INTERNET-RECHT
UND
ELECTRONIC COMMERCE LAW

Herausgegeben von
lic. iur. Oliver Arter / Dr. iur. Florian S. Jörg

Dike Verlag AG, 2001, Lachen SZ / St. Gallen

Inhaltsübersicht

E-Commerce – Die strafrechtliche Dimension

Prof. Dr. iur. Christian Schwarzenegger

Inhaltsverzeichnis

"The technology is light years ahead of the legislation and the police know-how."
Ronald K. NOBLE, Secretary-General, Interpol[1]

1. Erscheinungsformen der Internetkriminalität

Die verschiedenen Formen der Internetkriminalität stellen je länger je mehr einen Störfaktor für die weitere Entwicklung des E-Commerce dar. Einige aktuelle Schlagzeilen aus der Schweiz belegen dies eindrücklich:

Betrügerische Bestellungen via E-Mail aus Afrika[2]

Ein Zürcher Geschäft für Unterhaltungselektronik ist auf Betrüger hereingefallen, die via E-Mail Artikel im Wert von 160 000 Fr. bestellten. Die Betrüger benutzten echte Kreditkartennummern, deren rechtmässige Inhaber aber keine Ware bestellt hatten. Bei Internetkäufen mit Kreditkarten, bei denen der Käufer nicht persönlich unterschreibt, haftet das liefernde Geschäft für allfällige Schäden.

Fieses Virus[3]

Ein neuer Typ von Virus namens Sadmind wurde in Deutschland entdeckt. Das Virus verbreitet sich – nicht wie bisherige Viren – ohne menschliches Zutun auf Internetservern. Es verteilt selbständig einen Sabotagecode auf viele weitere Server. Unter Umständen werden dabei alle Daten auf den Servern gelöscht.

WEF war offen für Hacker[4]

Im Februar 2001 wurde der Sonntagszeitung eine CD-ROM zugespielt, die Informationen über 102 000 prominente Persönlichkeiten aus einer Datenbank des WEF enthielt. Als Tabelle ausgedruckt umfasste die Datensammlung über 400 000 A4-Seiten. Die Daten wurden via Internet von einem WEF-Server in Genf heruntergeladen, der durch eine Passwortsperre zugangsgeschützt war. Der Zugriff auf das Datenbankprogramm war jedoch ohne Probleme möglich, weil Nutzername und Passwort in der Grundeinstellung belassen worden waren.

1 CNN (3.11.2000): New Interpol chiefs to tackle cybercrime, abrufbar unter www.cnn.com/2000/WORLD/europe/11/03/interpol.bosses/index.html (Stand: 17.7.2001).

2 Siehe Meldungen in Tages-Anzeiger, Luxuswaren dank Kreditkartentrick, 29. Mai 2001, 14; ZüriExpress, Verhängnisvolle E-Mail-Orders, 29. Mai 2001, 1.

3 Siehe die Meldung in Tages-Anzeiger, Fieses Virus, 14. Mai 2001, 10.

4 Siehe Meldungen in Sonntagszeitung, Intime Details der Teilnehmer gesammelt, 11. Februar 2001, 21; Sonntagszeitung, WEF war offen für Hacker, 4. März 2001, 11; Sonntagszeitung, In vier Schritten ins Herz der Macht, 11. März 2001, 135.

In einer im Oktober 2000 weltweit durchgeführten Umfrage von KPMG nannten 50% der einbezogenen Unternehmen, Hacking und die schwachen Sicherheitsvorkehrungen seien die grössten Sicherheitsrisiken für ihre Online-Präsenz. 9% aller Firmen gaben an, dass es in ihrem E-Commerce-System in den letzten 12 Monaten zu Sicherheitsverletzungen gekommen sei (höchste Werte in: Indien 23%, Deutschland und Grossbritannien je 14%). 53% stellten keine derartigen Probleme fest, während 38% keine Angaben machen wollten bzw. konnten. In 83% der angegebenen Fälle wurden keine rechtlichen Schritte eingeleitet.

Weniger als 35% der Unternehmen lassen externe Sicherheitschecks ihres E-Commerce-Systems durchführen. Rund die Hälfte unter ihnen gab an, ein internes Verfahren zur Registrierung von Sicherheitsverletzungen eingeführt zu haben, worunter allerdings nur 43% (also 22% der gesamten Stichprobe) Richtlinien für die computerforensische Erfassung von Beweismitteln kennen. Über 80% der befragten Unternehmensleiter zählen den Zahlungskartenmissbrauch und die unkontrollierte Verbreitung persönlicher Daten zu den Hauptbedenken der Konsumenten gegen den E-Commerce. De facto wird der traditionelle Handel im Vergleich zum Handel über dot.com-Firmen von fast allen (88%) als sicherer eingeschätzt[5].

Alle E-Commerce-Konzepte, wie sie in Tabelle 1 wiedergegeben sind, können durch strafbare Handlungen beeinträchtigt werden. Besonders betroffen sind jedoch die sensitiven Bereiche des Online-Zahlungsverkehrs und des E-Bankings, bei denen erhöhte Sicherheitsbedürfnisse bestehen. Sonderprobleme können auch bei spezifischen Online-Transaktionen auftreten. So ergibt sich z.B. aus einer Statistik der NATIONAL CONSUMER LEAGUE (USA), welche die Konsumentenbeschwerden wegen Betrugs im Internet getrennt nach Geschäftsbereichen aufführt, dass deren überwiegender Anteil auf Online-Auktionen entfällt (78%)[6]. Der zentrale Server des Online-Auktionshauses dient dabei in der Regel bloss als Plattform, während die täuschenden Informationen dezentral von den Anbietern eingespeist werden. Gerade die Bereiche des C2C- und des B2C-Marktes sind anfällig für klassische Betrugsformen, vor allen Dingen für den Zahlungskartenbetrug[7].

5 Die Unternehmen sehen ihr E-Commerce-System überwiegend von aussen bedroht (79%), während Straftaten von Insidern, insbesondere von unzufriedenen oder ehemaligen Mitarbeitern, grob unterschätzt werden; KPMG, 2ff. (N = 1253, Rücklauf der schriftlichen Befragung = 9%); vgl. dazu die separaten Resultate der deutschen Stichprobe in: KPMG, efr@ud, 4ff.

6 National Consumers League (ed.), 2000 Internet fraud statistics, abrufbar unter www.fraud.org/internet/lt00totstats.htm (Stand: 17.7.2001).

7 Je nachdem, wer dabei getäuscht wird, fallen solche Sachverhalte in der Schweiz unter Art. 146 StGB (Betrug, falls ein Mensch arglistig getäuscht wird) oder Art. 147 StGB

Tabelle 1: E-Commerce-Konzepte getrennt nach Marktteilnehmern[8]

	Regierung	Unternehmen	Konsumenten
Regierung (G = Government)	**G2G** Bsp.: Koordination, Projektplanung	**G2B** Bsp.: Information, Submissionsausschreibung	**G2C** Bsp.: Information
Unternehmen (B= Business)	**B2G** Bsp.: Dienstleistungen	**B2B** Bsp.: E-Commerce	**B2C** Bsp.: E-Commerce
Konsumenten (C = Consumer, auch P = Peer)	**C2G** Bsp.: Nutzung der Online-Leistungsverwaltung	**C2B** Bsp.: Preisvergleich	**C2C (auch P2P)** Bsp.: Direktvertrieb von Musik usw.

Für die am E-Commerce Beteiligten ergeben sich aus strafrechtlicher Sicht zwei grundsätzlich divergierende Perspektiven:

(1) Es kann einerseits in Frage stehen, ob ein bestimmtes Verhalten der Markteilnehmer nach einer Bestimmung des StGB oder des Nebenstrafrechts strafbar sei. In diesem Zusammenhang sind vor allem die Inhalts- und Informationsverbreitungsdelikte, die Delikte gegen den Geheim- oder Privatbereich sowie die immaterialgüterrechtlichen und wettbewerbsrechtlichen Delikte zu nennen:
   - 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)
   - Pornographie (Art. 197 StGB)
   - öffentliche Aufforderung zu Verbrechen oder zu Gewalttätigkeit (Art. 259 StGB)
   - Störung der Glaubens- und Kultusfreiheit (Art. 261 StGB)
   - Rassendiskriminierung (Art. 261bis 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) u.a.

(betrügerischer Missbrauch einer Datenverarbeitungsanlage, falls ein Rechner "getäuscht" wird).

8 Nach der Tabelle in COPPEL, 4.

(2) Andererseits können die Marktteilnehmer als Geschädigte[9] bzw. "Opfer" von Online-Kriminalität betroffen sein. Dabei fallen insbesondere Angriffe auf die technische Infrastruktur oder die Daten eines E-Commerce-Anbieters in Betracht. Zu nennen sind folgende Computerdelikte:
   - 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 Computerleistungen ("Zeitdiebstahl", Art. 150 StGB).

Diese Aufzählungen sind nicht vollständig. Auch bei der Durchführung anderer Straftaten ist eine Nutzung der Internetdienste möglich, wie etwa bei Anstiftungen zu Vergewaltigung oder Tötung, Erpressungen mittels E-Mail, Nötigung zur einer Unterlassung durch Denial of Service Attacks[10] oder gewöhnlichen Betrügereien durch arglistig täuschende Angaben auf einer Website usw.

Eine weitere Differenzierung ist nach dem Grad der Beteiligung vorzunehmen. Ein E-Commerce-Unternehmen kann selbst als Content-Provider illegale Inhalte wie z.B. rassistische Texte, pornographische Bilddateien[11] oder urheberrechtswidrig erzeugte Kopien von MP3-Musikdaten zugänglichmachen oder verbreiten. Die Verantwortlichen des Unternehmens sind demzufolge als Haupttäter strafbar.

Fall 1: Eine deutsche Firma bietet auf ihrer Website unter anderem ein sogenanntes "Schweine-T-Shirt" einer Punk-Rock-Band zum Kauf an. Die Firma ist auf der Homepage als "Plattenlabel", d.h. als Hersteller und Vertreiber der CDs dieser Band, gekennzeichnet. Das T-Shirt hat als Motiv ein an ein Kreuz genageltes Schwein. Oben am senkrechten Balken des Kreuzes befindet sich in der Mitte ein Schild mit der Aufschrift des Bandnamens. Das Motiv ist christlichen Kreuzesdarstellungen nachgebildet.[12]

9 Im Sinne der §§ 192, 395 Abs. 1 Ziff. 2 ZH-StPO.

10 Näher dazu unter 5.

11 Zur quantitativen Bedeutung von Sex-Angeboten im www und in Newsgroups, siehe DÖRING, 164ff.

12 Beschluss des Oberlandesgerichts Nürnberg vom 23. Juni 1998, Az. Ws 1603/97 (Klageerzwingungsverfahren): "Für den Inhalt der Homepage ist in erster Linie der Ersteller, der sich mit dessen Inhalt selbst identifiziert, verantwortlich." Nach dem Schweizer StGB wäre der Straftatbestand Störung der Glaubens- und Kultusfreiheit (Art. 261 Abs. 1 StGB) relevant.

Möglich ist aber auch die strafbare Teilnahme des E-Commerce-Unternehmers an der Veröffentlichung oder Verbreitung fremder Informationen bzw. Inhalte durch einen Dritten, wie es beispielsweise bei einem Host-Service-Provider auftreten kann, der Dritten vertraglich die Möglichkeit einräumt, Daten auf seinen Web-Server einzustellen. Dabei handelt es sich unter Umständen um einen untergeordneten Tatbeitrag in der Form einer Gehilfenschaft (Art. 25 StGB). Umstritten ist, ob auch eine blosse Zugangsdienstleistung, wie sie von Access-Service-Providern angeboten wird, unter dem Aspekt der Gehilfenschaft zu einer Strafbarkeit führen kann[13].

2. Internationale Sachverhalte – nationales Strafrecht

Der elektronische Geschäftsverkehr kennt keine Landesgrenzen. Die Angebote des web-basierten Handels sind nicht auf nationale Märkte ausgerichtet, und schon heute liefern beispielsweise Online-Buchhandlungen wie amazon.de oder buecher.de kostenlos in die umliegenden Länder, wobei sich dieses Angebot auf Bücher aus dem englischsprachigen Sortiment der Partnerunternehmen erstreckt. Betreiber von Internet-Auktionen richten sich an eine internationale Kundschaft, wobei die Personendaten selbst bei national unterschiedlichen Portalen zentral verwaltet werden. Im Bereiche des Online-Vertriebes von Software, Musik oder Texten wird die weltweite Verbreitung durch das direkte digitale Übermitteln der Informationen noch zusätzlich erleichtert. Wenngleich das Potential des elektronischen Weltmarktes noch nicht voll ausgeschöpft wird, lässt sich schon jetzt prognostizieren, dass parallel zur Entwicklung des elektronischen Geschäftsverkehrs die internationalen Rechtsbeziehungen stark zunehmen werden. Leider geht damit aber auch eine Internationalisierung der kriminellen Tatgelegenheiten einher, wie die jüngsten Meldungen der INTERNATIONAL CHAMBER OF COMMERCE und der EUROPÄISCHEN KOMMISSION klar belegen[14].

Die Frage, welches Land Strafgewalt über solche grenzüberschreitenden Delikte habe, ist eine der aktuellsten im Bereiche des Internetstrafrechts[15]. Das Strafrecht

13 Näher dazu unter 3.

14 ICC Switzerland, Vorsicht Cybercrime!, 12.1.2001, abrufbar unter www.icc-schweiz.ch/d/detail.cfm?inh_id=233&pos=11 (Stand: 17.7.2001); Kommission der Europäischen Gemeinschaften, 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: 17.7.2001).

15 Überblick bei SCHWARZENEGGER, Geltungsbereich, 109ff.

unterscheidet sich in dieser Hinsicht grundlegend vom Internationalen Privatrecht, welches bekanntlich Kollisionen zwischen den verschiedenen Rechtsordnungen vermeiden will. Mit den Regeln des Strafanwendungsrechts bestimmen die Länder autonom und ohne Rücksicht auf Überschneidungen mit dem Strafrecht anderer Länder, wie weit sich ihr Strafanspruch erstrecken soll. Grenzen erwachsen dieser nationalstaatlichen Definitionsmacht allenfalls aus dem Völkerrecht, doch geht auch dieses sehr weit in der Anerkennung von "sinnvollen" Anknüpfungspunkten[16]. Folglich kann es im Strafrecht zu mehrfacher Strafverfolgung und Sanktionierung bezüglich der gleichen Straftat kommen. Diese Gefahr besteht insbesondere bei Internetdelikten, die durch die Verbreitung von strafbaren Inhalten auf dem WWW einen weltweiten Wirkungskreis haben.

Das schweizerische Strafanwendungsrecht (Art. 3 ff. StGB) ist sehr weit gefasst. Neben der Anknüpfung nach dem Territorialprinzip[17], die den Regelfall darstellt, können grenzüberschreitende Straftaten auch nach dem Flaggenprinzip[18], dem Staatsschutzprinzip[19], dem aktiven[20] und passiven[21] Personalitätsprinzip sowie nach dem Weltrechtsprinzip[22] der schweizerischen Strafgewalt unterstehen[23].

Die Anknüpfung nach dem Territorialprinzip wird durch das sogenannte *beschränkte Ubiquitätsprinzip*[24] konkretisiert, d.h. 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 verletztende bzw. gefährdende[25] Straftaten zu den Inlandstaten gezählt werden.

16 Council of Europe, 441ff.; vgl. dazu die berühmte "Lotus"-Entscheidung des Ständigen Internationalen Gerichtshofs, Court Permanente de Justice Internationale [CPJI], Recueil des Arrêts, Sér. A, No. 10, 1927.

17 Art. 3 StGB.

18 Art. 97 LFG (SR 748.0), Art. 4 Abs. 2-3 BG über die Seeschiffahrt unter Schweizer Flagge vom 23.9.1953 (SR 747.30).

19 Art. 4 Abs. 1 StGB, mit Deliktskatalog.

20 Art. 6 Ziff. 1 StGB.

21 Art. 5 Abs. 1 StGB.

22 Art. 6bis StGB, Art. 19 Ziff. 4 BetmG.

23 Siehe dazu den tabellarischen Überblick in SCHWARZENEGGER, Geltungsbereich, 115f. m.N; die Art. 3–7 StGB gelten nach Massgabe von Art. 333 Abs. 1 StGB (Vorbehalt abweichender Regelungen) auch für das Nebenstrafrecht.

24 Art. 7 StGB; vgl. zum parallelen § 9 dStGB BREMER, 125f.; HILGENDORF, 1843ff.; SCHWARZENEGGER, Abstrakte Gefahr, 240ff.; SIEBER, 2065f. alle m.w.N.

25 Genau genommen werden nicht Rechtsgüter gefährdet oder verletzt, sondern die Handlungs- oder Tatobjekte, in denen die Rechtsgüter jeweils konkret verkörpert sind.

2.1. Ort der Ausführung bei Internetdelikten

Massgebend für die Bestimmung des Ausführungsortes ist *immer der physische Aufenthaltsort des Täters* im Moment der inkriminierten Tathandlung.

Verbietet das Strafgesetz beispielsweise das Anpreisen, Anbieten, Zeigen, Auffordern, Verbreiten oder Zugänglichmachen bestimmter Informationen[26], ist der Ausführungsort dort, wo der Täter den Übermittlungs- oder Abspeicherungsbefehl betätigt, mit dem die Datenverarbeitung durch automatisierte Programmabläufe in Gang gesetzt wird.

Fordert der Straftatbestand Öffentlichkeit, ist abzustellen auf den Aufenthaltsort des Täters im Moment der Eingabe des Übermittlungs- bzw. Abspeicherungsbefehls, mit dem die Daten durch automatisierte Programmabläufe auf den öffentlichen Bereich der Festplatte eines Rechners (Web-Server, Usenet-Server) transferiert werden[27]. 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 Ausführungsort[28].

Für die Computerdelikte gilt nichts anderes. Beim Beschaffen von Daten, Eindringen in ein Datenverarbeitungssystem, Verändern von Daten oder Einwirken auf einen Datenverarbeitungsvorgang[29], falls sie über ein Netzwerk begangen werden, liegt der Ausführungsort dort, wo sich der Täter im Moment der Abgabe der diese Prozesse auslösenden Programmbefehle aufhält.

Fall 2: Der 24-jährige Onel de Guzman hat im Verlauf der Ermittlungen eingestanden, von seiner Wohnung in Manila aus versehentlich das "I Love You" Virus als E-Mail-Attachment verbreitet zu haben. Das sich ab 4. Mai 2000 weltweit von Computer zu Computer weiterverbreitende Virus soll nach Schätzungen der Swiss Re innert kürzester Zeit einen Schaden von $ 2,6 Mia. verursacht haben[30].

26 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 zu Gewalttätigkeit), Art. 261bis (Rassendiskriminierung) usw.

27 Zum Begriff der Öffentlichkeit allgemein im StGB und speziell in Art. 261bis StGB (Rassendiskriminierung) FIOLKA/NIGGLI, 533ff. m.N.; NIGGLI, Rassendiskriminierung, N691ff.

28 Ebenso unveröffentl. Entscheid der Anklagekammer des BGer vom 11.8.1999 (BG.43/1999/rei), 5.

29 Vgl. Art. 143, 143bis, 144bis, 147 StGB.

30 Quelle: www.pctip.ch/webnews/wn/18048.asp (Stand: 17.7.2001); vgl. Swiss Re, Natural catastrophes and man-made disasters in 2000, sigma No. 2/2001, 7: "... led to economic damage in excess of USD 1bn."; zum "I Love You" Fall siehe BURKE, 1f.; nach dem Schweizer StGB wäre der Straftatbestand Datenbeschädigung (Art. 144bis Ziff. 1 StGB) relevant.

Der Ausführungsort liegt gemäss Art. 7 Abs. 1 StGB alleine in Manila. Schlägt man das Handeln der Tatmittler (d.h. der nichtsahnenden Opfer, die mit der Aktivierung des Attachments den Beschädigungsprozess auslösten) ebenfalls zum Ausführungsort, wie es die h.L. allgemein bei mittelbarer Täterschaft vertritt[31], wäre an jedem Ort, wo ein Nutzer das Attachment geöffnet und die Schädigung ausgelöst hat, ein Ausführungsort gegeben, also wohl weltweit. Die h.L. basiert aber auf einer Fiktion, welche die Ausführungshandlungen des Täters mit ihren Auswirkungen vermischt und vom Wortlaut des Art. 7 StGB nicht gedeckt ist. Das Verfahren gegen Guzman wurde eingestellt, da auf den Philippinen zur Zeit der Tat keine Strafnorm gegen die Datenbeschädigung bestand.

Einige deutsche Autoren wollen den Begriff der Ausführungshandlung ausweiten auf den Standort des Servers, wohin der Täter seine Daten gezielt und kontrolliert abspeichere[32]. Eine unbefriedigende Konsequenz dieses Ansatzes wäre aber, dass im Resultat völlig zufällige Anknüpfungen möglich werden, weil es sich beim Zielserver letztlich bloss um einen technischen Transitknoten handelt, der irgendwo stehen kann. Diese sogenannte Theorie der langen Hand lässt sich mit dem Wortlaut des geltenden Gesetzes[33] kaum vereinbaren.

Beispiel: Wer etwa aus den USA strafbare Informationen an meine webbasierte Mailadresse schwarzi@yahoo.co.jp sendet (Push), würde zugleich in den USA und in Japan (Mail-Server) handeln, nicht aber in der Schweiz, wohin ich die Mail herunterlade (Pull). Liegt der Mail-Server von Yahoo.co.jp jedoch aus Kostengründen zufällig in Südkorea, würde der Täter in den USA und Südkorea handeln.

31 CASSANI, 247; REHBERG/DONATSCH, 43; STRATENWERTH, AT I, 98; TRECHSEL, N7 zu Art. 7 StGB; siehe auch BGE 78 IV 252; 85 IV 203.

32 CORNILS, 394ff.; ebenso ESER, in: SCHÖNKE/SCHRÖDER, N4 zu §9 dStGB und FISCHER, in: TRÖNDLE/FISCHER, N8 zu §9 dStGB; ähnlich SIEBER, 2068ff. (Tathandlungserfolg).

33 Sowohl Art. 7 StGB als auch § 9 Abs. 1 dStGB sind auf den Ort der Handlung/Ausführung und den Ort des Erfolgseintritts beschränkt. Siehe zur klaren Intention des schweizerischen Gesetzgebers ZÜRCHER, 25f.; vgl. zum Ausführungsort im Sinne von Art. 346 Abs. 1 StGB den unveröffentl. Entscheid der Anklagekammer des BGer vom 11.8.1999 (BG.43/1999/rei), 5: "Als Ausführungsort ... ist somit derjenige Ort anzusehen, von dem aus die Daten an den Server durch den Beschuldigten ... gesendet wurden, und nicht der Ort, wo der Server steht."

2.2. Ort des Erfolgseintritts bei Internetdelikten

Da Internetdelikte häufig im Ausland ausgeführt werden, im Inland aber Wirkungen zeigen, stellt sich die zentrale Frage nach der Bedeutung des Erfolges im Strafanwendungsrecht[34]. Dabei ist umstritten, ob es bei allen Straftatbeständen einen (zum gesetzlichen Tatbestand gehörenden) Erfolg gebe oder dies bei bestimmten Deliktstypen, namentlich den abstrakten Gefährdungsdelikten und den schlichten Tätigkeitsdelikten, nicht der Fall sei[35].

Es lassen sich – bei Abweichungen im Detail – zwei Auslegungsansätze unterscheiden:

Die vom Bundesgericht 1979[36] aus der Lehre[37] übernommene Auslegung des Erfolgsbegriffs in Art. 7 StGB orientiert sich an der Einteilung in die verschiedenen Deliktsarten, also in schlichte Tätigkeitsdelikte bzw. Erfolgsdelikte und in konkrete bzw. abstrakte Gefährdungsdelikte.

34 Zum aktuellen Meinungsstand in der Lehre SCHWARZENEGGER, Abstrakte Gefahr, 240ff.; SCHWARZENEGGER, Geltungsbereich, 120f.; WEBER, 536ff.; für Deutschland FISCHER, in: TRÖNDLE/FISCHER, N5ff. zu §9 dStGB alle m.w.N.

35 Aus der Praxis sind bisher nur vereinzelte Entscheide bekannt, siehe Arrêt du Tribunal correctionnel du District de Lausanne, 7. juillet 1997, medialex 1997, 235 mit Anmerkungen von RIKLIN; aktuell dazu das Urteil des BGH vom 12. Dezember 2000 - 1 StR 184/00 (Volksverhetzung) mit Anmerkungen von SCHWARZENEGGER, Abstrakte Gefahr, 240ff. m.w.N.

36 BGE 105 IV 326, zuletzt bestätigt in BGE 125 IV 180 ff.

37 Insbesondere von SCHULTZ, Geltung, 306ff.; SCHULTZ, Neue Probleme, 81ff.; vgl. zusammenfassend REHBERG/DONATSCH, 42; TRECHSEL, N6 zu Art. 7 StGB alle m.N.

Tabelle 2: Der Deliktstypus der wichtigsten Internetdelikte

STRAFTATBESTAND	DELIKTSTYPUS	GIBT ES EINEN ORT DES ERFOLGSEINTRITTES?
Gewaltdarstellung, Art. 135 StGB	abstraktes Gefährdungsdelikt	nein
Weiche Pornographie, Art. 197 Ziff. 1 StGB (Jugendschutz)	abstraktes Gefährdungsdelikt	nein
Harte Pornographie, Art. 197 Ziff. 3 StGB	abstraktes Gefährdungsdelikt	nein
Weiche Pornographie, Art. 197 Ziff. 2 StGB (Schutz von Erwachsenen vor ungewollter Konfrontation mit Pornographie)	konkretes Gefährdungsdelikt	ja
Aufforderung zu Verbrechen oder Gewalt, Art. 259 StGB	abstraktes Gefährdungsdelikt	nein
Rassendiskriminierung, Art. 261bis StGB	schlichtes Tätigkeitsdelikt	nein
Ehrverletzungen, Art. 173 ff. StGB	Erfolgsdelikte	ja
Wirtschaftlicher Nachrichtendienst, Art. 273 StGB	abstraktes Gefährdungsdelikt	nein (aber eine Anknüpfung gemäss Art. 4 Abs. 1 StGB ist möglich!)
Unbefugte Datenbeschaffung, Art. 143 StGB	Erfolgsdelikt[38] (strittig, nach h.L. schlichtes Tätigkeitsdelikt)	ja (nein, nach h.L.)
Hacking, Art. 143bis StGB	Erfolgsdelikt[39] (strittig, nach h.L. schlichtes Tätigkeitsdelikt)	ja (nein, nach h.L.)
Datenbeschädigung, Art. 144bis StGB	Erfolgsdelikt (Ziff. 1), abstraktes Gefährdungsdelikt (Ziff. 2)	ja (Ziff. 1) nein (Ziff. 2)
Computerbetrug, Art. 147 StGB	Erfolgsdelikt	ja
Urheberrechtsverletzung Werkexemplar herstellen, Art. 67 Abs. 1 lit. e URG Werkexemplare anbieten, veräussern oder verbreiten, Art. 67 Abs. 1 lit. f URG	schlichtes Tätigkeitsdelikt Rechtsgut: freies Verfügungsrecht des Urhebers über sein Werk (soweit nicht eingeschränkt, siehe Art. 19 ff. URG) Tatobjekt: Werkexemplar	nein
Verletzung verwandter Schutzrechte insbes. Art. 69 Abs. 1 lit. c, lit. f URG	schlichtes Tätigkeitsdelikt	nein
Unlautere Werbe- und Verkaufsmethoden insbes. Art. 3 i.V.m. Art. 23 UWG	abstraktes Gefährdungsdelikt	nein

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 in Art. 7 StGB einzig ein zeitlich und räumlich vom Handlungsort abtrennbarer Aussenerfolg, ein *Erfolg im technischen Sinne* gemeint sei, könne bei schlichten Tätigkeitsdelikten und abstrakten Gefährdungsdelikten nicht an einen Erfolg angeknüpft werden. Mit Ausführung der Handlung seien diese Delikte nämlich schon vollendet, so dass es bei ihnen auch keinen – vom Ort der Handlung unterscheidbaren – Ort des Erfolgseintrittes geben könne. Konsequenz: Gehört ein Internetdelikt zu den schlichten Tätigkeitsdelikten oder abstrakten Gefährdungsdelikten, kann es nur dann in der Schweiz verfolgt werden, wenn es hier ausgeführt wurde. Handelt der Täter dagegen im Ausland, entfällt die schweizerische Strafgewalt nach dem Territorialprinzip[40]. Die Anknüpfung an den Erfolg gemäss Art. 7 StGB wird also reduziert auf Distanzdelikte, die einen abtrennbaren Aussenerfolg haben.

Tabelle 2 gibt Aufschluss darüber, zu welchen Deliktstypen die wichtigsten Internetdelikte in der Doktrin gezählt werden. Wie aus der Rubrik ganz rechts zu entnehmen ist, gelten nur wenige dieser Straftatbestände als Erfolgsdelikte oder konkrete Gefährdungsdelikte. Damit wird das Anknüpfungskriterium des Erfolgsortes in Art. 7 StGB stark eingeschränkt, was zu wenig überzeugenden Resultaten führt und den Tätern noch dazu eine Umgehung des schweizerischen Strafrechts ermöglicht ("forum shopping" im Strafrecht).

Fall 3: Eine Täterin sendet aus den USA einem Erwachsenen in der Schweiz per E-Mail-Attachment unaufgefordert einige Bilddateien mit weicher Pornographie zu[41].

Der anwendbare Art. 197 Ziff. 2 StGB ist ein konkretes Gefährdungsdelikt, weil sich das Unrecht der Tat nicht allein aus dem "Anbieten" selbst ergibt (mit Einverständnis des Betroffenen wäre es ja straflos), sondern erst in seiner Verbindung mit dem Erfolg der unfreiwilligen Konfrontation mit der Pornographie. Da bei dieser Variante immer ein abtrennbarer Aussenerfolg gegeben ist, kann die schweizerische Strafgewalt an diesen Erfolgsort angeknüpft werden.

38 SCHWARZENEGGER, Geltungsbereich, 122 (es gibt einen räumlich und zeitlich abtrennbaren Aussenerfolg); a.M. CASSANI, 253; SCHMID, N17 zu Art. 143 StGB und N11 zu Art. 143bis StGB.

39 Siehe vorstehende Fn.

40 CASSANI, 246; NIGGLI, Rassendiskriminierung, N63f.; WIDMER/BÄHLER, 310f.

Anders wäre nach der h.L. zu entscheiden, wenn die Täterin Bilddateien mit harter Pornographie geschickt hätte. Der diesfalls anwendbare Art. 197 Ziff. 3 StGB ist ein abstraktes Gefährdungsdelikt, bei welchem nach h.L. nur eine Anknüpfung am Ausführungsort möglich wäre (= USA). Die schweizerische Strafhoheit entfiele, obwohl die Rechtsgutsgefährdung im zweiten Fall gravierender ist. Der h.L. kann nicht gefolgt werden. Richtigerweise ist die abstrakte Gefahr einer Wahrnehmung im Inland als Erfolg nach Art. 7 StGB zu werten, was für die Begründung der Schweizer Strafhoheit ausreicht (dazu sogleich).

Der zweite Auslegungsansatz geht nicht von der Einteilung der Straftatbestände in Deliktstypen aus, sondern vom Grundparadigma des Strafrechts: dem *Rechtsgüterschutz*. Alle Deliktstypen dienen dem Schutz eines Rechtsgutes vor Verletzung oder Gefährdung, beziehen sich demnach auf einen Erfolg, d.h. eine Aussenwirkung im sozialen Umfeld. So wurde der Erfolgsbegriff in Art. 7 StGB denn auch vom historischen Gesetzgeber verstanden. Die Unterteilung in "erfolghabende" und "erfolglose" Delikte je nach Vorliegen einer räumlich und zeitlich von der Ausführungshandlung abtrennbaren Aussenwirkung ist vor diesem Hintergrund missverständlich. Wenn der Gesetzgeber bei den schlichten Tätigkeitsdelikten oder den abstrakten Gefährdungsdelikten das geschützte Rechtsgut bzw. das Tatobjekt, in welchem es sich verkörpert, und den Erfolg im Tatbestand nicht nennt, heisst das nicht etwa, dass die tatbestandliche Handlung nur um ihrer selbst willen verboten würde, der Tatbestand folglich gar keine Verletzung bzw. Gefahr voraussetze[42]. Ohne eine Verletzung oder Gefahr entstünde gar kein Erfolgsunrecht, das aber bei jedem vollendeten Delikt Voraussetzung für eine Bestrafung ist.

Der Erfolg besteht bei den abstrakten Gefährdungsdelikten in der Schaffung einer sehr nahen Gefahr für noch nicht konkretisierte Tatobjekte (mindestens eines), und der Ort, über den sich diese abstrakte Gefahr erstreckt, lässt sich auch bestimmen. Ausserdem ist zu beachten, dass bei dieser Deliktsart der Ort derAusführungshandlung und der Ort des Erfolgseintritts keineswegs immer deckungsgleich sind. Betreffend Internetdelikte folgt daraus, dass ein im Ausland handelnder Täter der schweizerischen Strafgewalt immer dann untersteht, wenn sich die nahe Gefahr der

41 Dieser Sachverhalt (Versenden von harter Pornographie) lag dem Arrêt du Tribunal correctionnel du District de Lausanne, 7. juillet 1997, medialex 1997, 235, zugrunde. Das Gericht nahm stillschweigend schweizerische Strafgewalt an, was nach dem Auslegungsansatz der h.L. nicht anginge.

42 Vgl. ZÜRCHER, 57; Allgemein ARZT, 168ff.; ROXIN, N88 und N 98 zu §10 dStGB.

Wahrnehmung durch die Möglichkeit des Abrufs der inkriminierten Informationen in der Schweiz realisiert[43].

Zur Verhinderung von Doppelbestrafungen und einer unnötigen Überforderung der Strafverfolgungsbehörden mit aussichtslosen Verfahren bedarf es nicht einer auslegenden Reduktion des Erfolgsbegriffs von Art. 7 StGB, sondern anderer Einschränkungsmassnahmen: Die internationale Zusammenarbeit ist zu verstärken, um eine Verfolgung am Aufenthaltsort des Täters zu ermöglichen, wo sie zweifellos am effizientesten durchgeführt werden kann; in den Strafprozessordnungen ist das Opportunitätsprinzip auf im Ausland ausgeführte Taten, bei denen einzig der Erfolg im Inland eintritt, zu erweitern[44]. Eine quantitative Erfassung der Abfragen, die aus der Schweiz innerhalb eines bestimmten Zeitraumes auf die inkriminierte Website durchgeführt werden, könnte eine wichtige Entscheidungsgrundlage hierfür liefern. Eine geringe Anzahl von Abfragen würde beispielsweise auf eine geringe Gefahr für hiesige Rechtsgüter hindeuten. Werte im mittleren oder höheren Bereich wären dagegen ein Anzeichen für eine bedeutende Gefährdung, die eine Anknüpfung unter die schweizerische Strafgewalt besonders legitimieren[45]. Damit könnte nicht zuletzt auch das *völkerrechtliche Kriterium des "sinnvollen" Anknüpfungspunktes* konkretisiert und im Zusammenhang mit grenzüberschreitenden Internetdelikten praktikabel gemacht werden. Längerfristig sind Fortschritte in der internationalen Harmonisierung der materiellen Strafnormen und ein Ausbau der Rechtshilfe anzustreben[46].

43 RIKLIN, 581f.; SCHWARZENEGGER, Geltungsbereich, 123ff.; WEBER, 538 (Einschränkung: eine erhebliche Betroffenheit des Verletzten); zum deutschen StGB BARTON, 146ff.; HEINRICH, 72ff.; LEHLE, 57ff.; Urteil des BGH vom 12. Dezember 2000 - 1 StR 184/00 (Volksverhetzung) mit Anmerkungen von SCHWARZENEGGER, Abstrakte Gefahr, 240ff. m.w.N.

44 Eine flexible Lösung findet sich beispielsweise in Art. 4 Abs. 1 Ziff. 4 der BE-StPO. Ebenso ganz aktuell in Art. 8 Abs. 2 lit. d des VE zu einer Schweizerischen Strafprozessordnung (ausgearbeitet von Prof. SCHMID): 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 in EIDGENÖSSISCHES JUSTIZ- UND POLIZEIDEPARTEMENT, 36.

45 Vgl. Minnesota v. Granite Gate Resorts, Inc., C6-97-89, Court of Appeals, published September 5, 1997, in einem Fall betreffend Konsumentenbetrug und unlauteren Wettbewerb im Internet (Ausführungsort: Las Vegas, Nevada). Das Gericht bejahte die Strafhoheit des Bundesstaates Minnesota aufgrund einer Abwägung von 5 Kritieren: (1) Quantität der Kontakte mit dem Bundesstaat; (2) Art und Qualität der Kontakte mit dem Bundesstaat; (3) Beziehung zwischen dem Grund der Anklage und dem Kontakt mit dem Bundesstaat; (4) Interesse des Bundesstaates an einer Anknüpfung und (5) Annehmbarkeit für die Parteien.

2.3. Die Anknüpfung von Teilnahmehandlungen

Bei Teilnahmehandlungen in der Schweiz zu einem Internetdelikt, das vollumfänglich im Ausland realisiert wird, würde nach der Rechtsprechung des Bundesgerichts der inländische Ausführungsort des Teilnehmers (Gehilfe, Anstifter) wegen der Akzessorietät zur Haupttat nicht als Anknüpfungspunkt im Sinne von Art. 7 StGB gelten[47].

Diese Einschränkung der schweizerischen Strafhoheit ist für den Bereich des elektronischen Geschäftsverkehrs von zentraler Bedeutung. Eine Strafverfolgung gegen einen inländischen Internet-Service-Provider wegen einer Gehilfenhandlung durch Link-Verweisung oder anderer Teilnahmehandlungen wäre dieser Auffassung zufolge gar nicht möglich[48].

Dem Bundesgericht kann aber nicht gefolgt werden, denn es geht im Strafanwendungsrecht nicht um die Akzessorietät der Strafbarkeit, sondern um die Frage der Lokalisierung einer Straftat. Vom Tatbestandstypus her ist die Teilnahme ein Erfolgsdelikt, das in Handlung (z.B. irgendein die Haupttat fördernder Beitrag) und Erfolg (Durchführung bzw. Versuch der Haupttat) unterteilt wird. Führt der Täter seine Handlung in der Schweiz aus, hat er das Handlungsunrecht hier realisiert. Der schweizerische Ausführungsort der Teilnahme ist als objektives Faktum bei der Tatortbestimmung nach Art. 7 StGB zu berücksichtigen und reicht für eine Anknüpfung an die hiesige Strafhoheit aus. 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[49].

3. Zur strafrechtlichen Erfassung der Internet-Service-Provider

An der Informationsübermittlung im E-Commerce wie auch ganz allgemein an der Internetkommunikation sind verschiedene Dienstleister beteiligt. Unterschieden wird herkömmlicherweise nach:

46 Hinweise dazu unter 6.

47 BGE 81 IV 37; 104 IV 86; 108 Ib 303; vgl. SCHWARZENEGGER, Handlungs- und Erfolgsort, 158f. m.N.

48 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, vgl. z.B. BGE 80 IV 34 bezüglich Art. 5 StGB.

49 Prinzip der identischen Norm, TRECHSEL, N8 zu Art. 7 StGB m.N.

- **Content-Providern** (Inhalte-Anbieter), die eigene Informationen auf dem WWW zur Verfügung stellen bzw. diese bei einem Host-Provider ins Web einstellen,
- **Hosting-** oder **Host-Providern**, die für Dritte in der Regel gegen Bezahlung Speicherplatz auf ihren Webservern zur Verfügung stellen, damit diese darauf ihre Informationen zugänglichmachen können, und
- **Access-Providern**, die Internetnutzern den Zugang zum WWW und anderen Internetdiensten via Modem-, Kabelverbindung usw. ermöglichen.

Zwischen den einzelnen Funktionen gibt es Überschneidungen, etwa wenn ein Content-Provider seinen eigenen Web-Server betreibt oder ein Host-Provider für seine Kunden gleichzeitig das Access-Providing übernimmt. Die Netzwerke selbst, über welche die Datenübertragung ausgeführt wird, werden von *Carriern* und *Network-Providern* betrieben. Als *Nutzer* (User) werden schliesslich die Endkonsumenten bezeichnet, welche die verschiedenen Dienste auf dem Internet anwenden bzw. Informationen austauschen und abfragen.

Fall 4: Spanische Sympathisanten einer peruanischen Unabhängigkeitsbewegung fordern auf ihrer Website, die auf dem Web-Server eines Host-Providers in Australien abgespeichert ist, in verschiedenen Sprachen dazu auf, die Botschaften und Konsulate Perus in Brand zu setzen. Unter den genau beschriebenen Zielobjekten findet sich auch die Botschaft in Bern und das Generalkonsulat in Zürich. Auf diese Inhalte haben auch Schweizer Nutzer via ihren in der Schweiz niedergelassenen Access-Provider Zugang[50].

Fall 5: Einige Holländer schliessen sich zu einer Gruppe "Dutch White Nationalists" zusammen. Ihre rassistische Ideologie wollen sie auch über das WWW verbreiten und schliessen deshalb mit dem US-amerikanischen Host-Provider FRONT14.ORG einen Hosting-Vertrag ab. Auf dem Web-Server von FRONT14.ORG speichern sie ihre Texte unter dem Titel "Aryian Nation" ab, worin sie unter anderem für die "rassische Reinigung des weissen Europas" und eine systematische Diskriminierung anderer "Rassen" eintreten. Auf diese Inhalte haben auch Schweizer Nutzer via ihren in der Schweiz niedergelassenen Access-Provider Zugang[51].

50 Nach dem Schweizer StGB wäre der Straftatbestand öffentliche Aufforderung zu Verbrechen (Art. 259 Abs. 1 StGB) relevant.

51 Der Fall von FRONT14.ORG sorgte im Februar 2001 für Aufsehen, als die Schweizer Access-Provider Sunrise, Diax und IP-Plus (Swisscom) auf Druck der "Aktion Kinder des Holocaust" für ihre Kunden den Zugang zu diesem Web-Server sperrten. Siehe die Meldung und kritische Analyse in Frankfurter Allgemeine Zeitung, Die Schweiz macht

Da sich – wie in den Beispielen – die Haupttäter (Content-Provider) und Host-Provider meistens im Ausland befinden und deshalb in der Schweiz nicht belangt werden können, sind die einzigen Akteure, auf welche die Strafverfolgungsbehörden einen direkten Zugriff haben, die Schweizer Access-Provider. Deshalb wandte sich die Bundespolizei am 23. Juli 1998 an die Access-Provider der Schweiz und forderte diese in einem Rundschreiben auf, ausländische Websites mit gewaltextremistischen bzw. rassistischen Inhalten zu sperren, andernfalls sie sich wegen Vermittlung des Zugangs auf solche Inhalte als Gehilfen strafbar machen könnten[52]. Auf einen ähnlichen Standpunkt stellte sich unlängst auch die Eidgenössische Spielbankenkommission (ESBK), die mit Schreiben vom 1. November 2000 mehr als 200 Unternehmen der schweizerischen Telekommunikationsbranche aufgefordert hat, über 700 Internetspielbanken technisch zu sperren.

Die durch die erste Sperraufforderung veranlasste Diskussion sowie die Frage nach der Bedeutung der Sonderregelungen des Medienstrafrechts (Art. 27 und Art. 322bis StGB) in Bezug auf eine mögliche Strafbarkeit von Access-Providern veranlassten die Bundespolizei, um ein Gutachten des Bundesamtes für Justiz nachzusuchen. Dieses kommt zusammenfassend zur Schlussfolgerung, dass das Internet in der Ausprägung des World Wide Web als Medium der Massenkommunikation i.S.v. Art. 27 StGB zu verstehen sei und daher auf Veröffentlichungen im Web grundsätzlich das Medienstrafrecht Anwendung finde[53].

dicht. Dürfen Provider den Zugang zu bestimmten Websites sperren?, 20. Februar 2001; der Erfolg solcher Aktionen ist höchstens symbolischer Art. FRONT14.ORG kann weiterhin über die erwähnten Schweizer Access-Provider abgerufen werden (letzter Abruf via ANONYMIZER.COM: 17.5.2001). Nach dem Schweizer StGB wäre der Straftatbestand Rassendiskriminierung (Art. 261bis Abs. 2 StGB) relevant.

52 Für eine formelle Sperrverfügung im Sinne der polizeirechtlichen Gefahrenabwehr, die mit einer Strafdrohung gemäss Art. 292 StGB verbunden werden könnte, fehlt es an einer Bundeskompetenz, weshalb die Bundespolizei dazu gar nicht befugt wäre. Zuständig sind die kantonalen Polizeibehörden. Weiterführende Informationen zur Sperraufforderung der Bundespolizei finden sich auf der Website der Schweizerischen Internet User Group: www.siug.ch/bupo/ (Stand 20.6.2001); wie unter 2.3 ausgeführt, wäre nach der Bundesgerichtspraxis eine Gehilfenschaft zu einer Auslandstat in der Schweiz gar nicht verfolgbar!

53 BUNDESAMT FÜR JUSTIZ, 820ff.; vgl. dazu auch das Positionspapier der Bundespolizei zur strafrechtlichen Verantwortung von Internet-Service-Providern, April 2000, abrufbar unter www.admin.ch/bap/d/archiv/berichte/weitere/2000-05-15-d-internet-isp.pdf (Stand: 17.7.2001).

3.1. Die Sonderregelung des Medienstrafrechts (Art. 27, 322bis StGB) und ihre Anwendbarkeit auf Internet-Service-Provider

Bei Mediendelikten, die dadurch charakterisiert sind, dass die strafbare Handlung durch eine Veröffentlichung in einem Medium begangen wird und sich in dieser Veröffentlichung erschöpfen muss, gelten spezielle Regeln für die Teilnahme am Veröffentlichungsprozess. Grundsätzlich ist bei diesen Delikten 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), macht sich subsidiär der verantwortliche Redaktor, oder wo ein solcher fehlt, die für die Veröffentlichung verantwortliche Person nach Massgabe von Art. 322bis StGB strafbar. 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.

Komplizierend tritt aber hinzu, dass nach einem 1999 ergangenen Bundesgerichtsentscheid nicht alles, was sich medial veröffentlichen lässt und in der Veröffentlichung erschöpft, auch immer ein Mediendelikt ist[54]! Das Bundesgericht erwähnt in seiner Entscheidung explizit die Gewaltdarstellungen (Art. 135 StGB), harte Pornographie (Art. 197 Ziff. 3 StGB) oder das Leugnen von Völkermord (insbes. 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 intendiert 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[55]. Auch wenn dies im Bundesgerichtsentscheid und der dort zitierten Literatur nicht ausdrücklich erwähnt wird, geht es hierbei im Kern um die Frage, ob die Privilegierung der Medienverantwortlichen

54 BGE 125 IV 211f.; so schon SCHULTZ, Unerlaubte Veröffentlichungen, 278 und TRECHSEL/NOLL, 229; vgl. BUNDESAMT FÜR JUSTIZ, 832ff.

55 TRECHSEL/NOLL, 230.

nicht eine Verletzung des Gleichbehandlungsgebotes (Art. 8 Abs. 1 BV) und damit verfassungswidrig sei. Tatsächlich gibt es ausländische Rechtsordnungen, die kein Sonderstrafrecht für Mediendelikte vorsehen und trotzdem nicht zu einer Gängelung der Medien mittels unzähliger Strafverfahren gegen Medienschaffende geführt haben.

Da sich der Schweizer Gesetzgeber jedoch bei der Neuregelung des Medienstrafrechts[56] 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 entgegen der Auffassung des Bundesgerichts alle medialen Veröffentlichungen nach Art. 27 und Art. 322bis StGB beurteilt werden sollten, falls sie sich in der Veröffentlichung erschöpfen. Insofern ist die Kritik an BGE 125 IV 206 ff. berechtigt[57]. Festzuhalten bleibt, dass über den Anwendungsbereich des Medienstrafrechts momentan erhebliche Unsicherheit herrscht (vgl. Tabelle 3 zur Unterscheidung im Sinne von BGE 125 IV 206 ff.).

Tabelle 3: Unterscheidung in Medien- und Nicht-Mediendelikte (Auswahl)[58]

Mediendelikte:	Nicht-Mediendelikte:
Ehrverletzungsdelikte (Art. 173 ff. StGB)	Gewaltdarstellung (Art. 135 StGB)
Öffentliche Aufforderung zu Verbrechen oder zur Gewalttätigkeit (Art. 259 StGB)	Drohung (Art. 180 StGB)
Aufforderung und Verleitung zur Verletzung militärischer Dienstpflichten (Art. 276 StGB)	Nötigung (Art. 181 StGB)
Verletzung des Amtsgeheimnisses (Art. 320 StGB)	Pornographie (Art. 197 Ziff. 3 StGB)
Verletzung des Berufsgeheimnisses (Art. 321 StGB)	Schreckung der Bevölkerung (Art. 258 StGB)
Unlauterer Wettbewerb (Art. 3 i.V.m. Art. 23 UWG)	Rassendiskriminierung (Art. 261bis Abs. 4)[59]

56 Vgl. Botschaft über die Änderung des schweizerischen Strafgesetzbuches und des Militärstrafgesetzes (Medienstraf- und Verfahrensrecht), BBl 1996 IV 525; die Neuregelung trat am 1. April 1998 in Kraft, siehe SCHWARZENEGGER, StGB, XXXVIII.

57 REHBERG/DONATSCH, 166; RIKLIN/STRATENWERTH, 13ff.; SCHLEIMINGER/METTLER, 1039ff.

58 Nach TRECHSEL/NOLL, 229 m.N; siehe auch BUNDESAMT FÜR JUSTIZ, 834f.

59 Auch Art. 261bis Abs. 1–3 StGB gelten als Nicht-Mediendelikt; vgl. NIGGLI, Rassendiskriminierung, N1274 m.N; zu den widersprüchlichen Meinungen hierzu zusammenfassend RIKLIN/STRATENWERTH, 15 m.N.

Im Hinblick auf den Fall 4 (Aufforderung zur Brandlegung) wäre demnach ein Mediendelikt gegeben (Art. 27 Abs. 1 StGB). Da die Hauptverantwortlichen in der Schweiz nicht verfolgt werden können, ist zu fragen, ob überhaupt jemand und gegebenenfalls wer i.S.v. Art. 27 Abs. 2 StGB für die Veröffentlichung als verantwortlich gelten könnte. Hauptkriterien für die Bestimmung des Verantwortlichen sind einerseits die Nähe zum Autor und andererseits die Interventionsbefugnis bzw. -möglichkeit innerhalb des Veröffentlichungsablaufs.

Das Gutachten des Bundesamtes für Justiz benennt als subsidiär Verantwortlichen "ersten Grades" den Host-Provider, der es dem Autor erst ermögliche, mit seinen Inhalten auf das Internet zu gelangen. Seine Strafbarkeit bemesse sich nach den Kriterien von Art. 322bis StGB[60]. Dies mag auf den ersten Blick einleuchten und bei Medienunternehmen, die ihre Inhalte parallel im Offline- und Online-Bereich durch eigenes Web-Hosting verbreitet, auch zutreffen[61], mit Blick auf den Normalfall der Webpublikation überdehnt diese Auffassung aber den Anwendungsbereich des Medienstrafrechts. Im Normalfall ist nämlich der Host-Provider weder aktiv am Veröffentlichungsprozess seines Kunden beteiligt, noch überwacht er passiv die entsprechenden Informationsübertragungen. Die Daten werden vom Content-Provider per Webpublishing-Software direkt und automatisiert auf den Web-Server des Host-Providers transferiert. Der Host-Provider betreibt mit anderen Worten einzig die technische Infrastruktur und ist deshalb in der Regel *kein Medienverantwortlicher*[62]. Daher muss er – von den oben erwähnten Ausnahmen abgesehen – gänzlich vom Medienstrafrecht ausgenommen werden, wobei eine Strafbarkeit alleine nach den allgemeinen Voraussetzungen der Gehilfenschaft möglich bleibt[63].

Um so weniger kann ein Access-Provider in der Schweiz als subsidiärer Medienverantwortlicher "zweiten oder letzten Grades" i.S.v. Art. 27 Abs. 2 StGB angesehen werden, wie dies im Gutachten des Bundesamtes für Justiz "innerhalb enger Grenzen" und bei Vorliegen der Voraussetzungen von Art. 322bis StGB bejaht wird[64]. Der Access-Provider wirkt überhaupt nicht an der Veröffentlichung von verbotenen Inhalten auf fremden Servern mit. Seine Dienstleistung beschränkt sich auf das Zur-

60 BUNDESAMT FÜR JUSTIZ, 840f., 844ff.

61 Beispiele: SF/DRS, NZZ, Tages-Anzeiger, BBC Radio, CNN News usw.

62 Vgl. REHBERG/DONATSCH, 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."

63 Eine Erweiterung des Kreises der Medienverantwortlichen wurde mit der Neuregelung des Medienstrafrechts keineswegs angestrebt; siehe RIKLIN/STRATENWERTH, 19f. mit berechtigter Kritik.

64 BUNDESAMT FÜR JUSTIZ, 841ff.

verfügungstellen eines Zugangs zum Internet, der automatisch und unüberwacht abläuft. Da es sich hierbei eigentlich 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[65]. Nach dem geltenden Strafrecht ist strittig, ob die Zugangsvermittlung auch als Beihilfe zur Verbreitung der illegalen Inhalte oder Informationen, also als Unterstützung des Content-Providers, angesehen werden kann, oder ob seine sozialadäquate Infrastrukturleistung grundsätzlich straflos bleiben soll (dazu sogleich unter 3.2).

Im Sinne eines Zwischenfazits kann festgehalten werden, dass das Medienstrafrecht im Kontext von Internet-Publikationen einen viel beschränkteren Anwendungsbereich aufweist, als dies im Gutachten des Bundesamtes für Justiz dargetan wird. Content-Provider sind für eigene Inhalte als "Autoren" allein strafbar. Veröffentlicht ein Medienunternehmen mit Internetpräsenz einen fremden illegalen Inhalt auf dem WWW oder auf anderen massenmedial einsetzbaren Diensten wie Mailinglisten, Newsgroups oder Chat-Rooms, ist es der Sonderregelung von Art. 27 und 322bis StGB unterstellt. Das heisst, die für die Veröffentlichung verantwortlichen Personen werden nur subsidiär verfolgt, wenn der Content-Provider ("Autor") in der Schweiz nicht belangt werden kann[66]. Unter Umständen kann das Zusammenwirken des Content-Providers und der Medienverantwortlichen bei der Planung, Entschliessung und Ausführung der Straftat aber so intensiv sein, dass beide als Mittäter ins Recht zu fassen sind (vgl. Fall 6).

Fall 6: Ein ZSC-Fanclub betreibt eine regelmässig erscheinende Online-Zeitung, in der unter anderem auch elektronische Leserbriefe von Dritten veröffentlicht werden. Ein Vorstandsmitglied, das mit der Produktion der Web-Zeitung betraut ist, sichtet alle eingehenden E-Mails der Fans und wählt die publikationswürdigen Beiträge selbst aus. Eines Tages wählt es einen Text aus, der verleumderische Äusserungen gegenüber einem namentlich erwähnten Eishockey-Schiedsrichter enthält. Das Vorstandsmitglied selbst hält die Aussagen für völlig gerechtfertigt.

65 REHBERG/DONATSCH, 169; RIKLIN/STRATENWERTH, 21; WEBER, 547.

66 Nach der hier vertretenen Auffassung gilt dies für alle im Internet begangenen Äusserungsdelikte, soweit sie sich in der Veröffentlichung erschöpfen. Folgt man der Differenzierung des BGer (vgl. Tabelle 3), wären die Medienverantwortlichen bei Nicht-Mediendelikten – wie etwa in Fall 5 – immer nach Massgabe der allgemeinen Regeln über die Teilnahme (insbes. Gehilfenschaft, Art. 25 StGB) zu beurteilen; vgl. dazu die Ausführungen in BUNDESAMT FÜR JUSTIZ, 852ff.

Im Normalfall, d.h. in Fällen, in denen der Host-Provider keine Entscheidungs- und Eingriffsbefugnisse im Veröffentlichungsprozess hat, sind immer und alleine die allgemeinen Regeln über die Teilnahme anwendbar. Dies gilt allemal für den Access-Provider[67].

3.2. Die Gehilfenschaft (Art. 25 StGB) und ihre Anwendbarkeit auf Internet-Service-Provider

Bei beiden, Nicht-Mediendelikten (Fall 5) wie Mediendelikt (Fall 4), käme folglich meistens nur eine Gehilfenschaft des Host- und Access-Providers i.S.v. Art. 25 StGB in Frage. Damit sind gleichzeitig die unscharfen strafrechtsdogmatischen Grenzen zwischen Erlaubtem und Verbotenem bei Hilfe durch "harmlose Alltagshandlungen" bzw. "neutrale Handlungen" angesprochen[68]. Klärungsbedürftig – mindestens hinsichtlich der Hilfe durch den Access-Provider – ist auch die Fragen nach der Dauer der verschiedenen Äusserungsdelikte bzw. nach dem Zeitpunkt, bis zu welchem diese noch gefördert werden können. Ginge man, wie es die h.L. in den meisten Fällen tut, von einem Zustandsdelikt aus, wäre das Delikt mit dem Abspeichern auf einem Host-Server schon vollendet und beendet, also lange bevor ein Access-Provider wegen einer konkreten Nutzerabfrage überhaupt eine Gehilfenhandlung beisteuern könnte[69].

Objektiv gesehen erhöht das Einräumen eines Speicherplatzes auf einem Web-Server (Host-Providing) unzweifelhaft die Erfolgschancen der Haupttat, ist also als tatfördernde Gehilfenhandlung anzusehen[70]. Selbst das Verschaffen eines Zugangs zum Internet (Access-Providing) lässt sich – vom Schwanz her aufgerollt[71] – noch als objektive Förderung der Veröffentlichung des Haupttäters verstehen, weil die illegale Information nur dadurch überhaupt zum Nutzer gelangen kann. Folgt man dieser Logik, gibt es unweigerlich immer einen Access-Provider, der zum Gehilfen des Content-Providers erklärt werden kann! Wen die Strafbarkeit trifft, hängt dann

67 Entgegen BUNDESAMT FÜR JUSTIZ, 844ff.

68 Vgl. dazu FORSTER, 425ff.; NIGGLI, Klassische Teilnahme, 25ff.; REHBERG/DONATSCH, 131ff.; STRATENWERTH, AT I, 377f.; WOHLERS, 425ff. alle m.N.; siehe auch BGE 119 IV 289ff. (Antilopenfleisch); 121 IV 109ff. (Telekiosk-Entscheid, Verbreitung von Pornographie mit Hilfe der PTT).

69 Die Frage wurde erstmals im Zusammenhang mit der strafrechtlichen Bewertung von Links aufgeworfen, siehe SCHWARZENEGGER, Gefangen?, 71, mit Lösungsansatz für Art. 261bis StGB; näher dazu unter 4.

70 Zum objektiven Tatbestand der Gehilfenschaft statt aller REHBERG/DONATSCH, 130f.

71 Es wurde schon weiter oben erwähnt, dass der Access-Provider im Grunde ein Gehilfe des Nutzers und nicht des Content-Providers ist.

einzig davon ab, über welchen Access-Provider der Nutzer gerade den illegalen Inhalt abruft.

In subjektiver Hinsicht reicht ein Eventualvorsatz beim Gehilfen aus, d.h. die Kenntnis der deliktischen Absicht des Täters und Inkaufnahme der entsprechenden strafbaren Handlung. Weil aber allen Access-Providern bekannt sein muss, dass im Internet auch illegale Inhalte verbreitet und von ihren Nutzern mehr oder weniger häufig abgerufen werden, liesse sich dieser Eventualvorsatz bejahen, vor allem dann, wenn der Access-Provider durch eine Strafverfolgungsbehörde auf bestimmte strafbare Inhalte hingewiesen wird[72].

Hinsichtlich der Gehilfenschaft des Host-Providers ist zu entscheiden, ob es sich um ein aktives Tun (aktives Betreiben eines Web-Server) oder Unterlassen (Nichtüberwachung der Web-Publikation der Content-Provider) handelt und ob letzterenfalls eine Garantenstellung (z.B. aus Ingerenz) besteht. Diese dogmatisch schwierigen Probleme konnten in der Schweiz noch keiner Lösung zugeführt werden[73]; das geltende Strafrecht erlaubt wie gesehen "beinahe jede mögliche Auslegung"[74].

Die mit diesen Problemen einhergehende Rechtsunsicherheit hat den deutschen Gesetzgeber schon 1997 dazu bewogen, innert kürzester Zeit eine spezialgesetzliche Verantwortlichkeitsregelung für alle Rechtsgebiete vorzunehmen (in § 5 Teledienstegesetz bzw. § 5 Mediendienstestaatsvertrag). Unter dem Einfluss dieses deutschen Vorbilds hat die Europäische Union am 8. Juni 2000 eine Richtlinie über den elektronischen Geschäftsverkehr verabschiedet, die eine ähnliche, aber in einzelnen Punkten detailliertere Verantwortlichkeitsabgrenzung wie § 5 TDG/MDStV vorsieht und durch die Mitgliedsstaaten bis 17. Januar 2002 in die nationale Rechtsordnung umgesetzt werden muss[75]. Frankreich, England und Deutschland, die sich als Standorte für den E-Commerce profilieren wollen, sind jetzt gerade an der Verabschiedung der notwendigen gesetzlichen Anpassungen. In Deutschland hat die Bundesre-

72 So in der Tat BUNDESAMT FÜR JUSTIZ, 853.

73 Siehe RIKLIN, 585; WEBER, 547; WIDMER/BÄHLER, 326ff.; entgegen BUNDESAMT FÜR JUSTIZ, 853, kann der Telekiosk-Entscheid (BGE 121 IV 109ff.) nicht zur Begründung der strafrechtlichen Verantwortlichkeit der Host- oder Access-Provider herangezogen werden. Die PTT hatte damals bestimmten Telekioskbetreibern spezielle Dienste zur Verfügung gestellt, besorgte das Inkasso und bezog dafür hohe Gebühren, was sogar als Mittäterschaft der Verantwortlichen angesehen werden könnte.

74 NIGGLI, Fehlende Rechtssicherheit, B 15; siehe auch NIGGLI/SCHWARZENEGGER, 5ff.

75 Vgl. Art. 12ff. der Richtlinie 2000/31/EG des Europäischen Parlaments und des Rates vom 8. Juni 2000 über bestimmte rechtliche Aspekte der Dienste der Informationsgesellschaft, insbesondere des elektronischen Geschäftsverkehrs im Binnenmarkt, ABl. L 178 vom 17.7.2000, 1ff., abrufbar unter www.ispo.cec.be/ecommerce/legal/documents/2000_31ec/2000_31ec_de.pdf (Stand: 17.7.2001).

gierung bereits das entsprechende Umsetzungsgesetz in den Bundestag geschickt[76]. Mit der E-Commerce-Richtlinie wird ein einheitlicher rechtlicher Rahmen für ganz Europa abgesteckt, der von den Mitgliedsstaaten weder verschärft noch abgeschwächt werden kann.

Inhaltlich stuft die E-Commerce-Richtlinie die Verantwortlichkeit nach den verschiedenen Typen von Providern ab:

- Art. 12 RL entbindet Access-Provider für die reine Durchleitung und das automatische kurzzeitige Zwischenspeichern von Informationen von jeder Verantwortung, sofern sie die relevanten Übermittlungen nicht veranlassen, den Adressaten nicht auswählen sowie die übermittelten Informationen nicht verändern.
- Art. 13 RL enthält eine analoge Freistellung der Provider, die zum Zwecke der Effizienzsteigerung eine automatische, zeitlich begrenzte Zwischenspeicherung vornehmen (Caching). Art. 13 Ziff. 1 lit. e RL sieht aber eine Pflicht zur Sperrung bzw. Entfernung vor, sobald der Provider tatsächliche Kenntnis davon erhält, dass die Information am ursprünglichen Ausgangsort der Übertragung aus dem Netz entfernt oder der Zugang zu ihr gesperrt wurde oder ein Gericht oder eine Verwaltungsbehörde die Entfernung oder Sperrung angeordnet hat.
- Art. 14 RL sieht vor, dass ein Host-Provider nicht verantwortlich ist, sofern er keine tatsächliche Kenntnis von der rechtswidrigen Tätigkeit oder Information hat. Erhält er diese Kenntnis, muss er unverzüglich tätig werden, um die Information zu entfernen oder den Zugang zu ihr zu sperren; eine allgemeine Überwachungspflicht besteht für Host-Provider nicht (Art. 15 RL).

Mit Blick auf die Rechtssicherheit ist auch in der Schweiz eine explizite Regelung von Täterschaft und Teilnahme im Telekommunikations- und Teledienstebereich wünschenswert. Die Schwierigkeiten einer konsistenten Integration einer Horizontalregelung in das Strafrecht, wie sie in Deutschland mit § 5 TDG/MStV aufgetreten sind und intensiv diskutiert werden[77], sowie die zeitliche Dringlichkeit, lassen eine

76 Entwurf eines Gesetzes über rechtliche Rahmenbedingungen für den elektronischen Geschäftsverkehr (Elektronischer Geschäftsverkehr-Gesetz – EGG), Februar 2001, abrufbar unter www.bmwi.de/Homepage/download/infogesellschaft/EGG-Entwurf.pdf (Stand: 17.7.2001).

77 Eingehend HAFT/EISELE, 53ff.; KÜHL, in: LACKNER/KÜHL N7a zu §18 dStGB; LENKNER/PERRON, in: SCHÖNKE/SCHRÖDER, N66bff. zu §18 dStGB "... in mehrfacher Hinsicht unklar ... hat zu zahlreichen Rechtsunsicherheiten geführt: ..." alle m.w.N; zu parallelen Problemen im Haftpflichtrecht siehe SPINDLER, N28ff.: "Verschuldensregelung oder akzessorische Norm? ... Nach dem Begriff der "Verantwortlichkeit" sucht man im allgemeinen Deliktsrecht vergeblich."

Regelung im Strafrecht selbst, und zwar wegen der starken Überschneidungen mit dem Medienstrafrecht im Kontext von Art. 27 StGB als vorzugswürdig erscheinen. Ein entsprechender Gesetzesvorschlag wurde von Ständerat PFISTERER als Motion eingereicht und vom Ständerat am 6. März 2001 angenommen. Der Bundesrat hat dabei seine Bereitschaft bekundet, auf der Grundlage der Motion eine Revision des StGB zu prüfen[78].

Die Motion schlägt eine Neuregelung der Art. 27 ff. StGB vor, wobei diese nicht auf die Internetkommunikation beschränkt werden soll, sondern auch für andere Kommunikationsnetze wie das Telephon-Festnetz, Mobiltelephonnetz oder Fernsehkabelnetz gelten soll. Zudem werden darin die Überschneidungen zwischen Medien- und Netzwerkdelikten widerspruchsfrei gegeneinander abgegrenzt, wobei das Privileg für die Medienverantwortlichen auch im Online-Bereich aufrecht erhalten bleibt. Ähnlich wie in § 5 TDG/§ 5 MDStV bzw. Art. 12 ff. der E-Commerce-Richtlinie wird die Provider-Verantwortung nach der Art der Teledienste differenziert, wobei insbesondere die Access-Provider gänzlich von der strafrechtlichen Verantwortlichkeit ausgenommen werden. Der Revisionsvorschlag der Motion PFISTERER hat folgenden Wortlaut:

Art. 27 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 von Art. 27ter StGB und der nachfolgenden Bestimmungen, der Autor allein strafbar.

Abs. 2-4 unverändert

Art. 27bis StGB – Quellenschutz

unverändert

Art. 27ter StGB – 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.

78 Vgl. Amtliches Bulletin 2001, 28; weiterführende Informationen zur Motion PFISTERER (Netzwerkkriminalität) sind abrufbar unter www.parlament.ch/afs/data/d/gesch/2000/d_gesch_20003714.htm (Stand: 17.7.2001). Der darin enthaltene StGB-Revisionsentwurf geht auf einen Vorschlag von NIGGLI/SCHWARZENEGGER, 1ff., zurück.

Nimmt der Anbieter eine redaktionelle Informationskontrolle im Sinne von Art. 27 Abs. 2 StGB wahr, so wird er strafbar nach Massgabe von Art. 27 und 322bis StGB.

2. Wird mit fremden Informationen, namentlich Inhalten, eine strafbare Handlung begangen, ist derjenige, der diese Informationen zur Nutzung einem Telekommunikationsnetz bereithält, 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. Eine automatische und kurzzeitige Speicherung fremder Informationen infolge automatisierter Übermittlung gilt als Zugangsvermittlung.

Art. 27^{quater} StGB – Vorbehalt anderer Gesetze

Verpflichtungen zur Sperrung der Nutzung von Informationen nach anderen Gesetzen bleiben unberührt, wenn die in Art. 27ter StGB genannten Personen von diesen Informationen rechtmässig Kenntnis erlangen und eine Sperrung technisch möglich und zumutbar ist.

Art. 340ter StGB

Der Bundesgerichtsbarkeit unterstehen weiter strafbare Handlungen in Telekommunikationsnetzen (Art. 27ter und 27^{quater} StGB).

4. Zur strafrechtlichen Erfassung von Links

Links sind ein zentraler Bestandteil des World Wide Web. Durch die Dokumentenbeschreibungssprache HTML können irgendwelche Texte, Bilder oder Websites beliebig miteinander verlinkt bzw. verknüpft werden. Dabei spielt es keine Rolle, ob die Verknüpfung mit einer anderen Stelle des gleichen Dokuments, mit einem anderen Dokument der gleichen Website oder mit einer ganz anderen Website eingerichtet wird. Gerade diese Vernetzung der abrufbaren Informationen auf dem Web hat zur Attraktivität dieses Mediums wesentlich beigetragen. In letzter Zeit haben aber besonders die "strafbaren Links", beispielsweise auf rassistische oder pornographische Inhalte oder auf raubkopierte Musik, öffentliche Beachtung gefunden. Wegen der internationalen Netzstruktur stellt sich in vielen Fällen zunächst die Frage, wo ein Sachverhalt räumlich anzusiedeln und welche nationale Rechtsordnung dafür zuständig sei[79].

79 Näher dazu unter 2.

4.1. Multidimensionale Probleme und Lösungen

Es gibt grundsätzlich drei Varianten von Links: einfache Links (hypertext reference), Bild- oder Inline-Links und Links in sogenannten Frames, d.h. in Teilbereichen des Browser-Fensters:

- Der **einfache Link** ist die am häufigsten eingesetzte Methode des Verweisens im World Wide Web. Solche Links sind leicht erkennbar durch die Hervorhebung mit einer anderen Farbe (üblicherweise blau), eventuell ergänzt durch eine Unterstreichung. Klickt der Nutzer auf diesen Link, wird automatisch das verknüpfte Web-Dokument angezeigt. Der Uniform Resource Locator (URL), die genau Adresse des Dokuments, der mit dem Link erschlossenen Website erscheint in der entsprechenden Browser-Anzeige, während das Ausgangsdokument in der Regel nicht mehr angezeigt wird. Teilweise wird gemäss Konfiguration des Link-Setzers mit dem Anwählen des Links auch ein neues Fenster im Browser eröffnet, wobei das Ausgangsdokument im Hintergrund geöffnet bleibt.
- **Bild-** oder **Inline-Links** erlauben es, Bilddateien von einer anderen Website abzurufen und in das Dokument zu integrieren, auf welchem der Link gesetzt wurde. Durch Inline-Links werden also fremde Inhalte, etwa Bilder oder Suchmasken, im Browser am definierten Ort im eigenen Dokument wiedergegeben. Es ist kein Anklicken mehr nötig; dem Nutzer bleibt der URL des verlinkten Dokuments verborgen. So lassen sich WWW-Seiten mit Inhalten unterschiedlichen Ursprungs ergänzen.
- Mit dem **Framing** wird das Browser-Fenster in verschiedene Bereiche aufgeteilt, wobei jeder Teilbereich ein anderes Dokument anzeigt. Es ist möglich, dass alle Inhalte von der gleichen Website stammen. Durch Links, die in einem Frame-Bereich angebracht sind, können aber auch Inhalte anderer Websites in den eigenen Rahmen eingebettet werden. Wenn der Link auf eine Unterebene (deeplinking) einer anderen Website verweist, kann damit die Homepage des Inhalteanbieters samt allfälliger Werbung unterlaufen werden. Häufig wird ein eigenes Inhaltsverzeichnis in einem Rahmenfeld mit Dokumenten ganz unterschiedlicher Herkunft verlinkt, deren URL regelmässig nicht im Browser angezeigt werden.

Für die strafrechtliche Beurteilung ist es bedeutsam, welcher Art die konkrete Verknüpfung von eigenen und fremden Inhalten ist. Neben der technischen Gestaltung der Links sind noch weitere Dimensionen bei der strafrechtlichen Beurteilung zu beachten: eine *räumliche*[80] und eine *gesetzesbegriffliche Dimension*, in Ausnahmefällen kommt auch eine *Teilnahme an einem Mediendelikt* in Betracht. Bedenkt man

80 Dazu oben unter 2., insbes. 2.3.

die vielfältigen Kombinationsmöglichkeiten dieser Bereiche, wird deutlich, wieso es keine einfache Anwort auf die Frage nach der strafrechtlichen Verantwortung für das Setzen von Links gibt.

4.1.1. Gesetzesbegriffliche Dimension

Das Strafgesetzbuch belegt je nach Bestimmung jeweils eine andere Tathandlungen mit Strafe: Zum Beispiel erfasst die Rassendiskriminierungsnorm in Art. 261bis Abs. 3 StGB "organisieren, fördern, daran teilnehmen", während die üble Nachrede in der Version von Art. 173 Ziff. 1 Abs. 2 StGB durch "weiterverbreiten" geschieht. Weiche oder harte Pornographie i.S.v. Art. 197 Ziff. 1 und Ziff. 3 kann via Internet "zugänglich gemacht" werden.

Die unterschiedliche Umschreibung des strafbaren Verhaltens führt dazu, dass das Einrichten eines Links auf kriminelle Inhalte als eigenständige Täterschaft (Haupttäterschaft) anzusehen ist, wenn der Gesetzgeber die "blosse" Hilfe als unabhängige Tathandlungsvariante in den Tatbestand aufnimmt wie im Beispiel der Rassendiskriminierung (Art. 261bis Abs. 3 StGB). Obwohl der Linksetzende also die rassendiskriminierende Propaganda nicht selbst veröffentlicht, ist er durch deren Förderung Haupttäter[81].

Im Normalfall ist ein Link dagegen unter dem Aspekt der Gehilfenschaft zu beurteilen (Art. 25 StGB), weil ein "Verbreiten", "Anpreisen", "Anbieten", "Zeigen" oder "Auffordern" durch den Link selbst nicht begangen wird. Die Abrufwahrscheinlichkeit und Reichweite der inkriminierten Informationen, auf welche der Link verweist, wird aber dadurch zweifelsohne gesteigert, und somit die strafbewehrte Haupttat objektiv gefördert.

Immerhin muss der Linksetzer auch in subjektiver Hinsicht alle objektiven Tatbestandsmerkmale der Haupttat sowie seinen Förderungsbeitrag wissen und wollen, wobei in der Mehrzahl der anwendbaren Straftatbestände eine Inkaufnahme ausreicht (Eventualvorsatz). Ein Eventualvorsatz ist selbst dann zu bejahen, wenn neben dem Link ein sogenannten *Disclaimer* darauf hinweist, dass sich der Linksetzer nicht mit dem fremden Inhalt auf der verlinkten Webpage identifiziere und jede Haftung für deren Inhalt ablehne. Hier widersprechen sich nämlich Tat und Wort, denn mit dem Einrichten des Links wird die Förderung der Haupttat faktisch hingenommen, auch wenn dies nicht den Wünschen des Täters entsprechen sollte.

81 Allgemein, ohne Bezug zur Link-Problematik NIGGLI, Rassendiskriminierung, N901 m.N; dies gilt interessanterweise nicht für das Fördern der Tathandlungen gemäss Art. 261bis Abs. 4 StGB (z.B. Leugnen des Völkermordes), wo die allgemeinen Regeln der Gehilfenschaft anwendbar bleiben, d.h., wer bei der Verbreitung der Auschwitzlüge hilft, ist dadurch nicht automatisch ein Haupttäter.

Ein Gehilfenvorsatz ist dagegen immer dann ausgeschlossen, wenn die strafbaren Inhalte erst nach der Link-Setzung und ohne Kenntnis des Link-Setzers eingefügt werden.

Schwierig einzuordnen ist die Tathandlung des *Zugänglichmachens*[82], denn dafür genügt es, wenn der Täter einem anderen, sei es nur durch das Bereitstellen auf einem Web-Server, die Möglichkeit eröffnet, sich durch sinnliche Wahrnehmung vom inkriminierten Inhalt Kenntnis zu verschaffen[83]. Mit dem Link wird zwar nicht der fremde Inhalt selbst bereitgehalten, doch indem den Nutzern einerseits die Suche nach dem Inhalt und andererseits die manuelle URL-Eingabe abgenommen, das heisst, mit einem Mausklick die Gelegenheit zur Kenntnisnahme geboten wird, erscheint das Setzen selbst eines einfachen Links schon als Verschaffen des Zugangs. Wegen des weitgefassten Begriffsgehalts von Zugänglichmachen liegt es daher nahe, den Link schon als eigenständige Ausführung der tatbestandsmässigen Handlung anzusehen, was bei Vorliegen der anderen Voraussetzungen zu einer Bestrafung als Haupttäter führen muss[84].

Fall 7: Im Februar 2000 wurde bekannt, dass ein Professor einer Schweizer Hochschule auf seiner Instituts-Website Links auf zwei Link-Listen mit Verweisen auf ras-

82 Das StGB kennt diese Tathandlungsvariante bei Art. 135 Abs. 1 (Gewaltdarstellung), Art. 144bis Ziff. 2 (Datenbeschädigung), Art. 179bis (Abhören und Aufnehmen fremder Gespräche), Art. 179ter (unbefugtem Aufnehmen von Gesprächen), Art. 179^{quater} (Verletzung des Geheim- oder Privatbereichs durch Aufnahmegeräte), Art. 197 Ziff. 1 und Ziff. 3 (Pornographie), Art. 267 Ziff. 1 Abs. 1 und Ziff. 2 (diplomatischer Landesverrat), Art. 273 (wirtschaftlicher Nachrichtendienst).

83 So die einschlägige Definition in KÜHL, in: LACKNER/KÜHL, N5 zu §18 dStGB m.N.; LENCKNER/PERRON, in: SCHÖNKE/SCHRÖDER, N15 zu §184 dStGB; siehe auch TRECHSEL, N6 zu Art. 197 "... "zugänglich gemacht" [ist die Sache], wenn dem Kind die Möglichkeit eröffnet wird, sich selbst den Gewahrsam zu verschaffen." Diese Definition ist allerdings zu stark auf körperliche Gegenstände eingeschränkt.

84 So explizit BOESE, 115f. m.w.N.; zum "Zugänglichmachen" von Inhalten nach §§ 130 Abs. 2 Nr. 1 lit. b, 130a Abs. 1, Abs. 2 Nr. 1, 131 Abs. 1 Nr. 2, 184 Abs. 1 Nr. 1--2, Abs. 3 Nr. 2 dStGB. "Eine körperliche Überlassung ist demnach nicht erforderlich, weswegen etwa auch die Darstellung auf einem Monitor ausreicht."; siehe auch BARTON, 136ff., 243ff. m.w.N; STRATENWERTH, BT II, 246 m.N., weist im Zusammenhang mit dem wirtschaftlichen Nachrichtendienst (Art. 273 StGB) darauf hin, dass "... der Begriff des "Zugänglichmachens" die "Perspektive einer schrankenlosen extensiven Auslegung" [eröffnet] ... Er umfasst ... jedes Verhalten, das einem ausländischen Adressaten die Möglichkeit verschafft, in schweizerische Geschäftsgeheimnisse Einblick zu erlangen ..." (Hervorhebung im Original).

sistische bzw. pornographische Websites gesetzt hatte. Auf der pornographischen Link-Liste, für die keine Zugangskontrolle bestand, wurden per Inline-Link in abwechselnder Folge Bilder eingefügt, die Erwachsene beim Geschlechtsverkehr zeigten. Die andere Link-Liste mit Verweisen auf rassistische Inhalte auf dem WWW war Teil einer Anti-Hate-Website. Sowohl die Link-Listen selbst wie auch die darin nachgewiesenen Websites waren auf Web-Servern im Ausland (mehrheitlich in den USA) abgespeichert. Der Professor wollte mit seiner Aktion gegen die Reglementierung der Informatikdienste an der Hochschule und die Beschränkung der Meinungs(äusserungs)freiheit protestieren[85].

Folgt man der soeben erläuterten weiten Auffassung hinsichtlich des Begriffes des Zugänglichmachens, so ist der Link auf die Porno-Link-Liste selbst schon eine tatbestandsmässige Handlung im Sinne von Art. 197 Ziff. 1 StGB. Da man mit dem Anklicken des Links auch direkt pornographische Bilddaten einsehen konnte und sich diese Möglichkeit mangels Alterskontrolle auch den unter 16jährigen bot, sind alle objektiven Tatbestandsmerkmale von Art. 197 Ziff. 1 StGB erfüllt. Subjektiv ist wohl ein Eventualvorsatz anzunehmen. Da die Tathandlung in der Schweiz ausgeführt wurde und es sich nicht um eine Teilnahme handelt, wäre auch Schweizer Strafhoheit gemäss Art. 3 i.V.m. Art. 7 StGB gegeben[86].

Um einer ausufernden Kriminalisierung von Links Einhalt zu gebieten, müsste der Begriff des Zugänglichmachens einschränkend ausgelegt werden. Dafür böte sich etwa die Möglichkeit an, zur Erfüllung der Tathandlung als Haupttäter zusätzlich die Verfügungsmacht über die inkriminierten Daten – als Äquivalent zum Besitz von Sachen – zu verlangen[87]. Diese Interpretation vermag jedoch nicht zu befriedigen, weil auch in der realen Welt ein Zugänglichmachen ohne Besitz der Sache möglich ist und die einschlägigen Tatbestände nichts dergleichen bestimmen. Denkbar wäre auch eine "Entkriminalisierung" durch restriktive Auslegung anderer objektiver Tatbestandsmerkmale, etwa des Begriffs der weichen Pornographie bei Art. 197 Ziff. 1 StGB. Das Problem liegt aber letztlich im Tathandlungsbegriff selbst begründet und kann daher nur durch den Gesetzgeber mittels klarerer (engerer) Definitionen gelöst werden. Mehr Verwirrung als Klarheit hat im übrigen der Versuch in

85 Vgl. zu diesem Fall die Meldungen in NZZ 23. Februar 2000, 41; NZZ 24. Februar 2000, 42 und NZZ 3. März 2000, 75.

86 Zur Frage der Links auf Link-Listen und den Grenzen der Strafbarkeit für Links SCHWARZENEGGER, Gefangen?, 71.

87 So GERMANN, 212.

Deutschland gestiftet, die Verantwortlichkeitsregelung gemäss § 5 Abs. 1–3 TDG/MDStV auf die Link-Verweise anzuwenden[88].

Hinzu kommt, dass fremde (kriminelle) Inhalte bei Inline-Links oder beim Framing derart in ein eigenes Dokument einbezogen werden können, dass sie für den Betrachter als Bestandteil desselben Dokuments erscheinen. Je nach der technischen Gestaltung kann daher eine Inhaltsverknüpfung, die beim einfachen Link noch als Gehilfenschaft zu bewerten wäre, bei einem Inline-Link oder beim Framing als Haupttäterschaft erscheinen. Künftige Browser-Generationen werden die Art der Präsentation des Links allerdings völlig unabhängig vom Link machen, was die strafrechtliche Verantwortungszuschreibung erschweren wird, weil der Nutzer dann eine entsprechende Darstellungswahl hat.

4.1.2. Mediendelikte und Links

Gelten die Sonderregelungen des Medienstrafrechts auch für das Setzen eines Links? Dies tun sie nur in den seltenen Fällen, in denen der Linksetzende direkt am Veröffentlichungsprozess beteiligt ist. In der Regel wird er aber mit dem Link auf einen schon früher von einem Dritten im Internet veröffentlichten Inhalt verweisen. Für Personen, die nicht am eigentlichen Veröffentlichungsprozess mitwirken, ergibt sich die strafrechtliche Verantwortung aber nicht aus der Sonderregelung des Medienstrafrechts (Art. 27 StGB), sondern aus Art. 25 StGB. Liegt dagegen nach der Tatbestandsfassung eine Haupttäterschaft vor, entfällt eine Teilnahme an der Veröffentlichung allemal.

4.2. Dauer eines Delikts und Zeitpunkt der Teilnahme

Im Zusammenhang mit dem zeitlichen Ablauf einer strafbaren Veröffentlichung und der dazugehörigen Linksetzung stösst man auf ein weiteres Problem, dass noch kaum diskutiert wurde: Ist es möglich, eine strafbare Handlung zu fördern oder daran teilzunehmen, die schon lange abgeschlossen ist? Ist es beispielsweise noch ein Fördern, wenn ein halbes Jahr nach Einrichtung einer rassistischen Website auf diese ein Link gesetzt wird? Die einhellige Lehre setzt bei sogenannten Zustandsdelikten voraus, dass Gehilfenhandlungen spätestens bis zur Vollendung der Haupttat

88 Man vergleiche die gegensätzlichen Standpunkte in BOESE, 49ff.; GERMANN, 211ff.; LENCKNER/PERRON, in: SCHÖNKE/SCHRÖDER, N66i zu §184 m.w.N.; überzeugend die Ausführungen von BARTON, 244ff., Beschränkung der Verantwortlichkeitsregelung von § 5 TDG/MDStV auf technische Informationsdurchleitung, weshalb diese Norm insgesamt keine Anwendung auf Links findet, sondern das allgemeine Strafrecht.

gesetzt werden müssen[89], weil es ansonsten gar nichts mehr zum tatbestandsmässigen und rechtswidrigen Handeln eines anderen beizutragen gäbe. Freilich gibt es Dauerdelikte wie die Freiheitsberaubung (Art. 183 StGB) oder den Hausfriedensburch (Art. 186 StGB), bei denen die Tathandlung nicht schon mit der Herbeiführung eines bestimmten rechtswidrigen Zustandes endet, sondern auch die Aufrechterhaltung des Zustandes zur tatbestandsmässigen Handlung gehört. Hier ist es nur folgerichtig, Gehilfenschaft bis zur Beendigung, also bis zur Beseitigung des inkriminierten Zustandes, strafrechtlich zu erfassen. Ähnliches gilt auch für die Delikte mit überschiessender Innentendenz.

Ob etwa die Rassendiskriminierung (Art. 261bis StGB), die Störung der Glaubens- und Kultusfreiheit (Art. 261 StGB), die öffentliche Aufforderung zu Verbrechen oder zur Gewalttätigkeit (Art. 259 StGB) oder die Ehrverletzungsdelikte (Art. 173 ff. StGB) Zustands- oder Dauerdelikte sind, ist im Wege der Auslegung des Tatbestandes zu ermitteln.

Am Beispiel der Rassendiskriminierung: Dass durch die ständige Abrufbarkeit von rassistischen Website-Inhalten das Rechtsgut der Menschenwürde intensiver beeinträchtigt wird, ist unstreitig und legt nahe, Art. 261bis StGB als Dauerdelikt zu erachten[90]. Allerdings sind Lehre und Praxis im analogen Fall der üblen Nachrede (Art. 173 StGB) zum Schluss gekommen, diese sei ein Zustandsdelikt[91]. Auch gehört Art. 261bis StGB als schlichtes Tätigkeitsdelikt, das im Moment der rassendiskriminierenden Handlung oder Äusserung schon vollendet und beendet ist, nicht zu den Absichtsdelikten, bei denen ebenfalls eine von der Vollendung abgrenzbare Beendigung anerkannt wird, die erst beim Erreichen des beabsichtigten Ziels eintritt. Wollte man daher bei Art. 261bis Abs. 1 und 2 StGB von einem Zustandsdelikt ausgehen, hätte dies zur Konsequenz, dass eine Förderung oder Teilnahme gemäss Art. 261bis Abs. 3 nur bis zur Vollendung der Tathandlungen nach Abs. 1 und 2 möglich sein dürfte. Haupttäterschaft der Förderung oder Teilnahme nach Abs. 3 hin oder her: Unter der Prämisse, dass die Aufrechterhaltung der Rechtsgutsbeeinträchtigung bei Art. 261bis Abs. 1 und 2 StGB nicht tatbestandsmässig ist, kann man eine Propagandaaktion nur bis zur Ausführung der Tathandlungen (Aufruf, Verbreiten) fördern oder daran teilnehmen. Damit wäre der später gesetzte Link auf rassistische Website-Inhalte auch keine Förderung oder Teilnahme im Sinne von Art. 261bis Abs. 3

89 Siehe nur REHBERG/DONATSCH, 78, 133f.; STRATENWERTH, AT I, 298f.; TRECHSEL/NOLL, 77f., 212; zur deutschen Lehre JESCHECK/WEIGEND, 692f.; KÜHL, 835; ROXIN, 275.

90 Vgl. die Diskussion im Zusammenhang mit dem intertemporalen Recht bei NIGGLI, Rassendiskriminierung, N1283ff.

91 TRECHSEL, N8 zu Art. 173 StGB.

StGB. Dasselbe gilt für nachträgliche Links auf Web-Publikationen, die den Tatbestand von Art. Art. 261bis Abs. 4 StGB erfüllen[92].

Geht man dagegen davon aus, dass auch die Aufrechterhaltung der Rechtsgutsbeeinträchtigung[93] zum Tatbestand gehört, ist Gehilfenschaft bis zu deren Beseitigung möglich. Der nachträgliche Link kann dann sehr wohl als Förderung des hauptverantwortlichen Anbieters der rassistischen Website angesehen werden, weil die Zugriffswahrscheinlichkeit für die inkriminierten Inhalte erhöht wird.

Diese Interpretation verdient für den Fall eines "dauerhaften" Links den Vorzug, weil der Straftatbestand von Art. 261bis StGB gerade auch einer anhaltenden Verbreitung der Rassendiskriminierung entgegenstehen will, die eine die Menschenwürde weitaus stärker verletzende Langzeitwirkung hat als etwa eine einmalige mündliche Äusserung[94].

Generell ist bei den Gedankenäusserungsdelikten von der starren Zweiteilung in Zustands- und Dauerdelikte abzukommen. Auch die Ehrverletzungsdelikten sind vom Wortlaut her nicht auf eine der beiden Deliktstypen fixiert. Während die herkömmliche mündliche Äusserung mit Ausführung schon als vollendet und beendet zu gelten hat (Zustandsdelikt), hat die Publikation auf einer Webpage eine die Rechtsgutsverletzung perpetuierende Qualität. Immer dann, wenn der Haupttäter eine jederzeitige Kontrolle über die strafbaren Inhalte und die Möglichkeit der Entfernung der bereitgestellten Informationen hat, sollte das Aufrechterhalten des rechtswidrigen Zustandes als Teil des objektiven Tatbestandes angesehen werden (Dauerdelikt), so dass beispielsweise die üble Nachrede auf einer Webpage mit der Veröffentlichung vollendet, aber erst mit der Beseitigung des Textes beendet wäre[95]. Damit wäre eine differenzierte Lösung möglich, die nicht zum vornherein alle Links als straflos erklären muss.

92 Oder auch der üblen Nachrede, Art. 173 StGB, der Störung der Glaubens- und Kultusfreiheit, Art. 261 StGB, der öffentlichen Aufforderung zu Verbrechen oder zur Gewalttätigkeit, Art. 259 StGB, usw.

93 D.h. die Unterlassung der Beseitigung.

94 SCHWARZENEGGER, Gefangen?, 71.

95 Nach FISCHER, in: TRÖNDLE/FISCHER, §184 N13 ist etwa die Verbreitung pornographischer Schriften durch Ausstellen oder Anschlagen als Dauerdelikt aufzufassen (§ 184 Abs. 1 Nr. 2 dStGB).

5. Angriffe auf die E-Commerce-Infrastruktur am Beispiel der Denial of Service Attacken

In den letzten Monaten häuften sich die Meldungen über Hacker-Angriffe auf Webserver und über Datenmanipulationen auf den dort gespeicherten Dokumenten. So werden zeitweise mehr als hundert "gehackte" und veränderte Websites pro Tag gemeldet[96]. Bei dem enormen Schadenspotential, welche solchen Angriffen innewohnt, ist in der E-Commerce-Branche die Prävention vorrangig. Dennoch bedarf es auch einer griffigen strafrechtlichen Erfassung dieser neuen Formen der Netzwerkkriminalität. Unter den seit einiger Zeit diskutierten Erscheinungsformen sind die Denial of Service Angriffe[97] strafrechtlich besonders umstritten.

Fall 8: Anfangs Februar 2000 legten Hacker durch solche "Denial of Service Attacks (DoSA)" die Rechner von eBay.com, Amazon.com, Yahoo!, Buy.com und CNN.com lahm. Dabei wurden Hackerprogramme zunächst auf verschiedenen Server-Rechnern mit Lücken im Sicherheitsdispositiv installiert (Zombies). Von dort riefen diese Programme unter der Identifikationsnummer des Servers zum vorbestimmten Zeitpunkt automatisch riesige Datenmengen von den Zielrechnern ab, bis diese die Datenflut nicht mehr verarbeiten konnten und ausfielen. Die Wirkung wurde dadurch erhöht, dass die Programme falsche Ping-Angaben (Datei mit Web-Adresse) verwendeten. Die Attacke war vergleichbar mit simultanen Anrufen von 104 Mio. Personen auf das gleiche Firmentelephon. Die Hackerprogramme können ausgehend von Servern in ganz verschiedenen Ländern operieren, und dies unabhängig vom Ort, wo der Hacker agiert[98].

Abgesehen von Fragen des Strafanwendungsrechts[99] stellt sich die Frage, ob sich diese Sachverhalte unter einen der bestehenden Straftatbestände subsumieren las-

96 Siehe die Meldung in Tages-Anzeiger, Hacken im Akkord, 30. Mai 2001, 16, unter Hinweis auf www.attrition.org (Stand: 17.7.2001).

97 Zu den verschiedenen Arten von DoS-Attacken KURTZ/MCCLURE/SCAMBRAY, 429ff.

98 Siehe die Meldung in SPIEGEL, 7/2000, 108ff.; eine detaillierte Beschreibung einer DoS-Attacke, die am 4. Mai 2001 startete, bietet GIBSON, The strange tale of the denial of service attacks against grc.com, abrufbar unter http://media.grc.com:8080/files/grcdos.pdf (Stand: 17.7.2001); vgl. auch SCHWARZENEGGER, Geltungsbereich, 110f.; WEBER/UNTERNÄHRER, 375ff. mit strafrechtlicher Würdigung von einfachen und distributed DoSA.

99 Näher dazu unter 2.

sen. In Betracht zu ziehen sind die Datenbeschädigung gemäss Art. 144bis Ziff. 1 Abs. 1 StGB, die Nötigung nach Art. 181 StGB und eventuell die Störung von Betrieben, die der Allgemeinheit dienen, gemäss Art. 239 Ziff. 1 Abs. 1 StGB. Der Tatbestand des unbefugten Eindringens in eine Datenverarbeitungsanlage (Art. 143bis StGB), wie der Hacking-Tatbestand technisch bezeichnet wird, kommt ebenfalls in Frage, aber nur bezüglich der Unterwanderung eines Drittrechners, etwa durch Plazierung eines Trojanischen Pferdes, wodurch der Drittrechner zum Zombie wird und für ferngesteuerte DoS-Attacken eingesetzt werden kann. Im Hinblick auf den Zielrechner geht es aber bei DoS-Attacken gerade nicht um ein Eindringen, sondern um ein Blockieren.

Art. 144bis Ziff. 1 Abs. 1 StGB belegt mit Strafe, wer unbefugt elektronisch oder in vergleichbarer Weise gespeicherte Daten verändert, löscht oder unbrauchbar macht. Dieses Antragsdelikt will folglich die Integrität der Daten schützen, damit der Berechtigte nach seinem Willen darüber verfügen kann. Die einzige Tathandlungsvariante, die auf eine relativ kurze Blockierung eines Rechners eventuell anwendbar wäre, ist das Unbrauchbarmachen der Daten. Hierbei ist zwar in der Lehre anerkannt, dass der Eingriff nicht irreversibel zu sein braucht, doch wird eine Verhinderung des Zugangs während einer "erheblichen Zeitspanne" gefordert[100]. Zu denken sei etwa an Fälle, in denen die Daten zwar noch auf dem Datenträger vorhanden sind, dem Berechtigten aber durch inhaltliche Umgestaltung, Löschung oder Veränderung eines Dateinamens oder eines Passwortes zu einer Datei, die Einfügung einer dem Datenberechtigten nicht bekannten Verschlüsselung oder einer Sperre die Verwendung der Daten verunmöglicht wird. Ein bloss "vorübergehender Erfolg" in diesem Sinne soll genügen[101]. Zweifelhaft bleibt aber, ob damit auch stundenweise Systemblockierungen wie sie DoS-Attacken verursachen, abgedeckt werden. Es fällt auf, dass die eigentlich zutreffende Tathandlungsvariante des "Unterdrückens von Daten", wie sie das deutsche Strafgesetz in § 303 a benennt, in Art. 144bis Ziff. 1 Abs. 1 StGB fehlt. Deshalb wird in Deutschland die Tathandlungsvariante des Unbrauchbarmachens auch viel enger aufgefasst, und zwar als die Beeinträchtigung der Daten in ihrer Gebrauchsfähigkeit, so dass sie ihren Zweck nicht mehr erfüllen können[102]. Auch eine dem deutschen § 303 b dStGB über die Computersabotage entsprechende Norm fehlt im Schweizer StGB. Da solche Straftatbestände bewusst nicht in

100 TRECHSEL, N7 zu Art. 144bis StGB.

101 SCHMID, N29 zu Art. 144bis StGB; siehe auch STRATENWERTH, BT I, 309.

102 FISCHER, in: TRÖNDLE/FISCHER, N7 zu § 303a dStGB; KÜHL, in: LACKNER/KÜHL, N3 zu § 303a dStGB.

das StGB aufgenommen worden sind[103], ist davon auszugehen, dass von der Unbrauchmachung i.S.v. Art. 144bis Ziff. 1 Abs. 1 StGB nur solche Fälle erfasst werden, die von der Eingriffsintensität der Veränderung oder Löschung gleichkommen. Die "erhebliche Zeitspanne" muss daher mindestens in Tagen bemessen sein, was die üblichen DoS-Attacken vom Anwendungsbereich von Art. 144bis Ziff. 1 Abs. 1 StGB ausschliesst[104].

Falls die Host-Provider als *öffentliche Verkehrsanstalten* angesehen werden, wäre eine Strafbarkeit wegen Hinderung, Störung oder Gefährdung deren Betriebes nach Massgabe von Art. 239 Ziff. 1 Abs. 1 StGB möglich, wobei Ziff. 2 dieser Bestimmung selbst fahrlässiges Handeln unter Strafe stellt. Es besteht Unklarheit darüber, welche Tatobjekte in der heutigen, von grossen Veränderungen in der öffentlichen Leistungsverwaltung und einer Privatisierungswelle gekennzeichneten Gesellschaft überhaupt von Art. 239 StGB geschützt werden[105]. In der bisherigen Doktrin wurde vornehmlich auf das Merkmal der Konzessionierung abgestellt, so dass etwa Radio, Fernsehen und Gemeinschaftsantennen (für 13 Gemeinden) sowie Transporteinrichtungen als Verkehrsanstalten gelten[106]. Art. 4 Abs. 1 FMG sieht eine Konzessionspflicht nur für Netzwerk-Provider vor, welche erhebliche Teile der für die Übertragung benutzten Fernmeldeanlagen unabhängig betreiben, während andere Fernmeldedienstleister bloss eine Meldepflicht trifft (Art. 4 Abs. 2 FMG). Aus der bisherigen Rechtsprechung lässt sich ausserdem entnehmen, dass bei Kommunikationsnetzen die Störung eines einzelnen Anschlusses, z.B. die Beschädigung einer einzelnen Telephonkabine, eines Billetautomaten oder Störung des Radio- oder Fernsehempfanges im engeren Umkreis, nicht genügt[107]. Es bedarf also eines erheblichen Angriffes auf die öffentliche Versorgungsfunktion des Betriebes. Da aber das Blockieren eines am Internet angeschlossenen Rechners alleine keine erhebliche Funktionsstörung des Netzes auszulösen vermag, dürften DoS-Attacken gegen einzelne Web-Server regelmässig nicht unter Art. 239 StGB fallen. Anders wäre jedoch zu entscheiden, wenn durch DoS-Angriffe mittels Manipulation der Routing-Informationen (Border Gateway Protocol), die von vielen Backbone-Providern eingesetzt werden, direkt die Einsatzfähigkeit des Netzwerks gestört würde[108].

103 SCHMID, N15 zu Art. 144bis StGB: "geht es ... schlicht um Datenveränderung oder Datenbeschädigung"; siehe auch N31 zu Art. 144bis StGB.

104 Die Strafbarkeit nach Art. 144bis Ziff. 1 Abs. 1 StGB bejahen WEBER/UNTERNÄHRER, 378f., "selbst wenn die Norm nicht gut "passt" ...".

105 STRATENWERTH, BT II, 82f., "nicht ganz einfach".

106 REHBERG, 88; TRECHSEL, N2 zu Art. 239 StGB beide m.N.; vgl. BGE 85 IV 232 "Geschützt ist das öffentliche Interesse an der Benützbarkeit einer für die Allgemeinheit bestimmten Verkehrsanlage ...".

107 TRECHSEL, N5 zu Art. 239 StGB.

Somit bleibt zu prüfen, ob das Überfluten von Rechnern zum Zwecke ihrer Blokkierung einer *Nötigung* (Art. 181 StGB) gleichkommt. Diese ist prima vista die zutreffendere Strafnorm, weil die DoS-Attacke ein Angriff auf die Willensbetätigungsfreiheit der Daten- und Infrastrukturberechtigten ist, müssen diese doch gegen ihren Willen das Betreiben des Rechners und die Verfügung über die Daten unterlassen. Als Nötigungsmittel kommt einzig die Generalklausel "andere Beschränkung der Handlungsfreiheit" in Betracht, von welcher gefordert wird, dass sie das üblicherweise geduldete Mass eindeutig überschreiten muss[109]. Der Zwang kann durch ein beliebiges Mittel ausgeübt werden. Die Praxis bejahte dies etwa bei einer Blockierung des morgendlichen Berufsverkehrs während 10 Min. durch das Fixieren einer geschlossenen Bahnschranke oder bei der Blockade des Schwerverkehrs in Romanshorn[110].

Vollendet ist die Nötigung, wenn die Datenberechtigten das abgenötigte Verhalten an den Tag legen, wobei dies im Falle der DoS-Attacken schon mit dem Unterlassen-Müssen der Nutzung für eine kurze, die sozial übliche Wartezeit überschreitende Zeitspanne eintritt. Die Rechtswidrigkeit bedarf bei der Nötigung einer expliziten Begründung, wobei bei DoS-Angriffen regelmässig der Zweck unrechtmässig sein wird, weil dadurch die freie Willensbetätigung Dritter behindert werden soll. Im Gegensatz zum Grundtatbestand der Datenbeschädigung ist die Nötigung ein Offizialdelikt, was die Strafverfolgungsbehörden zum Einschreiten zwingt, sobald sie von einer DoS-Attacke Kenntnis erlangen.

Resumierend lässt sich feststellen, dass DoS-Angriffe schon nach geltendem Recht als Nötigung i.S.v. Art. 181 StGB strafbar sind. In der Cyber-Crime Convention des Europarates, die in Kürze zur Unterzeichnung aufgelegt werden soll, ist in Artikel 5 ein spezieller Tatbestand der "System Interference" vorgesehen. Mit der Ratifikation dieser Konvention müssen die Mitgliedsstaaten eine entsprechende explizite Strafnorm in ihre nationalen Strafgesetze aufnehmen, so dass in den nächsten Jahren mit einer weltweiten Harmonisierung der materiell-strafrechtlichen Grundlagen zur Bekämpfung der DoS-Attacken gerechnet werden kann.

108 Vgl. zu solchen DoS-Attacken KURTZ/MCCLURE/SCAMBRAY, 446.

109 Vgl. statt aller TRECHSEL, N7 zu Art. 181 StGB.

110 BGE 119 IV 306; TRECHSEL, N7 zu Art. 181 StGB mit anderen Beispielen aus der Praxis.

6. Harmonisierung und Zusammenarbeit auf europäischer und internationaler Ebene

Die technische und wirtschaftliche Globalisierung lässt sich nicht aufhalten. Mit ihr schwindet die Durchsetzungsmacht des Nationalstaates, dies insbesondere im Bereiche der Internetkriminalität. Neben den schon erwähnten Revisionsbestrebungen in der Schweiz ist eine klare internationale Abgrenzung der Strafanwendungsrechte, ein effizientes Auslieferungs- und Rechtshilferecht, sowie eine Harmonisierung der materiellrechtlichen Strafnormen anzustreben. Diese Themen stehen nunmehr auf der Agenda mehrerer internationaler Organisationen und Regierungstreffen (G-8, OECD, UNESCO, EU, Europarat).

Der *Europarat* ist beispielsweise daran, in enger Zusammenarbeit mit den USA, Kanada, Japan und Australiens eine Cyber-Crime Convention vorzulegen, die vor allem im Bereich der Computerdelikte und bezüglich der Kinderpornographie eine materiell-rechtliche Harmonisierung bringen wird. Auch strafprozessuale Massnahmen zur Beweisermittlung und –sicherung sind in diesem Konventionsentwurf enthalten[111].

Auch die *Europäische Union* hat ein ganzes Massnahmenpaket zur Bekämpfung der Internetkriminalität geschnürt. Als erste Massnahme soll in allen Mitgliedstaaten mit wirksamen Sanktionen gegen die Kinderpornographie im Internet vorgegangen werden. Langfristig beabsichtigt die Europäische Kommission Gesetzesvorschläge zur weiteren Angleichung der materiellen Strafrechtsvorschriften für den Bereich der High-Tech-Kriminalität vorzulegen. In Übereinstimmung mit den Schlussfolgerungen des Europäischen Rats von Tampere vom Oktober 1999 prüft die Kommission zudem, inwieweit die im Rahmen von Ermittlungsverfahren gegen Internetdelikte ergangenen Anordnungen gegenseitige anerkannt werden könnten. Parallel dazu beabsichtigt die Kommission, darauf hinzuwirken, dass in den Ländern, in denen noch keine spezialisierten Polizeidienste bestehen, derartige Internet-Police-Einheiten auf nationaler Ebene eingerichtet werden. Vorgesehen sind ausserdem Förderungsprogramme für geeignete Schulungsmassnahmen für Strafverfolgungsbeamte und europaweite Aktionen zum Thema der Informationssicherheit. Auf technischer Ebene wird die Kommission in Übereinstimmung mit dem rechtlichen Rahmen Massnahmen zur Sensibilisierung von Forschern und Entwicklern sowie zur Verbreitung von Fachwissen ergreifen, um die Anfälligkeit der neuen Technologien

111 Zum Text und einem erläuternden Bericht, siehe Conseil de l'Europe, Projet de convention sur la cyber-criminalité (Projet N° 27 rev.), 25 mai 2001, abrufbar unter http://conventions.coe.int/treaty/fr/projets/cybercrime27.htm (Stand: 17.7.2001).

gegenüber der Computerkriminalität zu mindern. Die Kommission hat bereits ein EU-Forum geschaffen, welches die Strafverfolgungsbehörden, die Internet-Service-Provider, die Telekommunikationsbetreiber, Bürgerrechtsorganisationen, die Vertreter der Konsumenten und der Datenschutzbehörden sowie andere interessierte Parteien zusammenzubringen soll, um den Meinungsaustausch und die Zusammenarbeit auf europäischer Ebene zu fördern. Ziel des Forums wird es auch sein, das öffentliche Bewusstsein für die Gefährdung durch über das Internet begangene Straftaten zu schärfen, optimale Sicherheitsbedingungen zu schaffen, Instrumente und Verfahren für eine wirksame Bekämpfung der Computerkriminalität aufzuzeigen und die Weiterentwicklung von Frühwarnsystemen und Mechanismen der Krisenbewältigung anzuregen[112]. Eine Einbindung der Schweizer Behörden und Betroffenen in diesen internationalen Informationsaustausch und Harmonisierungsprozess ist dringend angezeigt.

112 Die entsprechende Mitteilung der Kommission kann abgerufen werden unter: http://europa.eu.int/ISPO/eif/InternetPoliciesSite/Crime/CrimeComEN.pdf (Stand: 17.7.2001).

Literaturverzeichnis

ARZT, Gunther: Erfolgsdelikt und Tätigkeitsdelikt, ZStrR 1990, 168ff.

BARTON, Dirk-M.: Multimedia-Strafrecht. Ein Handbuch für die Praxis, Neuwied/Kriftel 1999.

BOESE, Oliver: Strafrechtliche Verantwortlichkeit für Verweisungen durch Links im Internet, Frankfurt am Main 2000.

BREMER, Karsten: Strafbare Internet-Inhalte in internationaler Hinsicht. Ist der Nationalstaat wirklich überholt?, Frankfurt am Main 2000.

BUNDESAMT FÜR JUSTIZ: Frage der strafrechtlichen Verantwortlichkeit von Internet-Access-Providern gemäss Art. 27 und 322bis StGB. Gutachten vom 24. Dezember 1999, VPB 2000 III, 820ff., abrufbar unter www.bj.admin.ch/themen/ri-ir/access/ga-acc-prov.pdf (Stand: 17.7.2001).

BURKE, Lynn: Love bug case dead in Manila, Wired, 21/8/2000, abrufbar unter www.wired.com/news/politics/0,1283,38342,00.html (Stand: 17.7.2001).

CASSANI, Ursula: Die Anwendbarkeit des schweizerischen Strafrechts auf internationale Wirtschaftsdelikte (Art. 3–7 StGB), ZStrR 1996, 237ff.

COPPEL, Jonathan: E-Commerce: Impacts and policy challenges, OECD Economics Department Working Papers No. 252, Paris 2000.

CORNILS, Karin: Der Begehungsort von Äusserungsdelikten im Internet, JZ 1999, 394ff.

COUNCIL OF EUROPE, European Committee on Crime Problems: Extraterritorial criminal jurisdiction, Criminal Law Forum 1992, 441ff.

DÖRING, Nicola: Sozialpsychologie des Internet. Die Bedeutung des Internet für Kommunikationsprozesse, Identitäten, soziale Beziehungen und Gruppen, Göttingen 1999.

EIDGENÖSSISCHES JUSTIZ- UND POLIZEIDEPARTEMENT: Begleitbericht zum Vorentwurf für eine Schweizerischen Strafprozessordnung, Bern 2001.

FIOLKA, Gerhard/NIGGLI, Marcel Alexander: Das Private und das Politische. Der Begriff der Öffentlichkeit im Strafrecht am Beispiel der Bundesgerichtsentscheide vom 21. Juni 2000 und vom 23. August 2000 betreffend Rassendiskriminierung, AJP 2001, 533ff.

FORSTER, Marc: Der Wirtschaftsalltag als strafrechtsdogmatischer «Hort des Verbrechens», Zum «zielobjektivierten Beihilfetatbestand» bei sogenannten Alltagsgeschäften und berufstypischen Dienstleistungen, in: ACKERMANN, Jürg-Beat/DONATSCH, Andreas/REHBERG, Jörg (Hrsg.): Wirtschaft und Strafrecht. Festschrift für Niklaus Schmid, Zürich 2001, 127ff.

GERMANN, Michael: Gefahrenabwehr und Strafverfolgung im Internet, Berlin 2000.

HAFT, Fritjof/EISELE, Jörg: Zur systematischen Stellung des § 5 TDG bei der Prüfung der strafrechtlichen Verantwortlichkeit von Internet-Providern, in: WIEBE, Andreas (Hrsg.): Regulierung in Datennetzen, Darmstadt 2000, 53ff.

HEINRICH, Bernd: Der Erfolgsort beim abstrakten Gefährdungsdelikt, GA 1999, 72ff.

HILGENDORF, Eric: Überlegungen zur strafrechtlichen Interpretation des Ubiquitätsprinzips im Zeitalter des Internet, NJW 1997, 1873ff.

JESCHECK, Hans-Heinrich/WEIGEND, Thomas: Lehrbuch des Strafrechts. Allgemeiner Teil, 5. Aufl., Berlin 1996.

KPMG: 2001 global e.fr@ud.survey, o.O. 2001, abrufbar unter www.kpmg.de/library/surveys/ (Stand: 17.7.2001).

KPMG (efr@ud): efr@ud.survey. Umfrage zur Wirtschaftskriminalität im eCommerce, o.O. 2001, abrufbar unter www.kpmg.de/library/surveys/ (Stand: 17.7.2001).

KÜHL, Kristian: Strafrecht, Allgemeiner Teil, 3. Aufl., München 2000.

KURTZ, George/MCCLURE, Stuart/SCAMBRAY, Joel: Das Anti-Hacker-Buch, Bonn 2000.

LACKNER, Karl/KÜHL, Kristian: Strafgesetzbuch mit Erläuterungen, 23. Aufl., München 1999.

LEHLE, Thomas: Der Erfolgsbegriff und die deutsche Strafrechtszuständigkeit im Internet, Konstanz 1999.

NIGGLI, Marcel Alexander (Rassendiskriminierung): Rassendiskriminierung. Ein Kommentar zu Art. 261bis StGB und Art. 171c MStG, Zürich 1996.

NIGGLI, Marcel Alexander (Klassische Teilnahme): Klassische Teilnahme (Gehilfenschaft), in: NIGGLI, Marcel Alexander/RIKLIN, Franz/STRATENWERTH, Günter (Hrsg.): Die strafrechtliche Verantwortlichkeit von Internet-Providern, medialex Sonderausgabe 2000, 22ff.

NIGGLI, Marcel Alexander (Fehlende Rechtssicherheit): Fehlende Rechtssicherheit bei der Bekämpfung illegaler Inhalte, Strittige strafrechtliche Verantwortung von Internet-Service-Providern, NZZ 29. Mai 2001, B 15.

NIGGLI, Marcel Alexander/RIKLIN, Franz/STRATENWERTH, Günter: Die strafrechtliche Verantwortlichkeit von Internet-Providern, medialex Sonderausgabe 2000, abrufbar unter www.vit.ch/gutachten_isp.pdf (Stand: 17.7.2001).

NIGGLI, Marcel Alexander/SCHWARZENEGGER, Christian: Vorschlag für eine Gesetzesrevision im Bereich der Netzwerkkriminalität, Murten/Zürich 2000.

REHBERG, Jörg: Strafrecht IV, Delikte gegen die Allgemeinheit, 2. Aufl., Zürich 1996.

REHBERG, Jörg/DONATSCH, Andreas: Strafrecht I, Verbrechenslehre, 7. Aufl., Zürich 2001.

RIKLIN, Franz: Information Highway und Strafrecht, in: HILTY, Reto M. (Hrsg.): Information Highway, Beiträge zu rechtlichen und tatsächlichen Fragen, Bern/München 1996, 559ff.

RIKLIN, Franz/STRATENWERTH, Günter: Medienstrafrecht/Kaskadenhaftung, in: NIGGLI, Marcel Alexander/RIKLIN, Franz/STRATENWERTH, Günter (Hrsg.): Die strafrechtliche Verantwortlichkeit von Internet-Providern, medialex Sonderausgabe 2000, 8ff.

ROXIN, Claus: Strafrecht. Allgemeiner Teil, Band I, Grundlagen, Aufbau der Verbrechenslehre, 3. Aufl., München 1997.

SCHMID, Niklaus: Computer- sowie Check- und Kreditkarten-Kriminalität. Ein Kommentar zu den neuen Straftatbeständen des schweizerischen Strafgesetzbuches, Zürich 1994.

SCHLEIMINGER, Dorrit/METTLER, Christoph: Strafbarkeit der Medienverantwortlichen im Falle der Rassendiskriminierung. Art. 27, Art. 261bis Abs. 4 StGB, Bemerkungen zu BGE 125 IV 206 ff., AJP 2000, 1039ff.

SCHÖNKE, Adolf/SCHRÖDER, Horst: Strafgesetzbuch, Kommentar, 26. Aufl., München 2001.

SCHULTZ, Hans (Geltung): Die räumliche Geltung des schweizerischen Strafgesetzbuches nach der neueren Gerichtspraxis, ZStrR 1957, 306ff.

SCHULTZ, Hans (Neue Probleme): Neue Probleme des internationalen Strafrechts und des Auslieferungsrechtes, SJZ 1964, 81ff.

SCHULTZ, Hans (Unerlaubte Veröffentlichung): Die unerlaubte Veröffentlichung – ein Pressedelikt, ZStrR 1991, 273ff.

SCHWARZENEGGER, Christian (Geltungsbereich): Der räumliche Geltungsbereich des Strafrechts im Internet. Die Verfolgung von grenzüberschreitender Internetkriminalität in der Schweiz im Vergleich mit Deutschland und Österreich, ZStrR 2000, 109ff.

SCHWARZENEGGER, Christian (Gefangen?): Gefangen im Spinnennetz der Strafjustiz? Die strafrechtliche Bewertung von Links, NZZ 30. Juni 2000, 71.

SCHWARZENEGGER, Christian (Abstrakte Gefahr): Abstrakte Gefahr als Erfolg im Strafanwendungsrecht - Ein leading case zu grenzüberschreitenden Internetdelikten. Zum Urteil des BGH vom 12. Dezember 2000 – 1 StR 184/00, sic! 2001, 240ff.

SCHWARZENEGGER, Christian (Handlungs- und Erfolgsort): Handlungs- und Erfolgsort beim grenzüberschreitenden Betrug, in: ACKERMANN, Jürg-Beat/DONATSCH, Andreas/REHBERG, Jörg (Hrsg.): Wirtschaft und Strafrecht. Festschrift für Niklaus Schmid, Zürich 2001, 143ff.

SCHWARZENEGGER, Christian (StGB): Schweizerisches Strafgesetzbuch, mit Verordnungen zum StGB und den Texten der hängigen StGB-Revisionsvorhaben, Zürich 2001.

SIEBER, Ulrich: Internationales Strafrecht im Internet. Das Territorialitätsprinzip der §§ 3, 9 StGB im globalen Cyberspace, NJW 1999, 2065ff.

SPINDLER, Gerald: Haftungsrecht, in: HOEREN, Thomas/SIEBER, Ulrich (Hrsg.): Handbuch Multimedia-Recht, Rechtsfragen des elektronischen Geschäftsverkehrs (Loseblatt), München 2000, 29ff.

STRATENWERTH, Günter (BT I): Schweizerisches Strafrecht, Besonderer Teil I: Straftaten gegen Individualinteressen, 5. Aufl., Bern 1995.

STRATENWERTH, Günter (AT I): Schweizerisches Strafrecht, Allgemeiner Teil I: Die Straftat, 2. Aufl., Bern 1996.

STRATENWERTH, Günter (BT II): Schweizerisches Strafrecht, Besonderer Teil II: Straftaten gegen Gemeininteressen, 5. Aufl., Bern 2000.

TRECHSEL, Stefan: Schweizerisches Strafgesetzbuch, Kurzkommentar, 2. Aufl., Zürich 1997.

TRECHSEL, Stefan/NOLL, Peter: Schweizerisches Strafrecht, Allgemeiner Teil I, Allgemeine Voraussetzungen der Strafbarkeit, 5. Aufl., Zürich 1998.

TRÖNDLE, Herbert/FISCHER, Thomas: Strafgesetzbuch und Nebengesetze, 50. Aufl., München 2001.

WEBER, Rolf H.: E-Commerce und Recht. Rechtliche Rahmenbedingungen elektronischer Geschäftsformen. Zürich 2001.

WEBER, Rolf H./UNTERNÄHRER, Roland: Wirtschaftsterrorismus im Internet, in: ACKERMANN, Jürg-Beat/DONATSCH, Andreas/REHBERG, Jörg (Hrsg.): Wirtschaft und Strafrecht. Festschrift für Niklaus Schmid, Zürich 2001, 365ff.

WIDMER, Ursula/BÄHLER, Konrad: Rechtsfragen beim Electronic Commerce. Sichere Geschäftstransaktionen im Internet, 2. Aufl., Zürich 2000.

WOHLERS, Wolfgang: Gehilfenschaft durch «neutrale» Handlungen. Ausschluss strafrechtlicher Verantwortlichkeit bei alltäglichem bzw. berufstypischem Verhalten?, ZStrR 1999, 425ff.

ZÜRCHER, Emil: Schweizerisches Strafgesetzbuch. Erläuterungen zum Vorentwurf vom April 1908, Bern 1914.