *verspätet*.

In hochkomplexen Fällen von grenzüberschreitenden Computerdelikten, die über Netzwerke ablaufen, fehlt es an *spezialisierten Kriminalisten* und entsprechender Ausrüstung auf kantonaler Ebene.

Schliesslich ist zu Beginn der Ermittlungen auch häufig *unklar, welche kantonale Behörde für die Verfolgung zuständig* ist. So ermittelten im Fall des sog. „WEF-Hacks“ [260] zunächst die Genfer Behörden, weil der betroffene Web-Server am Sitz des World Economic Forum (WEF) stand. Der Fall wurde nach aufwändigen Ermittlungen dann an die Berner Behörden weitergeleitet, als ein Tatverdächtiger mit Wohnsitz in diesem Kanton ausfindig gemacht werden konnte. In Fällen von Erfolgsanknüpfung im Inland kann es zu einer Vielzuständigkeit kommen, wenn ein Erfolg überall eintritt (z.B. Kenntnisnahme bei Ehrverletzungen). Gemäss Art. 346 Abs. 2 StGB wäre dann jener Kanton zuständig, der die Untersuchung zuerst angehoben hat; das kann aber von Zufälligkeiten abhängen [261].

9.42 Postulate der Expertenkommission

Vor dem Hintergrund dieser Erfahrungen ist eine zentrale Spezialabteilung beim Bundesamt für Polizei wünschenswert, die gestützt auf eine klare Zuständigkeitsnorm als *Clearing-Stelle* für grössere oder grenzüberschreitende Delikte wirken sollte. Im Bereich dieser komplexen Straftaten, die mittels eines elektronischen Netzwerkes ausgeführt werden, sollen speziell ausgebildete Kriminalisten einen schnellen, interkantonal wie international koordinierten Zugriff vornehmen können. Dies ist im Grundsatz unbestritten und auch international das favorisierte Modell (USA, Japan, Italien, Österreich).

Gleichzeitig ist es aber nicht erstrebenswert, für alle möglichen Delikte, bei denen beispielsweise ein E-Mail eingesetzt wurde, oder für Bagatellfälle eine

---

[260] Zusammenfassend zu diesem Fall: SCHWARZENEGGER, E-COMMERCE (Bibl.), S. 333 m.N.

[261] Zum Gerichtsstand bei Internetdelikten nach geltendem Recht (Art. 346 ff. StGB), s. oben Kapitel 6, Ziff. 6.4.

Bundeskompetenz einzuführen. Solche Fälle müssen durch eine entsprechende Formulierung in der Kompetenznorm ausgeschieden werden.

Nach Abschluss der Sachverhaltsermittlung und komplizierten Beweissicherungen ist es ausserdem nicht notwendig, den Fall im Bundesstrafverfahren zu Ende zu führen. Vielmehr erscheint ein *gemischtes Modell* effektiver sowie institutionell und finanziell leichter zu verwirklichen.

9.43 Grundzüge des vorgeschlagenen Modells

9.431 Im Allgemeinen

Dieses Modell sieht eine *zentrale Einheit* zur Bekämpfung der Netzwerkkriminalität vor. Dies könnte durch den Ausbau der Koordinationsstelle zur Bekämpfung von Internetkriminalität (KOBIK) abgedeckt werden, die zunächst unter der Verfahrensleitung eines Staatsanwaltes des Bundes ermittelt. Diese Stelle ist zudem für den Kontakt und Informationsaustausch mit den Cybercrime-Einheiten anderer Länder zuständig.

Nach der Ermittlungsphase werden die einfacheren Fälle an die kantonalen Strafverfolgungsbehörden delegiert, worauf ein kantonaler Untersuchungsrichter, Bezirksanwalt oder Staatsanwalt die Anklage vor dem kantonal zuständigen Gericht erhebt.

Gleich wie bei der Bundesgerichtsbarkeit in Fällen von organisiertem Verbrechen (Art. 340bis Abs. 1 StGB) kann der Bundesanwalt die Bundesstrafsache nach Abschluss der Voruntersuchung der kantonalen Behörde zur Beurteilung übertragen und dabei selbst die Anklage vertreten.

9.432 Zwingende oder fakultative Bundeskompetenz?

9.432.1 Im Allgemeinen

Für die konkrete Kompetenzregelung besteht die Wahl zwischen einer zwingenden Norm mit Beschränkung auf grössere oder grenzüberschreitende Internetdelikte (analog Art. 340bis Abs. 1 StGB) und einer Kann-Vorschrift (analog Art. 340bis Abs. 2 StGB).

Im Sinne einer möglichst klaren Regelung tritt die *Expertenkommission für eine zwingende Vorschrift* ein. Das heisst, bei Vorliegen der (eingeschränkten) Voraussetzungen sind die Bundesbehörden zur Verfolgung und Beurteilung zuständig. Die bisherigen Erfahrungen der Bundeskriminalpolizei haben etwa im Bereich der Organisierten Kriminalität gezeigt, dass die Anwendung von Art. 340bis Abs. 1 StGB unproblematisch ist. Ein *Vorteil* der vorgeschlagenen Version liegt darin, dass sie für die kantonalen Strafverfolgungsbehörden und die Bundesanwaltschaft *klare Verhältnisse* schafft. Mit den zwei genannten Voraussetzungen der Bundeskompetenz wird die Filterwirkung gegenüber allerlei einfachen Internetsachverhalten gesichert.

9.432.2 (neu) Art. 340ter StGB im Besonderen

(Neu) Art. 340ter *Abs. 1 lit. a* StGB orientiert sich an Art. 340bis Abs. 1 lit. b StGB, während (neu) Art. 340ter *Abs. 1 lit. b* StGB eine wichtige Ergänzung hinsichtlich der Koordinationsfunktion im Ermittlungsverfahren enthält, wenn eine Vielzahl gleichartiger Fälle in verschiedenen Kantonen auftreten (Stichwort „Genesis“).

Als *Kann-Vorschrift* wird dagegen die Übernahme der Strafverfolgung durch die Bundesanwaltschaft auf Ersuchen eines Kantones ausgestaltet: (neu) Art. 340ter *Abs. 2* StGB. Im weiteren Verlauf des Verfahrens ist mit der Delegation an die kantonalen Behörden ein zusätzlicher Filter vorzusehen.

Ein solcher ist schon in *Art. 18bis BStP* angelegt. Nach dieser Bestimmung kann der Bundesanwalt einen Fall nach Abschluss der Voruntersuchung an eine kantonale Behörde übertragen (Art. 18bis Abs. 1 BStP), wobei er in einfachen Verfahren sowohl Untersuchung und Anklage als auch die Beurteilung an die kantonalen Behörden delegieren kann (Art. 18bis Abs. 2 BStP).

An der Delegationsbefugnis des Bundesanwaltes wird sich auch nach Inkrafttreten des *Bundesgesetzes über das Bundesstrafgericht* (SGG) nichts ändern, da in dessen Art. 26 ausdrücklich vorbehalten bleibt, dass der Bundesanwalt die Untersuchung und Beurteilung den kantonalen Behörden übertragen kann.

9.44 Einzelbemerkungen zu (neu) Art. 340ter StGB

- Der vorgeschlagene (neu) Art. *340ter Abs. 1 lit. a* StGB erfasst sowohl komplexe nationale Sachverhalte (vgl. WEF-Hack), bei denen der Gerichtsstand zunächst unklar bleiben kann, als auch grenzüberschreitende Delikte, die mehrere Kantone betreffen, ohne dass es in einem von ihnen einen Schwerpunkt gibt. Diese Sachverhalte können zentral aufgegriffen und bei Bedarf wieder an einen Kanton delegiert werden.
- (Neu) Art. *340ter Abs. 1 lit. b* StGB ist eine Neuschöpfung, die auf Fälle zugeschnitten ist, in denen gegen eine Vielzahl von Tätern wegen gleichartiger Internetdelikte ermittelt werden muss und ein koordiniertes Vorgehen unabdingbar ist. Auch hier bleibt eine Delegation an die Kantone nach Art. 18bis BStP möglich.
- Art. *340ter Abs. 2* StGB ermöglicht schliesslich eine Aktivierung der Bundesbehörden auf Ersuchen der kantonalen Strafverfolgungsbehörden. Die Bundesanwaltschaft kann aber solche Ersuchen ablehnen, falls ihr eine lokale Strafverfolgung als unproblematisch erscheint. Sie hat bei dieser Entscheidung die konkreten Umstände des Einzelfalles zu prüfen.
- Art. *340ter Abs. 3* StGB macht analog zu Art. 340bis Abs. 3 StGB deutlich, dass die Anhebung eines Ermittlungsverfahrens automatisch eine Bundeskompetenz begründet.

Die Expertenkommission äussert sich im Licht ihrer strafrechtlichen Regelungsvorschläge kritisch zu derzeit parallel laufenden Gesetzgebungsverfahren im Bereich der Netzwerkkriminalität. Zudem gibt sie Empfehlungen für weitere gesetzgeberische Schritte auf diesem Gebiet.

10. Parallele Gesetzgebungsverfahren und weitere gesetzgeberische Aufgaben im Bereiche der Netzwerkkriminalität

10.1 Stellungnahme zu parallelen Gesetzgebungsverfahren

Parallel zu den Arbeiten der Expertenkommission „Netzwerkkriminalität“ sind zur Zeit verschiedene weitere Gesetzgebungsverfahren im Gange. Sie tangieren auch Fragen, mit denen sich diese Kommission auseinandergesetzt hat. Die Kommission hält es für opportun und dringlich, zu diesen parallel entstehenden Erlassen Stellung zu nehmen und auf drohende Widersprüche zwischen dem Kernstrafrecht und anderen Bundeserlassen hinzuweisen.

10.11 Bundesgesetz über den elektronischen Geschäftsverkehr

Im Begleitbericht zum Vorentwurf des Bundesgesetzes über den elektronischen Geschäftsverkehr (Teilrevisionen des Obligationenrechts und des Bundesgesetzes gegen den unlauteren Wettbewerb) vom 17. Januar 2001 [262] findet sich u.a. folgender Passus:

> „Ebenfalls wesentlich von der internationalen Rechtsentwicklung hängen auch allfällige Anpassungen des Immaterialgüterrechts sowie der straf- und zivilrechtlichen Verantwortlichkeit der Provider ab. Ein unmittelbarer Handlungsbedarf besteht diesbezüglich nicht. Sachgerechte Lösungen lassen sich auf der Grundlage des geltenden Rechts finden“.

Die *Kommission „Netzwerkkriminalität“* divergiert in diesem Punkt. Sie ist der Ansicht, dass eine vertiefte Prüfung der zivilrechtlichen Haftungsfragen bzw. -beschränkungen im Zusammenhang mit der automatisierten Datenübermittlung und -bereitstellung in Netzwerken erwünscht wäre [263]. Die entsprechenden Fragen könnten einerseits im Rahmen der laufenden Gesetzgebung über den elektronischen

[262] Abrufbar unter: www.ofj.admin.ch/themen/e-commerce/vn-ber-b-d.pdf
[263] Vgl. oben Kapitel 8, am Ende, sowie unten Kapitel 11. Ziff. 11.33.

Geschäftsverkehr behandelt werden. Wegen der grundsätzlichen Bedeutung dieser Frage müsste eine entsprechende Ergänzung allerdings einer erneuten separaten Vernehmlassung zugeführt werden. Andererseits wäre eine abgestufte Haftungsbeschränkung für die verschiedenen Providergruppen auch im Rahmen der Revisionsarbeiten am *Urheberrechtsgesetz* oder der *Haftpflichtrechtsrevision* möglich.

10.12 Bundesgesetz über die Lotterien und Wetten

Über den Entwurf vom 25. Oktober 2002 zu einem revidierten Bundesgesetz über die Lotterien und Wetten hat bis 31. März 2003 ein *Vernehmlassungsverfahren* stattgefunden [264].

Art. 50 lit. d des Entwurfes lautet wie folgt:

> „Art. 50 Vergehen
>
> *[1] Mit Gefängnis bis zu einem Jahr oder mit Busse bis zu 1 Million Franken wird bestraft, wer:*
> *...*
> *d. als Zugangsvermittler (Provider) nicht bewilligte Spiele nach diesem Gesetz vermittelt.*
>
> [2] In schweren Fällen ist die Strafe Zuchthaus bis zu fünf Jahren oder Gefängnis nicht unter einem Jahr. Damit kann zusätzlich eine Busse bis zu zwei Millionen Franken verbunden werden.
>
> [3] Wer fahrlässig handelt, wird mit Busse bis zu 500 000 Franken bestraft."

Der *Begleitbericht* äussert sich zu Art. 50 Abs. 1 lit. d des Entwurf folgendermassen:

> „Die angedrohten Höchstbussen liegen deutlich über den Bussenmaxima des Allgemeinen Strafrechts. Nach Ansicht der Kommission rechtfertigt sich die Höhe der Bussen aufgrund der grossen wirtschaftlichen Interessen, die auf dem Spiel stehen. Nur empfindliche Sanktionen können dazu beitragen, dass in- und ausländische Veranstalterinnen und Veranstalter die Vorschriften des Gesetzes respektieren und die Strafen nicht von vornherein bereits mit in ihr Kalkül einbeziehen.
>
> Die Kommission ist zudem überzeugt, dass das Anbieten von nicht bewilligten Lotterien und Wetten im Internet nur dann wirksam bekämpft werden kann, wenn auch die Zugangsvermittler (Provider) ins Recht gefasst werden " [265].

Die *Expertenkommission „Netzwerkkriminalität"* ist in diesem Punkte anderer Ansicht. Sie erachtet die aus einer solchen Strafbestimmung entstehenden Kontrollpflichten der Access-Provider aus verfassungs- und verwaltungsrechtlicher Perspektive als unzulässig, weil unverhältnismässig. Die Massnahme einer lokalen Sperrung ist aus technischer Sicht kaum wirksam, weil eine Vielzahl von Umgehungsmöglichkeiten bestehen, die ausserhalb der Kontrolle des jeweiligen Access-Providers liegen. Nicht

---

[264] Abrufbar unter: www.ofj.admin.ch/themen/lotterie/lg-rev/intro-d.htm
[265] Erläuternder Bericht zum Entwurf eines Bundesgesetzes über die Lotterien und Wetten, vom 25. Oktober 2002, 44.

zuletzt würde die Strafbarkeit des Zugangsvermittlers auch dem im europäischen Umfeld geltenden Recht widersprechen [266].

Aus strafrechtlicher Sicht würde eine entsprechende Pflicht zur Kontrolle bzw. Sperrung nicht nur unverhältnismässig erscheinen; sie würde zudem eine Strafbarkeit für völlig legale wirtschaftliche Tätigkeiten begründen, obwohl der ins Recht gefasste Zugangsvermittler – anders als etwa im Bereich der Geldwäscherei – mit dem für das Unrecht verantwortlichen Betreiber der illegalen Lotterie oder Wette keinerlei Kontakt hat, diesen nicht kennt und von seinen Handlungen auch nicht profitiert.

Der von der Expertenkommission vorgeschlagene Strafbarkeitsausschluss für reine Zugangsvermittlung ([neu] Art. 27 Ziff. 4 StGB) soll auch für das gesamte Nebenstrafrecht gelten (vgl. Art. 333 Abs. 1 StGB). Mit einer abweichenden Bestimmung im Bundesgesetz über die Lotterien und Wetten würde die angestrebte Einheitlichkeit der Neuregelung grundlos aufgegeben. Art. 50 lit. d des Entwurfs zum Bundesgesetz über die Lotterien und Wetten sollte deshalb ersatzlos gestrichen werden.

10.13 Bundesgesetz über Massnahmen gegen Rassismus, Hooliganismus und Gewaltpropaganda

Bis zum 31. Mai 2003 dauerte die *Vernehmlassung* zum Bundesgesetz über Massnahmen gegen Rassismus, Hooliganismus und Gewaltpropaganda [267].

Eine darin enthaltene Änderung des Bundesgesetzes vom 21. März 1997 über Massnahmen zur Wahrung der inneren Sicherheit (BWIS, SR 120) lautet:

> „Art.13bis Sicherstellung, Beschlagnahme und Einziehung von Propagandamaterial (neu)
>
> [1] Die Polizei- und die Zollbehörden stellen zuhanden des Bundesamtes, ungeachtet der Menge, Beschaffenheit und Art, Material sicher, das Propagandazwecken dienen kann und dessen Inhalt:
> a. rassendiskriminierend ist; oder
> b. konkret und ernsthaft zur Gewalt gegen Personen oder Gruppen von Personen oder zu deren Schädigung am Vermögen oder an anderen Rechten aufruft.
> [2] Wenn Mitarbeiterinnen und Mitarbeiter des Bundesamtes entsprechendes Material antreffen, können sie es auch direkt sicherstellen.
> [3] Liegt ein Verdacht auf eine strafbare Handlung vor, so übermittelt die sicherstellende Behörde das Material der zuständigen Strafbehörde.
> [4] In den übrigen Fällen übermitteln die Polizei- und die Zollbehörden das Material dem Bundesamt. Dieses entscheidet über die Beschlagnahme und die Einziehung. Das Bundesgesetz vom 20. Dezember 1968 über das Verwaltungsverfahren ist anwendbar.
> [5] Bei Verbreitung von Propagandamaterial nach Absatz 1 über das Internet kann das Bundesamt den Internet-Providern die Sperrung der entsprechenden Internetseiten empfehlen.“

[266] Vgl. Art. 12 E-Commerce-Richtlinie; oben Kapitel 4.
[267] Abrufbar unter: www.ejpd.admin.ch/doks/mm/2003/030212c-d.htm.

Zum hier besonders interessierenden *Abs. 5* der Bestimmung sagt der entsprechende *Bericht* Folgendes aus:

> "Zu Art. 13bis Abs. 5 E- BWIS: Auf Empfehlungen in der Ämterkonsultation sieht der neue Artikel auch ein Handeln des zuständigen Bundesamtes vor, was die Verbreitung von Propaganda gemäss Buchstabe a und b des neuen Artikels im Internet betrifft. Das Bundesamt kann den zuständigen Internet-Providern eine Sperrung der entsprechenden Propaganda nahe legen. Diese Sperrung erfolgt nur bei Sites, die auf Computern im Ausland geführt werden. Bei inländischen Websites erfolgt eine Anzeige an den Strafrichter."

Der dem Entwurf und Bericht vorangegangene Bericht der *Arbeitsgruppe Rechtsextremismus* (AG Rechtsextremismus) vom September 2000 [268] hatte demgegenüber noch betont, dass die Strafverfolgung hinsichtlich Internet-Inhalten auf europäischen Servern keine übermässigen Probleme aufwerfe [269], dass aber umgekehrt die Sperrung entsprechender Inhalte durch (schweizerische) Internet Service Provider vielfältige technische Probleme mit sich bringe [270].

Entsprechend hatte die Arbeitsgruppe empfohlen, die zuständigen Behörden anzuweisen,

- weiterhin in Zusammenarbeit mit Schweizer Providern dahingehend zu wirken, dass die Verbreitung rechtsextremer Inhalte auf dem Internet bekämpft werde,
- internationale Anstrengungen zur Schaffung einer Konvention bezüglich der verbotenen Inhalte auf dem Internet zu unternehmen,
- den diplomatischen Druck auf Staaten, die Ausgangspunkt für die Verbreitung solcher Inhalte darstellen, aufrecht zu erhalten oder zu verstärken [271].

Die *Expertenkommission „Netzwerkkriminalität"* hält mit den ursprünglichen Empfehlungen zwar eine Zusammenarbeit der Behörden mit den Providern für durchaus positiv. Sie erachtet aber Abs. 5 des neu zu schaffenden Art. 13bis BWIS als unnötig. Blosse Empfehlungen der zuständigen Behörden, welche bei Nichtbeachtung ohne straf-, zivil- oder verwaltungsrechtliche Folgen bleiben, bedürfen keiner expliziten gesetzlichen Grundlage und sind schon nach jetziger Rechtslage möglich.

Eine Kompetenz der Bundesbehörden zur Anordnung einer Sperrung entsprechender Inhalte durch Access-Provider wäre aus den genannten Gründen unverhältnismässig (vgl. oben Ziff. 7.215) und könnte folglich auch nicht auf Art. 13bis Abs. 5 E-BWIS gestützt werden. Die etwas ungenaue Kommentierung der Norm im Begleitbericht sollte in diesem Sinne korrigiert werden. Um Missverständnisse auszuräumen, tritt die Expertenkommission für eine Streichung von Art. 13bis Abs. 5 E-BWIS ein.

---

[268] Abrufbar unter: www.bap.admin.ch/d/aktuell/berichte/bericht-d-ag-rex-d-01-s.pdf
[269] Bericht der AG Rechtsextremismus, S. 28.
[270] Bericht der AG Rechtsextremismus, S. 41.
[271] Bericht der AG Rechtsextremismus, S. 44.

10.2 Weitere gesetzgeberische Aufgaben im Bereich der Netzwerkkriminalität

Die Expertenkommission hat sich zu Beginn ihrer Beratungen für ein *etappenweises Vorgehen* entschieden. *Erste Priorität* wurde dabei der Klärung von Strafbarkeitsschranken bei automatisierter Datenübertragung und -bereithaltung in Netzwerken eingeräumt; dabei waren die parallelen Fragestellungen des öffentlichen Rechts und des Zivilrechts einzubeziehen. Vorrangig behandelte sie auch die Frage der Schaffung neuer Rahmenbedingungen für eine *effektive Bekämpfung der Internetkriminalität*.

Dabei steht die Schaffung zentralisierter Ermittlungskompetenzen und einer Clearing-Zentrale auf Bundesebene im Vordergrund; damit soll eine schnelle Reaktion und internationale Koordination in komplexen Fällen gewährleistet werden, ohne damit die Bundeskompetenzen unnötig aufzublähen. Daneben geht es um die Einführung eines strafrechtlichen Instrumentariums für die Beseitigung von inkriminierten Informationen, soweit sie in der Schweiz bereitgestellt bzw. -gehalten werden. Diese Zielsetzung entspricht jener der Motion Pfisterer (vgl. oben Ziff. 1.21) und ebenso dem Auftrag des EJPD an die Expertenkommission (vgl. oben Ziff. 1.3).

Die Expertenkommission hält ausdrücklich fest, dass mit ihren Vorschlägen *erst ein erster Schritt* auf dem Weg zu griffigen strafrechtlichen Rahmenbedingungen und einer effizienten Verfolgung der Netzwerkkriminalität getan wird. Weitere müssen folgen.

10.21 Anpassung des innerstaatlichen Rechts an die Cybercrime-Konvention

Als nächstes ist zügig mit den Gesetzesanpassungen im Hinblick auf die Ratifikation der Convention on Cybercrime (Convention sur la cybercriminalité, CCC) vom 23. November 2001 (ETS Nr. 185) [272] zu beginnen, zu deren 31 Erstunterzeichnerstaaten die Schweiz gehört. Dieses Europarats-Übereinkommen macht verschiedene Änderungen im innerstaatlichen Strafrecht und insbesondere im Strafprozessrecht erforderlich.

10.211 Inhalt der Konvention

Die Cybercrime-Konvention verfolgt erstens das Ziel, eine *Harmonisierung der materiellen Strafbestimmungen* auf dem Gebiete der Computer- und Netzwerkkriminalität herbeizuführen [273].

---

[272] Der Wortlaut der Cybercrime-Convention ist unter http://conventions.coe.int im Internet abrufbar.

[273] Kapitel II Abschnitt 1 der Konvention. Neben den Delikten gegen die Vertraulichkeit von Computerdaten und –systemen (Art. 2–3 CCC) definiert das Übereinkommen auch den Eingriff in die Datenintegrität (Art. 4 CCC), den Eingriff in die Systemintegrität (Art. 5 CCC), den Missbrauch von Vorrichtungen (Art. 6 CCC), die Computerurkundenfälschung (Art. 7 CCC), den Computerbetrug (Art. 8 CCC), Straftaten in Bezug auf Kinderpornographie (Art. 9 CCC) und Straftaten in Zusammenhang mit Verletzungen des Urheberrechts und verwandter Schutzrechte (Art. 10 CCC). Ausserdem enthält dieser Abschnitt eine Bestimmung über die Verantwortlichkeit juristischer Personen (Art. 12 CCC). Ein *1. Zusatzprotokoll* zur Harmonisierung der materiellen Strafnormen im Bereich der *Rassendiskriminierung und Fremdenfeindlichkeit* wurde am 28. Januar 2003 zur Unterzeichnung aufgelegt. Die Schweiz hat dieses Zusatzprotokoll noch nicht unterzeichnet.

Zweitens strebt sie die Schaffung eines *einheitlichen strafprozessualen Instrumentariums* zur Ermittlung und Verfolgung von Computer- und Netzwerkdelikten an. Insbesondere soll damit die rechtzeitige Sicherung von „flüchtigen" Beweismitteln und Verbindungsdaten in elektronischer Form ermöglicht bzw. erleichtert werden [274].

Drittens versucht das Übereinkommen ein schnelleres und effizienteres *Rechtshilfe- und Auslieferungssystem* bei herkömmlichen und computerbezogenen Delikten zu etablieren; es soll bestehende Rechtshilfeübereinkommen und bilaterale Verträge ergänzen oder in die Lücke springen, wo solche fehlen [275].

Vorgesehen sind auch *provisorische Massnahmen* wie die beschleunigte Sicherung gespeicherter Computerdaten (Art. 29 CCC) oder die beschleunigte Weitergabe gesicherter Verbindungsdaten (Art. 30 CCC).

Im abschliessenden Kapitel IV der Konvention (Standardvertragsklauseln für im Rahmen des Europarates geschlossene Übereinkünfte) ist in Art. 41 CCC eine für die Schweiz zu beachtende „*Bundesstaatsklausel*" eingefügt. Danach können Bundesstaaten den Vorbehalt anbringen, die Verpflichtungen nach Kapitel II nur soweit zu übernehmen, wie sie mit den Grundprinzipien der innerstaatlichen Kompentenzausscheidung zwischen Bund und Gliedstaaten vereinbar sind. Bringt ein Bundesstaat einen solchen Vorbehalt an, muss er gleichwohl eine umfassende und wirksame Strafverfolgung nach den Grundsätzen des II. Kapitels garantieren. Da der Vorbehalt nicht auf Kapitel III ausgeweitet werden kann, sind auch alle Verpflichtungen zur grenzüberschreitenden Zusammenarbeit einzuhalten [276].

10.212 Anpassungsbedarf

Insbesondere die Anpassungen des *Strafprozessrechts*, die vorläufig noch in die Zuständigkeit der Kantone fallen, hätten den zeitlichen Rahmen des Auftrages dieser Expertenkommission gesprengt.

Zu berücksichtigen sind hierbei namentlich die laufenden Arbeiten an einer *Schweizerischen Strafprozessordnung;* mit ihnen ist die Umsetzung der Vorgaben der Cybercrime-Konvention zu koordinieren. Daneben steht aber auch die Änderung des *Bundesgesetzes betreffend die Überwachung des Post- und Fernmeldeverkehrs* (BÜPF, SR 780.1) und der zugehörigen Verordnung über die Überwachung des Post- und Fernmeldeverkehrs (VÜPF; SR 780.11) zur Debatte, sieht doch die Cybercrime-Konvention weitergehende Befugnisse im Hinblick auf die Erlangung von sogenannten Randdaten vor.

---

[274] Kapitel II Abschnitt 2 der Konvention. Von besonderer Bedeutung ist der erweiterte Geltungsbereich dieser Normen. Sie sind nicht nur auf Straftaten gemäss den Art. 2–11 CCC anwendbar, sondern auf alle mittels Computersystemen begangenen Straftaten und alle Massnahmen zur Sicherung elektronischer Beweismittel (Art. 14 Abs. 2 lit. b und c CCC).

[275] Kapitel III der Konvention.

[276] Vgl. hierzu OFFICE FEDERAL DE LA JUSTICE, Rapport national de la Suisse sur la prévention et la lutte contre la cybercriminalité, Conférence sur la Cybercriminalité, Budapest, 22 novembre 2001; CHRISTIAN SCHWARZENEGGER: Die internationale Harmonisierung des Computer- und Internetstrafrechts durch die Convention on Cybercrime vom 23. November 2001, in: Festschrift Trechsel, Zürich 2002, S. 305 ff. m.w.N.

Darüber hinaus werden auch Anpassungen der *Strafnormen des Besonderen Teils* des StGB notwendig.

Die Cybercrime-Konvention setzt einen flexiblen Regelungsrahmen, der vielfach Erklärungen (vgl. Art. 40 CCC) bzw. Vorbehalte (vgl. Art. 42 CCC) durch die Unterzeichnerstaaten zulässt, womit eine eingeschränkte Umsetzung ermöglicht wird. Daher muss zunächst bestimmt werden, ob für die Schweiz eher eine Minimallösung oder eine möglichst umfassende Anpassung anzustreben ist.

10.213 Empfehlungen der Experternkommission

Der Expertenkommission empfielt, die sich aus der Cybercrime Convention ergebenden Probleme – sei es im Rahmen einer Mandatserweiterung dieser Kommission, sei es im Rahmen einer weiteren Expertenkommission – aufzugreifen und einer Lösung im Strafgesetzbuch, in einem eigenständigen Bundesgesetz über strafprozessuale Zwangsmassnahmen im Bereiche der Netzwerkkriminalität sowie im BÜPF/VÜPF zuzuführen.

Mit einem baldigen Ende der Arbeiten an der Schweizerischen Strafprozessordnung ist nicht zu rechnen. Da eine Umsetzung der Cybercrime-Konvention im Interesse der effizienten Verfolgung der Netzwerkkriminalität von besonderer Dringlichkeit ist (siehe unten Ziff.10.22) und es sich dabei ausserdem um eine Spezialmaterie handelt, hält es die Expertenkommission für angezeigt, die Vorbereitungen zur Ratifikation der Cybercrime Convention sofort an die Hand zu nehmen. Auf kantonaler Ebene dürften die erforderlichen strafprozessualen Instrumente nicht mehr selbständig implementiert werden.

10.22 Ergänzung des BÜPF [277] zur Bestimmung des Tatortes

Zentraler Anhaltspunkt bei der Verfolgung strafrechtlich relevanter Tätigkeiten und Inhalte auf dem Internet ist die in fast jeder Art von Internetkommunikation übermittelte *IP-Adresse* [278]. Sie allein bietet namentlich bei Tätigkeitsdelikten die Möglichkeit, die *örtliche Zuständigkeit* rasch zu klären und allfällige Beweissicherungsmassnahmen einzuleiten.

Ist der Täter über eine sogenannte *statische IP-Adresse* mit dem Internet verbunden, so können in Anwendung von Art. 14 BÜPF (in Verbindung mit Art. 27 lit. a VÜPF) unter anderem die schweizerischen Polizeibehörden auch ausserhalb eines formellen Strafverfahrens Namen und Wohnadresse der Teilnehmerin oder des Teilnehmers erfahren; dabei unterstützt sie der Dienst für besondere Aufgaben (DBA), welcher dem UVEK administrativ unterstellt ist.

In der Mehrheit der Fälle verfügt der Täter jedoch über keine statische IP-Adresse. Vielmehr wird ihm vom angewählten Internet Provider für jede Internet-Sitzung eine IP-Adresse (sog. *dynamische IP-Adresse*) zugeteilt. Seine Wohnadresse ist dann nur über eine richterliche Anordnung und damit nur im Rahmen eines formellen

[277] Bundesgesetz vom 6. Oktober 2000 betreffend die Überwachung des Post- und Fernmeldeverkehrs (SR 780.1).

[278] Internet-Protokoll-Adresse: Eindeutige viergliedrige Zahl, die jedem mit dem Internet verbundenen Rechner zugewiesen wird.

Strafverfahrens in Erfahrung zu bringen (vgl. Art. 24 lit. f VÜPF). Denn die individuellen Angaben zur dynamischen IP-Adresse sind als Rand- und Rechnungsdaten vom Fernmeldegeheimnis nach Art. 43 FMG mitumfasst. Die kantonale örtliche Zuständigkeit ist hier nur bis zum Sitz des Providers bestimmbar, was in vielen Fällen (insbesondere bei grossen Providern mit nationaler Kundschaft) zu unbefriedigenden und ineffizienten Ergebnissen führt.

Im Interesse einer *effizienten Strafverfolgung* ist jedoch unabdingbar, dass die von den Kantonen und vom Bund betriebene Koordinationsstelle zur Bekämpfung der Internet-Kriminalität (KOBIK) auch *ausserhalb eines formellen Strafverfahrens* möglichst rasch Kenntnis vom Einwählort [279] erlangt, damit eine korrekte Zuweisung an die zuständigen Behörden erfolgen kann.

Obwohl diese Information an sich keine Rückschlüsse auf die Fernmeldeteilnehmerin oder den Fernmeldeteilnehmer beziehungsweise auf Umfang und Dauer der Internetverbindung zulässt, ist nach geltendem BÜPF davon auszugehen, dass es sich um *Randdaten* handelt, die nur unter den Voraussetzungen von Art. 3 i.V.m. Art. 5 BÜPF erlangt werden können. Nachdem die Cybercrime-Konvention eine beschleunigte Sicherung von Verbindungsdaten verlangt (Art. 16 CCC), für die sie ein weniger hohes Schutzniveau statuiert als für *Inhaltsdaten*, ist anlässlich der zu leistenden Anpassungsarbeiten (vgl. oben Ziff. 10.21) vordringlich zu diskutieren, wie die entsprechende Differenzierung zwischen Rand- und Inhaltsdaten in einem revidierten BÜPF auszugestalten ist.

Dabei wird im Auge zu behalten sein, dass der erleichterte Zugriff auf diese Randdaten – er könnte etwa mittels Verfügung anstelle der Überwachungsanordnung erfolgen – auch für die Tatortbestimmung von zentraler Bedeutung ist, welche die Strafhoheit und den Gerichtsstand determiniert; nach der hier vorgeschlagenen neuen Kompetenzregelung ([neu] Art. 340ter StGB) wird der Zugriff in vielen Fällen durch KOBIK durchzuführen sein.

[279] Gemeint ist der Telefon- oder Kabelanschluss, von dem aus der Teilnehmer eine Verbindung zum Internet aufbaute.

11. Zusammenfassung

11.1 Allgemein

Das Thema „Netzwerkkriminalität“ ist in sachlicher und rechtlicher - sowie auch in politischer - Hinsicht *facettenreich* und komplex.

Die Expertenkommission war bestrebt, einen *möglichst breiten Überblick* über die Thematik zu gewinnen und sich mit allen wesentlichen Aspekten auseinanderzusetzen. Dabei hat sie aber bewusst *Schwerpunkte gesetzt* und bestimmte Bereiche grundlegend und intensiv diskutiert (vgl. unten Ziff. 11.2), andere aber mit einem *geringeren Vertiefungsgrad* behandelt (vgl. unten Ziff. 11.3).

Dass die Kommission auf den Themenkomplex „*Strafrecht*“ (vgl. unten Ziff. 11.2) besonderes Gewicht gelegt hat, hängt mit dem ihr erteilten Auftrag zusammen, der primär die Prüfung der strafrechtlichen Verantwortlichkeit im Internet zum Gegenstand hat. Es war insbesondere die umstrittene Frage der strafrechtlichen *Verantwortlichkeit der Internet-Provider,* die einen der Auslöser für ihre Einsetzung bildete. Hinzu kommt das aktuelle, Öffentlichkeit und Politik stark bewegende Problem der *Pädokriminalität* (und einiger weiterer Verbrechensformen), für welche das Internet zunehmend als Tatmittel eingesetzt wird.

11.2 Schwerpunkt Strafrecht (Kapitel 6 und 9)

11.21 Strafrechtliche Verantwortlichkeit

Problem

Das geltende Strafrecht enthält keine klare, ausdrückliche Regelung der Verantwortlichkeit im Zusammenhang mit illegalen Internet-Inhalten. Ob und inwieweit die Vorschriften des Medienstrafrechts und die allgemeinen Regeln des Strafgesetzbuches anwendbar seien, ist umstritten. Darum ist eine eindeutige Regelung im Gesetz angezeigt.

Lösungsvorschlag der Expertenkommission

In Anlehnung an ausländische Vorschriften, welche die E-Commerce-Richtlinie der Europäischen Union umsetzen (vgl. rechtsvergleichende Hinweise in Kapitel 4), schlägt die Expertenkommission in Kapitel 9 (v.a. Ziff. 9.2 und 9.3) *eine neue Regelung im Strafgesetzbuch* (neue Art. 27 und 322^{bis}) vor, wonach:

- der Autor und der *Content-Provider* für von ihnen ausgehende illegale Inhalte strafrechtlich voll verantwortlich sind,

- der *Hosting-Provider* beschränkt haftet, d.h. im Wesentlichen nur, wenn er die mögliche und zumutbare Vehinderung der Nutzung deliktischer Informationen wider besseres Wissen unterlässt oder von Dritten erhaltene Hinweise auf solche Informationen nicht an die Strafverfolgungsbehörde weiterleitet,
- der *Access-Provider* für im Netz zirkulierende deliktische Inhalte nicht strafrechtlich verantwortlich ist.

11.22 Internationalität der Netzwerkriminalität

Problem

Netzwerkkriminalität beachtet keine Landesgrenzen, sondern ereignet sich weltweit. Oft befindet sich die Täterschaft (der Autor) - von der Schweiz aus gesehen - im Ausland, wo manchmal andere rechtliche Grundlagen bestehen als hier. Gemessen an den traditionellen Anknüpfungspunkten für die schweizerische Strafgerichtsbarkeit liesse sich diese Täterschaft in der Schweiz nicht strafrechtlich belangen.

Lösungsvorschlag der Expertenkommsission

- Wie oben in Ziff. 11.21 erwähnt, soll unter gewissen Voraussetzungen der *Hosting-Provider*, der sich in der Schweiz befindet, strafrechtlich belangt werden können (vgl. Kapitel 9, Ziff. 9.3)
- Dieser Regelungsansatz *entschärft* die geschilderte Problematik der Internationalität dieses Typus Kriminalität. Denn insoweit auf dem inländischen Host auch ausländische Inhalte gespeichert sind, können diese nach schweizerischem Strafrecht beurteilt werden.
- Daneben empfiehlt die Expertenkommission, rasch mit der *Anpassung des schweizerischen Rechts* an die Vorgaben der - von den Schweiz unterzeichneten - *Cybercrime-Konvention* zu beginnen (vgl. Kapitel 10, Ziff. 10.2).

11.23 Wem obliegt die Strafverfolgung?

Problem

Um deliktische Internet-Inhalte rasch erkennen und entsprechende Gegenmassnahmen treffen zu können, bedarf es eines zweckmässigen Instrumentariums auf der Ebene von Polizei und Strafjustiz. Wegen des betont internationalen Charakters der Netzwerkkriminalität und der kaum übersehbaren Menge von Inhalten fehlt es manchem der Kantone, denen ja heute die Verfolgung und Beurteilung solcher Straftaten obliegt, an den dafür nötigen Ressourcen und Kapazitäten.

Lösungsvorschlag der Expertenkommission

- Bereits seit 1. Januar 2003 besteht im Bundesamt für Polizei eine Stelle, die ein Internet-Monitoring durchführt und eingehende Meldungen von Privaten koordiniert (Koordinationsstelle für die Bekämpfung der Internet-Kriminalität,

KOBIK). Der Bund muss diese Aufgabe, in Zusammenarbeit mit den Kantonen, weiterhin erfüllen.

- Darüber hinaus sollte der Bund in bestimmten Fällen die Möglichkeit erhalten, in Anlehnung an die Regelung der sog. Effizienzvorlage [280] selber entsprechende Strafverfahren zu führen (neuer Art. 340ter StGB; vgl. Kapitel 9, v.a. Ziff. 9.4).

11.3 Weitere behandelte Aspekte

Auch wenn die Expertenkommission den strafrechtlichen Komplex prioritär behandelte, hat sie doch andere Aspekte des Themas „Netzwerkkriminalität“ nicht übersehen, die neben dem Strafrecht bestehen oder sich daraus ergeben:

11.31 Technische Kontrollen des Internet (vgl. Kapitel 3)

Kontrollen des Zugangs zum Internet und von dessen Inhalt sind mit technischen Mitteln zum Teil möglich. Weil aber das Internet von seiner Grundidee her dezentral organisiert ist und eine hohe Verfügbarkeit gewährleisten soll, erfordern solche Kontrollen einen sehr grossen Aufwand. Aus dem gleichen Grund lassen sich Kontroll- bzw. Sperrmassnahmen vergleichsweise einfach umgehen.

11.32 Verwaltungsrechtliche Massnahmen (vgl. Kapitel 7)

Verwaltungsrechtliche Massnahmen wären denkbar, um, ergänzend zum Strafrecht, Rechtsgutverletzungen in elektronischen Kommunikationsnetzen vorzubeugen. Das geltende Recht bietet keine entsprechenden Grundlagen. Vorstellbare neue Instrumente kollidieren aber meist mit praktischen oder verfassungsrechtlichen Schranken, besonders jenen, die sich aus den Grundrechten freier Kommunikation und aus dem Verfassungsgrundsatz der Verhältnismässigkeit behördlicher Eingriffe ergeben (vgl. dazu auch Kapitel 5). Deshalb verzichtet die Kommission in ihren Vorschlägen auf verwaltungsrechtlichen Flankenschutz zum Strafrecht.

11.33 Zivilrecht (vgl. Kapitel 8*)*

Das Strafrecht und der Haftungsaspekt des Zivilrechts weisen im Zusammenhang mit der Netzwerkkriminalität verschiedene Berührungspunkte auf. Zwischen diesen beiden Rechtsbereichen bestehen aber ebenso Unterschiede. Diese ergeben sich vor allem aus den unterschiedlichen Verschuldensbegriffen (v.a. wegen der im Zivilrecht bestehenden verschuldensunabhängigen Unterlassungs- und Beseitigungsansprüche sowie im Zusammenhang mit spezifisch zivilprozessualen Aspekten).

Die Kommission hält es für erwünscht, dass bestimmte Fragen, die sich hier stellen, gesetzgeberisch geklärt werden. Sie ist jedoch der Auffassung, dass der sachgerechte und geeignete Rahmen dafür in laufenden Gesetzgebungs- und Revisionsvorhaben (z.B. Gesetzgebung über den elektronischen Geschäftsverkehr oder Revision und Vereinheitlichung des Haftpflichtrechts) zu suchen ist.

---

[280] Massnahmen zur Verbesserung der Effizienz und der Rechtsstaatlichkeit in der Strafverfolgung (Botschaft BBl 1998, 1529 ff. Änderung des Strafgesetzbuches vom 22.12.1999, in Kraft seit 1. Januar 2002, AS 2001, 3071).

Anhang

A - In der Motion Pfisterer (Begründung) vorgeschlagene StGB-Änderungen

6. Strafbare Handlungen in Telekommunikationsnetzen und Medien

Art. 27 Strafbare Handlungen in Medien

[1] Wird eine strafbare Handlung durch Veröffentlichung in einem Medium begangen und erschöpft sie sich in dieser Veröffentlichung, so ist, unter Vorbehalt von Artikel 27ter StGB und der nachfolgenden Bestimmungen, der Autor allein strafbar.

Abs. 2-4 Unverändert.

Art. 27bis Quellenschutz
Unverändert

Art. 27ter Strafbare Handlungen in Telekommunikationsnetzen

[1] Wird eine strafbare Handlung durch Übermittlung, Bereitstellen oder Bereithalten von Informationen, namentlich Inhalten, in einem Telekommunikationsnetz begangen, so ist - unter Vorbehalt der nachfolgenden Bestimmungen - der Anbieter dieser Informationen allein strafbar.
Nimmt der Anbieter eine redaktionelle Informationskontrolle im Sinne von Artikel 27 Absatz 2 wahr, so wird er strafbar nach Massgabe der Artikel 27 und 322bis.

[2] Wird mit fremden Informationen, namentlich Inhalten, eine strafbare Handlung begangen, ist derjenige, der diese Informationen zur Nutzung in einem Telekommunikationsnetz bereit hält, nur strafbar, wenn er es wider besseres Wissen unterlässt, die Nutzung dieser Informationen zu verhindern, obwohl es ihm technisch möglich und zumutbar ist.

[3] Wer lediglich den Zugang zu fremden Informationen, namentlich zu fremden Inhalten, in einem Telekommunikationsnetz vermittelt, ist nicht strafbar, sofern er:
a. die Informationsübermittlung nicht veranlasst;
b. den Adressaten der übermittelten Informationen nicht ausgewählt;
c. die übermittelten Informationen nicht ausgewählt oder verändert hat.
Eine automatische und kurzzeitige Speicherung fremder Informationen infolge automatisierter Übermittlung gilt als Zugangsvermittlung.

Art. 27^{quater} Vorbehalt anderer Gesetze

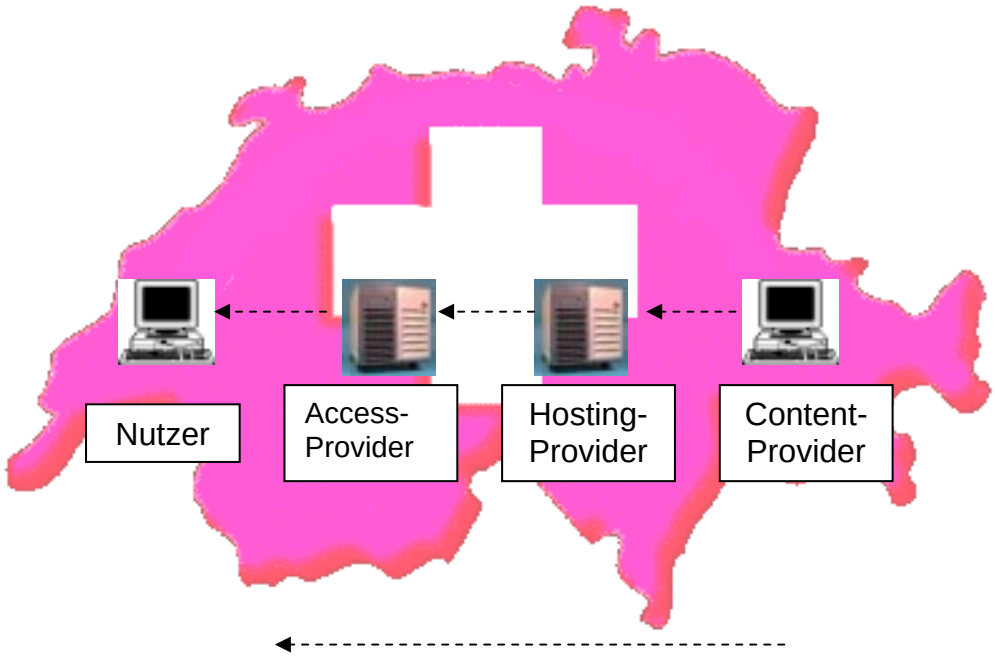
Artikel 27ter regelt die strafrechtliche Verantwortlichkeit in Telekommunikationsnetzen abschliessend. Verpflichtungen zur Entfernung oder Sperrung der Nutzung von Informationen nach den allgemeinen Erlassen des Bundes und der Kantone bleiben unberührt, wenn die in Artikel 27ter genannten Personen von diesen Informationen rechtmässig Kenntnis erlangen und eine Sperrung technisch möglich und zumutbar ist.

Art. 340ter

Der Bundesgerichtsbarkeit unterstehen weiter strafbare Handlungen in Telekommunikationsnetzen (Art. 27ter und 27^{quater}).

B - Fallbeispiele zu Kapitel 6, Ziff. 6.4

1. Konstellation: Alle Akteure handeln in der Schweiz



Fall 1: Kinderpornographische Bilddatei im WWW

• ***Anwendbarkeit des Medienstrafrechts***: nein (Bundesgericht), mehrheitlich abweichend allerdings die Lehre (vgl. oben Ziff. 6.2).
• ***Content-Provider***: Ort der Tatausführung in der Schweiz, daher Strafhoheit nach Territorialprinzip gegeben (vgl. oben Ziff. 6.41); Haupttäterschaft durch Zugänglichmachen nach Art. 197 Ziff. 3 StGB.
• ***Hosting-Provider***: (Neben-)Täterschaft durch Zugänglichmachen nach Art. 197 Ziff. 3 StGB oder Gehilfenschaft durch Förderungsbeitrag zur Haupttat (beides unklar, vgl. oben Ziff. 6.3). Bei beiden Varianten: Strafhoheit nach Territorialprinzip gegeben (vgl. oben Ziff. 6.41).
• ***Access-Provider***: (Neben-)Täterschaft durch Zugänglichmachen nach Art. 197 Ziff. 3 StGB oder Gehilfenschaft durch Förderungsbeitrag zur Haupttat (beides abzulehnen, aber unklar, vgl. oben Ziff. 6.3). Bei beiden Varianten: Strafhoheit nach Territorialprinzip gegeben (vgl. oben Ziff. 6.41).
• ***Nutzer***: Haupttäterschaft, falls die Bilddatei auf der eigenen Festplatte abgespeichert wird (Besitz von Kinderpornographie, Art. 197 Ziff. 3bis StGB).Ort der Tatausführung in der Schweiz, daher Strafhoheit nach Territorialprinzip gegeben (vgl. oben Ziff. 6.41).

Fall 2: Aufforderung zu einem Brandanschlag in Newsgroup

• ***Anwendbarkeit des Medienstrafrechts***: ja (vgl. oben Ziff. 6.1).
• ***Content-Provider***: Haupttäterschaft durch öffentliche Aufforderung nach Art. 259 Abs. 1 StGB. Ort der Tatausführung in der Schweiz, daher Strafhoheit nach Territorialprinzip gegeben (vgl. oben Ziff. 6.41);
• ***Hosting-Provider***: Anwendbarkeit des Medienstrafrechts abhängig davon, ob der Hosting-Provider als Verbreiter unter den Regelungsbereich des Art. 27 StGB fällt; falls ja, entfällt die Strafbarkeit, weil gegen den Autor vorgegangen werden kann; falls nein, kommt Gehilfenschaft durch Förderungsbeitrag zur Haupttat in Frage (unklar, vgl. oben Ziff. 6.3). Infolge Akzessorietät der Gehilfenschaft, Beurteilung nach dem Recht des Ortes der Tatausführung der Haupttat (Schweiz), daher Strafhoheit nach Territorialprinzip gegeben (vgl. oben Ziff. 6.41).
• ***Access-Provider***: Anwendbarkeit des Medienstrafrechts abhängig davon, ob der Access-Provider als Verbreiter unter den Regelungsbereich des Art. 27 StGB fällt; falls ja, entfällt die Strafbarkeit, weil gegen den Autor vorgegangen werden kann; falls nein, kommt Gehilfenschaft durch Förderungsbeitrag zur Haupttat in Frage (abzulehnen vgl. oben Ziff. 6.3). Infolge Akzessorietät der Gehilfenschaft, Beurteilung nach dem Recht des Ort der Tatausführung der Haupttat (Schweiz), daher Strafhoheit nach Territorialprinzip gegeben (vgl. oben Ziff. 6.41).
• ***Nutzer***: straflos.

Fall 3: Rassendiskriminierende Texte im WWW

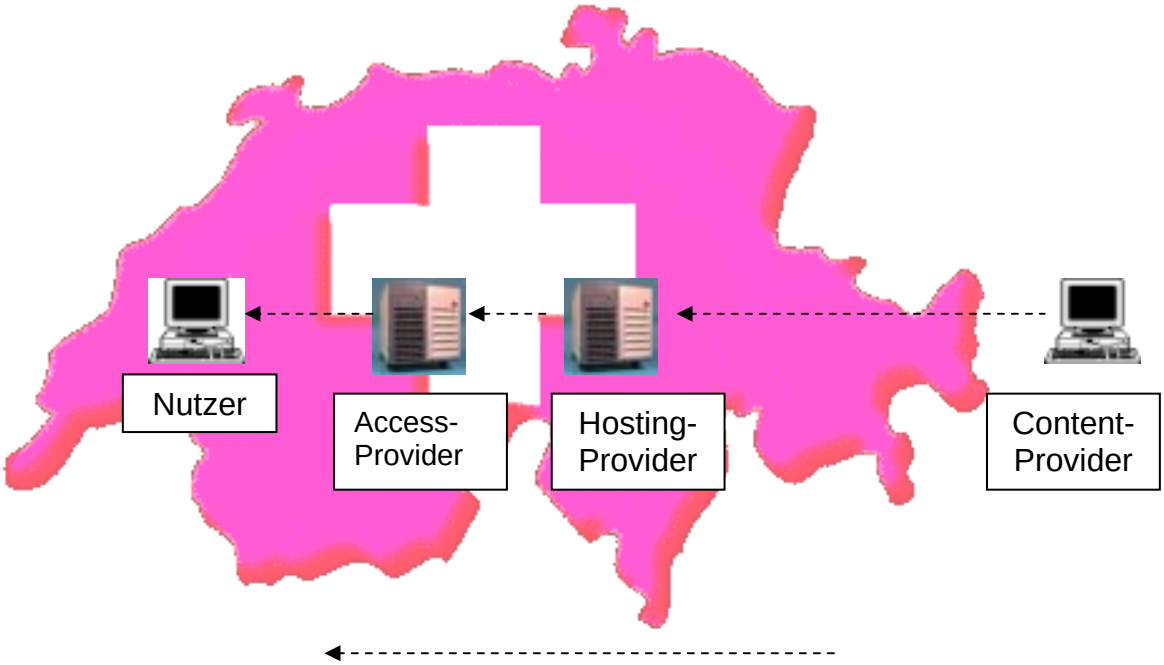
• ***Anwendbarkeit des Medienstrafrechts***: unklar (eher abzulehnen) [281].
• ***Content-Provider***: Haupttäterschaft durch öffentliche Verbreitung nach Art. 261bis Abs. 2 StGB fraglich [282]. Ort der Tatausführung in der Schweiz, daher Strafhoheit nach Territorialprinzip gegeben (vgl. oben Ziff. 6.41).
• ***Hosting-Provider***: Soweit eine eigenständige Tatvariante von Art. 261bis Abs. 3 StGB durch Förderung der Haupttat angenommen wird, Beurteilung nach schweizerischem Strafrecht (unklar, vgl. oben Ziff. 6.3). Soweit Gehilfenschaft angenommen wird, Akzessorietät zur Haupttat, d.h. Beurteilung nach dem Recht des Ortes, an welchem die Haupttat ausgeführt wurde (Schweiz).
• ***Access-Provider***: Soweit eine eigenständige Tatvariante von Art. 261bis Abs. 3 StGB durch Förderung der Haupttat angenommen wird, Beurteilung nach schweizerischem Strafrecht (unklar, vgl. oben Ziff. 6.3). Soweit Gehilfenschaft angenommen wird, Akzessorietät zur Haupttat, d.h. Beurteilung nach dem Recht des Ortes, an welchem die Haupttat ausgeführt wurde (Schweiz).
• *Nutzer*: straflos.

---

[281] Zu den widersprüchlichen Meinungen hierzu zusammenfassend RIKLIN/STRATENWERTH (Bibl.), S. 15 m.N. Das Bundesgericht äusserte sich in BGE 125 IV 206 ff. nicht zur Klassifizierung von Art. 261bis Abs. 2 StGB.

[282] Ob die Tathandlung des Verbreitens nur erfüllt, wer Informationen aktiv an einen grösseren Personenkreis überträgt, oder ob schon das Bereitsstellen auf einem Web-Server diesem objektiven Tatbestandsmerkmal genügt, ist in der Schweiz noch ungeklärt (vgl. PETER VON INS/PETER-RENÉ WYDER, in: Niggli/Wiprächtiger, StGB Kommentar, Basel 2003, Art. 179 N 41 „Mitteilung, also Weitergabe an Dritte“). Nach einer umstrittenen Entscheidung des deutschen BGH handelt es sich beim Verbreiten um eine Untergruppe des Zugänglichmachens, nämlich als Zugänglichmachen einer Information, die mindestens einmal konkret von einem Nutzer „abgeholt“ wurde, s. Urteil des BGH vom 27.6.2001 – 1 StR 66/01 Erw. III.3.b)bb).

2. Konstellation: Content-Provider handelt im Ausland, alle anderen Akteure in der Schweiz



Fall 1: Kinderpornographische Bilddatei im WWW

• ***Anwendbarkeit des Medienstrafrechts***: nein (Bundesgericht), mehrheitlich abweichend allerdings die Lehre (vgl. oben Ziff. 6.2).
• ***Content-Provider***: Ort der Tatausführung im Ausland; bei abstrakten Gefährdungsdelikten keine Anknüpfung an einen Erfolg in der Schweiz möglich, daher keine Strafhoheit nach Territorialprinzip gegeben (vgl. oben Ziff. 6.42), auch keine Strafhoheit nach dem Weltrechtsprinzip (Art. 6bis StGB)[283], somit in der Schweiz nicht verfolgbar, auf Ersuchen Rechtshilfe für einen anderen Staat möglich[284].
• ***Hosting-Provider***: Sofern (Neben-)Täterschaft durch Zugänglichmachen nach Art. 197 Ziff. 3 StGB angenommen wird, rechtliche Beurteilung nach schweizerischem Strafrecht. Sofern Gehilfenschaft durch Förderungsbeitrag zur Haupttat angenommen wird, Akzessorietät zur Haupttat, d.h. in der Schweiz nicht verfolgbar, Beurteilung nach dem Recht des Ortes, an welchem die Haupttat begangen wurde (beides unklar, vgl. oben Ziff. 6.3).
• ***Access-Provider***: Sofern (Neben-)Täterschaft durch Zugänglichmachen nach Art. 197 Ziff. 3 StGB angenommen wird, rechtliche Beurteilung nach schweizerischem Strafrecht. Sofern Gehilfenschaft durch Förderungsbeitrag zur Haupttat besteht, Akzessorietät zur Haupttat, d.h. in der Schweiz nicht verfolgbar, Beurteilung nach dem Recht des Ortes, an welchem die Haupttat begangen wurde (beides abzulehnen, aber unklar, vgl. oben Ziff. 6.3).

---

[283] Anders nach Art. 5 des revidierten Allgemeinen Teils StGB.
[284] Möglich bleibt noch eine Anknüpfung an das aktive Personalitätsprinzip, Art. 6 Ziff. 1 StGB, falls der Content-Provider Schweizer Staatsangehöriger ist und sich (nach Ausführung der Tat im Ausland) in der Schweiz aufhält.

• ***Nutzer***: Haupttäterschaft, falls die Bilddatei auf der eigenen Festplatte abgespeichert wird (Besitz von Kinderpornographie, Art. 197 Ziff. 3bis StGB). Ort der Tatausführung in der Schweiz, daher Strafhoheit nach Territorialprinzip gegeben (vgl. oben Ziff. 6.41).

Fall 2: Aufforderung zu einem Brandanschlag in Newsgroup

• ***Anwendbarkeit des Medienstrafrechts***: ja (vgl. oben Ziff. 6.1).
• ***Content-Provider***: Ort der Tatausführung im Ausland; bei abstrakten Gefährdungsdelikten keine Anknüpfung an einen Erfolg in der Schweiz möglich, daher keine Strafhoheit nach Territorialprinzip gegeben (vgl. oben Ziff. 6.42), somit in der Schweiz nicht verfolgbar.
• ***Hosting-Provider***: Ort der Tatausführung in der Schweiz (Art. 3 i.V.m. Art. 7 StGB), daher Strafhoheit nach Territorialprinzip gegeben (vgl. oben Ziff. 6.41); nach einer Meinung Strafbarkeit nach Massgabe von Art. 27 Abs. 2 i.V.m. Art. 322bis StGB, da gegen den Autor nicht vorgegangen werden kann und der Hosting-Provider als eine für die Veröffentlichung verantwortliche Person angesehen wird; nach einer anderen Meinung ist das Medienstrafrecht nicht anwendbar. Die allenfalls in Betracht kommende Gehilfenschaft kann in der Schweiz nicht verfolgt werden, auf Ersuchen ist Rechtshilfe für einen anderen Staat möglich. Nach einer dritten Auffassung entfällt die Strafbarkeit gemäss Art. 27 StGB wegen Privilegierung der Verbreiter (unklar, vgl. oben Ziff. 6.43).
• ***Access-Provider***: Ort der Tatausführung in der Schweiz (Art. 3 i.V.m. Art. 7 StGB), daher Strafhoheit nach Territorialprinzip gegeben (vgl. oben Ziff. 6.41); nach einer Meinung Straflosigkeit nach Massgabe von Art. 27 Abs. 2 StGB, da gegen den Hosting-Provider vorgegangen werden kann; nach einer anderen Meinung ist das Medienstrafrecht nicht anwendbar. Die allenfalls in Betracht kommende Gehilfenschaft kann in der Schweiz nicht verfolgt werden, auf Ersuchen ist Rechtshilfe für einen anderen Staat möglich. Nach einer dritten Auffassung entfällt die Strafbarkeit gemäss Art. 27 StGB wegen Privilegierung der Verbreiter (unklar, vgl. oben Ziff. 6.43).
• ***Nutzer***: straflos.

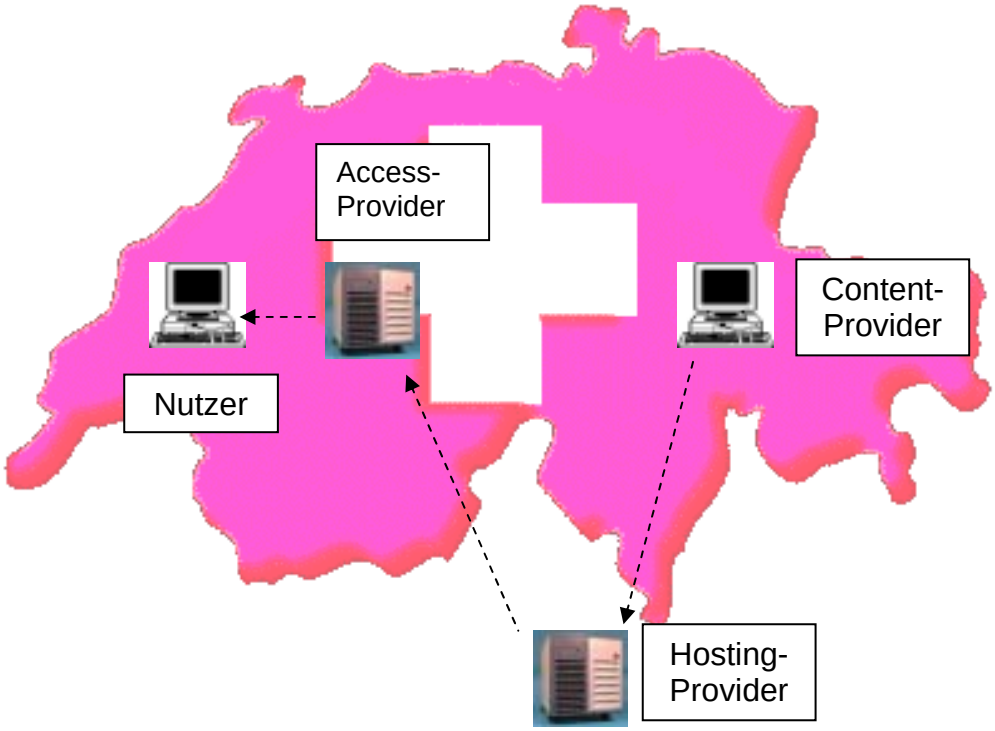
Fall 3: Rassendiskriminierende Texte im WWW

• ***Anwendbarkeit des Medienstrafrechts***: unklar (eher abzulehnen).
• ***Content-Provider***: Ort der Tatausführung im Ausland; bei schlichten Tätigkeitsdelikten keine Anknüpfung an einen Erfolg in der Schweiz möglich, daher keine Strafhoheit nach Territorialprinzip gegeben (vgl. oben Ziff. 6.42), somit in der Schweiz nicht verfolgbar, auf Ersuchen Rechtshilfe für einen anderen Staat möglich[285].
• ***Hosting-Provider***: Soweit eine eigenständige Tatvariante von Art. 261bis Abs. 3 StGB durch Förderung der Haupttat angenommen wird, Beurteilung nach schweizerischem Strafrecht (unklar, vgl. oben Ziff. 6.3). Soweit Gehilfenschaft

[285] A.M. SCHWARZENEGGER, ABSTRAKTE GEFAHR (Bibl.), S 252. Vgl. zur deutschen Lehre, nach welcher Äusserungsdelikte allesamt als Erfolgsdelikte gelten, weshalb eine Anknüpfung an den Erfolg i.S.v. § 9 Abs. 1 3. Alt. des deutschen StGB möglich ist, THOMAS FUHR: Die Äusserung im Strafgesetzbuch, Berlin 2001, 175 ff. und 188 ff. m.N.; THEODOR LENCKNER – in: Schönke/Schröder, Strafgesetzbuch, Kommentar, 26. Aufl., München 2001, § 185 N 12 und § 186 N 8 a.E. am Beispiel der Beleidigung und üblen Nachrede.

angenommen wird, Akzessorietät zur Haupttat, d.h. Beurteilung nach dem Recht des Ortes, an welchem die Haupttat ausgeführt wurde, keine Strafhoheit der Schweiz.
• ***Access-Provider***: Soweit eine eigenständige Tatvariante von Art. 261bis Abs. 3 StGB durch Förderung der Haupttat angenommen wird, Beurteilung nach schweizerischem Strafrecht. Soweit Gehilfenschaft angenommen wird, Akzessorietät zur Haupttat, d.h. Beurteilung nach dem Recht des Ortes, an welchem die Haupttat ausgeführt wurde, keine Strafhoheit der Schweiz (beides abzulehnen, unklar, vgl. oben Ziff. 6.3).
• ***Nutzer***: straflos.

3. Konstellation: Hosting-Provider handelt im Ausland, alle anderen Akteure in der Schweiz



Fall 1: Kinderpornographische Bilddatei im WWW

• ***Anwendbarkeit des Medienstrafrechts***: nein (Bundesgericht), mehrheitlich abweichend allerdings die Lehre (vgl. oben Ziff. 6.2).
• ***Content-Provider***: Ort der Tatausführung in der Schweiz, daher Strafhoheit nach Territorialprinzip gegeben (vgl. oben Ziff. 6.41); Haupttäterschaft durch Zugänglichmachen nach Art. 197 Ziff. 3 StGB.
• ***Hosting-Provider***: Sofern (Neben-)Täterschaft durch Zugänglichmachen nach Art. 197 Ziff. 3 StGB angenommen wird, rechtliche Beurteilung nach dem Recht des

Ortes, an welchem diese Tat begangen wurde, d.h. Ausland, keine Strafhoheit der Schweiz. Sofern Gehilfenschaft durch Förderungsbeitrag zur Haupttat besteht, Akzessorietät zur Haupttat, d.h. Beurteilung nach schweizerischem Strafrecht (beides unklar, vgl. oben Ziff. 6.3) [286].
• ***Access-Provider***: Sofern (Neben-)Täterschaft durch Zugänglichmachen nach Art. 197 Ziff. 3 StGB angenommen wird, rechtliche Beurteilung nach schweizerischem Strafrecht. Sofern Gehilfenschaft durch Förderungsbeitrag zur Haupttat besteht, Akzessorietät zur Haupttat, d.h. Beurteilung ebenfalls nach schweizerischem Recht (beides abzulehnen, aber unklar, vgl. oben Ziff. 6.3).
• ***Nutzer***: Haupttäterschaft, falls die Bilddatei auf der eigenen Festplatte abgespeichert wird (Besitz von Kinderpornographie, Art. 197 Ziff. 3bis StGB). Ort der Tatausführung in der Schweiz, daher Strafhoheit nach Territorialprinzip gegeben (vgl. oben Ziff. 6.41).

Fall 2: Aufforderung zu einem Brandanschlag in Newsgroup

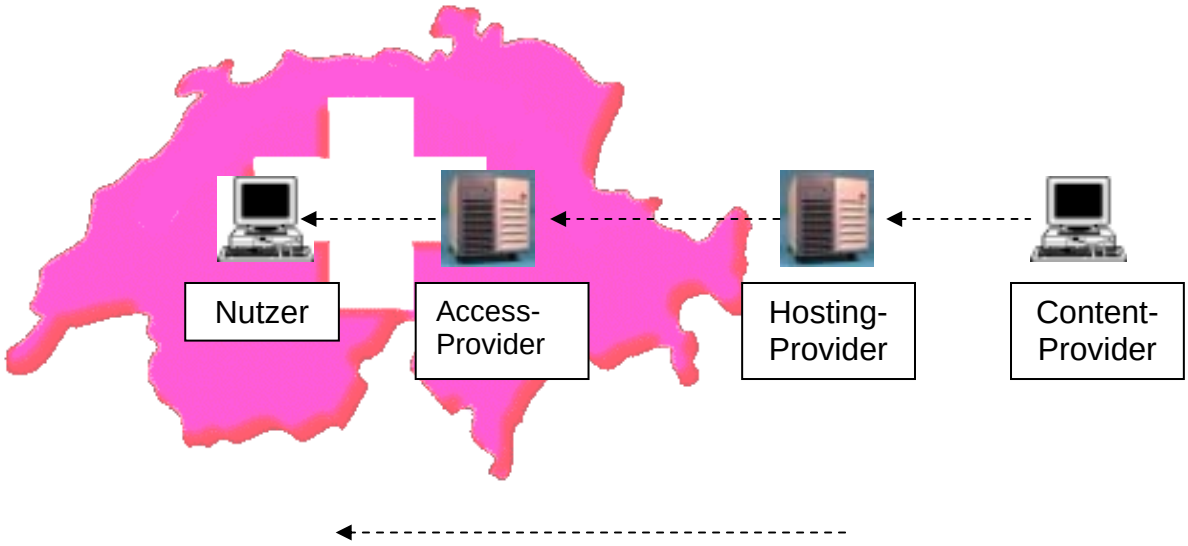
• ***Anwendbarkeit des Medienstrafrechts***: ja (vgl. oben Ziff. 6.1).
• ***Content-Provider***: Ort der Tatausführung in der Schweiz, daher Strafhoheit nach Territorialprinzip gegeben (vgl. oben Ziff. 6.41); Haupttäterschaft durch öffentliche Aufforderung nach Art. 259 Abs. 1 StGB.
• ***Hosting-Provider***: Sofern Gehilfenschaft durch Förderungsbeitrag zur Haupttat besteht, Akzessorietät zur Haupttat, d.h. Beurteilung nach schweizerischem Recht. Nach einer anderen Auffassung entfällt die Strafbarkeit gestützt auf Art. 27 (Verbreiter).
• ***Access-Provider***: Nach einer Meinung Strafbefreiung gemäss Art. 27 Abs. 1 StGB, da gegen den Autor vorgegangen werden kann; nach einer anderen Meinung ist das Medienstrafrecht nicht anwendbar, aber auch keine Gehilfenschaft anzunehmen (vgl. oben Ziff. 6.3).
• ***Nutzer***: straflos.

Fall 3: Rassendiskriminierende Texte im WWW

• ***Anwendbarkeit des Medienstrafrechts***: unklar (eher abzulehnen).
• ***Content-Provider***: Haupttäterschaft durch öffentliche Verbreitung nach Art. 261bis Abs. 2 StGB. Ort der Tatausführung in der Schweiz, daher Strafhoheit nach Territorialprinzip gegeben (vgl. oben Ziff. 6.41);
• ***Hosting-Provider***: Soweit eine eigenständige Tatvariante von Art. 261bis Abs. 3 StGB durch Förderung der Haupttat angenommen wird, Beurteilung nach Ort der Begehung, keine Strafhoheit der Schweiz. Soweit Gehilfenschaft angenommen wird, Akzessorietät zur Haupttat, d.h. Beurteilung nach schweizerischem Recht.
• ***Access-Provider***: Soweit eine eigenständige Tatvariante von Art. 261bis Abs. 3 StGB durch Förderung der Haupttat angenommen wird, Beurteilung nach schweizerischem Strafrecht. Soweit Gehilfenschaft angenommen wird, Akzessorietät zur Haupttat, d.h. Beurteilung ebenfalls nach schweizerischem Recht (beides abzulehnen).
• ***Nutzer***: straflos.

[286] Möglich bleibt auch eine Anknüpfung an das aktive Personalitätsprinzip, Art. 6 Ziff. 1 StGB, falls der für den Web-Server Verantwortliche Schweizer Staatsangehöriger ist und sich in der Schweiz aufhält.

4. Konstellation: Content- und Hosting-Provider handeln im Ausland, Access-Provider und Nutzer handeln in der Schweiz



Fall 1: Kinderpornographische Bilddatei im WWW

• ***Anwendbarkeit des Medienstrafrechts***: nein (Bundesgericht), mehrheitlich abweichend allerdings die Lehre (vgl. oben Ziff. 6.2).
• ***Content-Provider***: Ort der Tatausführung im Ausland; bei abstrakten Gefährdungsdelikten keine Anknüpfung an einen Erfolg in der Schweiz möglich, daher keine Strafhoheit nach Territorialprinzip gegeben (vgl. oben Ziff. 6.42), auch keine Strafhoheit nach dem Weltrechtsprinzip (Art. 6bis StGB) [287], somit in der Schweiz nicht verfolgbar, auf Ersuchen Rechtshilfe für einen anderen Staat möglich [288].
• ***Hosting-Provider***: Ort der Tatausführung im Ausland; bei abstrakten Gefährdungsdelikten keine Anknüpfung an einem Erfolg in der Schweiz möglich, daher keine Strafhoheit nach Territorialprinzip gegeben (vgl. oben Ziff. 6.42), somit in der Schweiz nur Rechtshilfe möglich.
• ***Access-Provider***: Soweit Nebentäterschaft durch Zugänglichmachen nach Art. 197 Ziff. 3 StGB angenommen wird (abzulehnen, aber unklar, vgl. oben Ziff. 6.3), Anwendbarkeit des schweizerischen StGB. Soweit Gehilfenschaft durch Förderung der Haupttat angenommen wird, Akzessorietät zur Haupttat, Beurteilung nach dem Recht des Ortes, an welchem die Haupttat ausgeführt wurde, keine Strafhoheit der Schweiz. Nur Rechtshilfe möglich.
• ***Nutzer***: Haupttäterschaft, falls die Bilddatei auf der eigenen Festplatte abgespeichert wird (Besitz von Kinderpornographie, Art. 197 Ziff. 3bis StGB). Ort der Tatausführung in der Schweiz, daher Strafhoheit nach Territorialprinzip gegeben (vgl. oben Ziff. 6.41).

---

[287] Möglich bleibt noch eine Anknüpfung an das aktive Personalitätsprinzip, Art. 6 Ziff. 1 StGB, falls der für den Web-Server Verantwortliche Schweizer Staatsangehöriger ist und sich in der Schweiz aufhält.
[288] Anders nach Art. 5 des revidierten Allgemeinen Teils StGB.

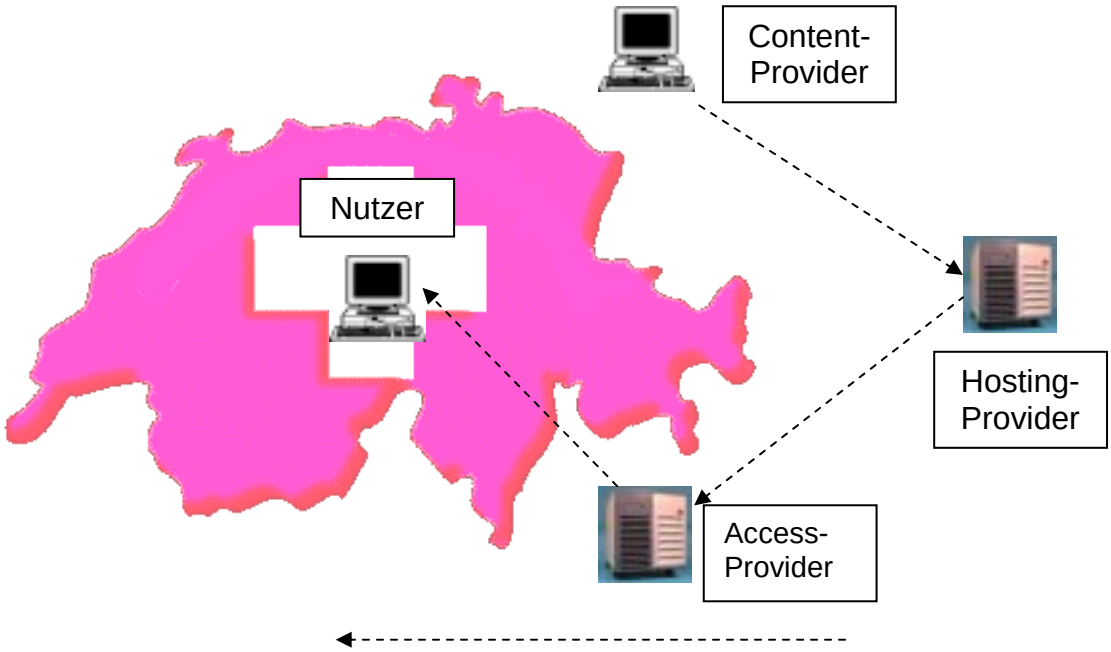
Fall 2: Aufforderung zu einem Brandanschlag in Newsgroup

• ***Anwendbarkeit des Medienstrafrechts***: ja (vgl. oben Ziff. 6.1).
• ***Content-Provider***: Ort der Tatausführung im Ausland; daher keine Strafhoheit nach Territorialprinzip gegeben (vgl. oben Ziff. 6.42), somit in der Schweiz nicht verfolgbar, auf Ersuchen Rechtshilfe für einen anderen Staat möglich.
• ***Hosting-Provider***: Ort der Tatausführung im Ausland; bei abstrakten Gefährdungsdelikten keine Anknüpfung an einem Erfolg in der Schweiz möglich, daher keine Strafhoheit nach Territorialprinzip gegeben (vgl. oben Ziff. 6.42), somit in der Schweiz nur Rechtshilfe möglich.
• ***Access-Provider***: Ort der Tatausführung in der Schweiz, daher Strafhoheit nach Territorialprinzip gegeben (vgl. oben Ziff. 6.41); nach einer Meinung Strafbarkeit nach Massgabe von Art. 27 Abs. 2 i.V.m. Art. 322bis StGB, da gegen den Autor und den Hosting-Provider nicht vorgegangen werden kann und der Access-Provider als eine für die Veröffentlichung verantwortliche Person angesehen wird; nach einer anderen Meinung ist das Medienstrafrecht nicht anwendbar, auch die allenfalls in Betracht kommende Gehilfenschaft könnte nicht verfolgt werden, auf Ersuchen Rechtshilfe für einen anderen Staat möglich. Nach einer anderen Auffassung ist der Access-Provider gemäss Art. 27 StGB (Verbreiter) generell von der Strafbarkeit ausgenommen (unklar, vgl. oben Ziff. 6.43).
• ***Nutzer***: straflos.

Fall 3: Rassendiskriminierende Texte im WWW

• ***Anwendbarkeit des Medienstrafrechts***: unklar (eher abzulehnen).
• ***Content-Provider***: Ort der Tatausführung im Ausland; bei schlichten Tätigkeitsdelikten keine Anknüpfung an einen Erfolg in der Schweiz möglich, daher keine Strafhoheit nach Territorialprinzip gegeben (vgl. oben Ziff. 6.42), somit in der Schweiz nicht verfolgbar, auf Ersuchen Rechtshilfe für einen anderen Staat möglich.
• ***Hosting-Provider***: Ort der Tatausführung im Ausland; bei schlichten Tätigkeitsdelikten keine Anknüpfung an einem Erfolg in der Schweiz möglich, daher keine Strafhoheit nach Territorialprinzip gegeben (vgl. oben Ziff. 6.42), somit in der Schweiz nicht verfolgbar, auf Ersuchen Rechtshilfe für einen anderen Staat möglich.
• ***Access-Provider***: Sofern eigenständige Tatvariante von Art. 261bis Abs. 3 StGB durch Förderung der Haupttat angenommen wird (unklar, vgl. oben Ziff. 6.3), Ort der Tatausführung in der Schweiz, daher Strafhoheit nach Territorialprinzip gegeben (vgl. oben Ziff. 6.41). Sofern Gehilfenschaft angenommen, Akzessorietät zur Haupttat, d.h. Beurteilung nach dem Recht des Ortes, an welchem die Haupttat ausgeführt wurde, keine Strafhoheit der Schweiz. Rechtshilfe möglich
• ***Nutzer***: straflos.

5. Konstellation: Nur der Nutzer handelt in der Schweiz, alle anderen Akteure handeln im Ausland



Fall 1: Kinderpornographische Bilddatei im WWW

• ***Anwendbarkeit des Medienstrafrechts***: nein (Bundesgericht), mehrheitlich abweichend allerdings die Lehre (vgl. oben Ziff. 6.2).
• ***Content-Provider***: Ort der Tatausführung im Ausland; bei abstrakten Gefährdungsdelikten keine Anknüpfung an einen Erfolg in der Schweiz möglich, daher keine Strafhoheit nach Territorialprinzip gegeben (vgl. oben Ziff. 6.42), auch keine Strafhoheit nach dem Weltrechtsprinzip (Art. 6bis StGB) [289], somit in der Schweiz nicht verfolgbar, auf Ersuchen Rechtshilfe für einen anderen Staat möglich.[290].
• ***Hosting-Provider***: gleich wie beim Content-Provider.
• ***Access-Provider***: gleich wie beim Content-Provider.
• ***Nutzer***: Haupttäterschaft, falls die Bilddatei auf der eigenen Festplatte abgespeichert wird (Besitz von Kinderpornographie, Art. 197 Ziff. 3bis StGB). Ort der Tatausführung in der Schweiz, daher Strafhoheit nach Territorialprinzip gegeben (vgl. oben Ziff. 6.41).

Fall 2: Aufforderung zu einem Brandanschlag in Newsgroup

• ***Anwendbarkeit des Medienstrafrechts***: ja (vgl. oben Ziff. 6.1).
• ***Content-Provider***: Ort der Tatausführung im Ausland; bei abstrakten Gefährdungsdelikten keine Anknüpfung an einen Erfolg in der Schweiz möglich, daher keine Strafhoheit nach Territorialprinzip gegeben (vgl. oben Ziff. 6.42), somit in

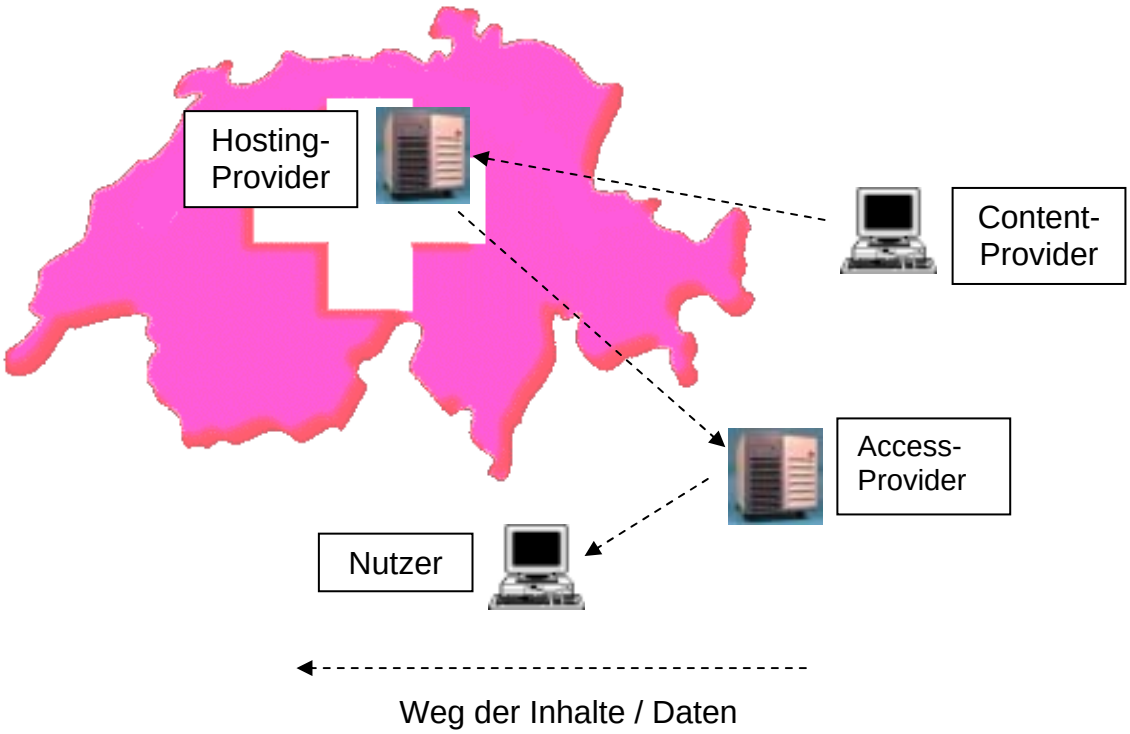
[289] Möglich bleibt noch eine Anknüpfung an das aktive Personalitätsprinzip, Art. 6 Ziff. 1 StGB, falls der für den Web-Server Verantwortliche Schweizer Staatsangehöriger ist und sich in der Schweiz aufhält.
[290] Anders nach Art. 5 des revidierten Allgemeinen Teils StGB.

der Schweiz nicht verfolgbar, auf Ersuchen Rechtshilfe für einen anderen Staat möglich.
• ***Hosting-Provider***: gleich wie beim Content-Provider.
• ***Access-Provider***: wie beim Content-Provider.
• ***Nutzer***: straflos.

Fall 3: Rassendiskriminierende Texte im WWW

• ***Anwendbarkeit des Medienstrafrechts***: unklar (eher abzulehnen).
• ***Content-Provider***: Ort der Tatausführung im Ausland; bei schlichten Tätigkeitsdelikten keine Anknüpfung an einen Erfolg in der Schweiz möglich, daher keine Strafhoheit nach Territorialprinzip gegeben (vgl. oben Ziff. 6.42), somit in der Schweiz nicht verfolgbar, auf Ersuchen Rechtshilfe für einen anderen Staat möglich.
• ***Hosting-Provider***: wie beim Content-Provider.
• ***Access-Provider***: wie beim Content-Provider.
• ***Nutzer***: straflos.

6. Konstellation: Nur der Hosting-Provider handelt in der Schweiz, alle anderen Akteure handeln im Ausland



Fall 1: Kinderpornographische Bilddatei im WWW

• ***Anwendbarkeit des Medienstrafrechts***: nein (Bundesgericht), mehrheitlich abweichend allerdings die Lehre (vgl. oben Ziff. 6.2).
• ***Content-Provider***: Ort der Tatausführung im Ausland; bei abstrakten Gefährdungsdelikten keine Anknüpfung an einen Erfolg in der Schweiz möglich, daher keine Strafhoheit nach Territorialprinzip gegeben (vgl. oben Ziff. 6.42), auch keine Strafhoheit nach dem Weltrechtsprinzip (Art. 6^{bis} StGB), somit in der Schweiz nicht verfolgbar, auf Ersuchen Rechtshilfe für einen anderen Staat möglich.

• ***Hosting-Provider***: Sofern (Neben-)Täterschaft durch Zugänglichmachen nach Art. 197 Ziff. 3 StGB angenommen wird, rechtliche Beurteilung nach schweizerischem Strafrecht. Sofern Gehilfenschaft durch Förderungsbeitrag zur Haupttat angenommen wird, Akzessorietät zur Haupttat, d.h. in der Schweiz nicht verfolgbar, Beurteilung nach dem Recht des Ortes, an welchem die Haupttat begangen wurde (beides unklar, vgl. oben Ziff. 6.3).
• ***Access-Provider***: wie beim Content-Provider.
• ***Nutzer***: Ort der Tatausführung im Ausland (Besitz), daher keine Strafhoheit nach Territorialprinzip gegeben; in der Schweiz nicht verfolgbar.

Fall 2: Aufforderung zu einem Brandanschlag in Newsgroup

• ***Anwendbarkeit des Medienstrafrechts***: ja (vgl. oben Ziff. 6.1).
• ***Content-Provider***: Ort der Tatausführung im Ausland; bei abstrakten Gefährdungsdelikten keine Anknüpfung an einen Erfolg in der Schweiz möglich, daher keine Strafhoheit nach Territorialprinzip gegeben (vgl. oben Ziff. 6.42), somit in der Schweiz nicht verfolgbar, auf Ersuchen Rechtshilfe für einen anderen Staat möglich.
• ***Hosting-Provider***: Nach einer Meinung Strafbarkeit nach Massgabe von Art. 27 Abs. 2 i.V.m. Art. 322bis StGB, da gegen den Autor nicht vorgegangen werden kann und der Hosting-Provider als eine für die Veröffentlichung verantwortliche Person angesehen wird; nach einer anderen Meinung ist das Medienstrafrecht nicht anwendbar, auch die allenfalls in Betracht kommende Gehilfenschaft kann in der Schweiz nicht verfolgt werden; nach einer weiteren Auffassung ist der Hosting-Provider als Verbreiter bei Mediendelikten stets strafrei (unklar, vgl. oben Ziff. 6.43).
• ***Access-Provider***: wie beim Content-Provider.
• ***Nutzer***: straflos.

Fall 3: Rassendiskriminierende Texte im WWW

• ***Anwendbarkeit des Medienstrafrechts***: unklar (eher abzulehnen).
• ***Content-Provider***: Ort der Tatausführung im Ausland; bei schlichten Tätigkeitsdelikten keine Anknüpfung an einen Erfolg in der Schweiz möglich, daher keine Strafhoheit nach Territorialprinzip gegeben (vgl. oben Ziff. 6.42), somit in der Schweiz nicht verfolgbar, auf Ersuchen Rechtshilfe für einen anderen Staat möglich.
• ***Hosting-Provider***: Soweit eine eigenständige Tatvariante von Art. 261bis Abs. 3 StGB durch Förderung der Haupttat angenommen wird, Beurteilung nach schweizerischem Strafrecht (unklar, vgl. oben Ziff. 6.3). Soweit Gehilfenschaft angenommen wird, Akzessorietät zur Haupttat, d.h. Beurteilung nach dem Recht des Ortes, an welchem die Haupttat ausgeführt wurde, keine Strafhoheit der Schweiz.
• ***Access-Provider***: wie beim Content-Provider
• ***Nutzer***: straflos.