

Internetstrafrecht in Deutschland¹

Dr. Brian Valerius²

A. Einleitung

Internetstrafrecht in Deutschland. Ein sehr weites Feld, das im Rahmen eines kurzen Vortrags allenfalls abgesteckt, keineswegs aber auch nur annähernd zufriedenstellend bearbeitet werden kann. Die Zeit reicht immerhin für einen kleinen Überblick, der jedoch nur ein sehr oberflächlicher bleiben können wird. Ein Überblick über das, was bisher war, was derzeit ist und was eventuell bald sein wird, illustriert anhand markanter, zum Teil einschneidender Beispiele aus der Rechtssetzung sowie aus der Rechtsanwendung.

Dass sich eine nähere Beschäftigung mit der Materie lohnt, lässt sich an der rechtswissenschaftlichen Rezeption des Internetstrafrechts hierzulande ablesen. So werden mindestens drei etablierte Fachzeitschriften zur Thematik – freilich unter Einschluss zivil- und öffentlich-rechtlicher Aspekte des Internets – herausgegeben,³ hinzu kommen zumindest zwei reine Online - Zeitschriften.⁴ Seit mehreren Jahren schon vermehren sich die Lehrstühle, deren Inhaber eine Lehrbefugnis speziell zum Internet-, Medien- oder Informationsstrafrecht vorweisen können. Endgültig dürfte das Internetstrafrecht zur eigenen Subdisziplin der Strafrechtswissenschaft im Jahre 2005 aufgestiegen sein, als drei Lehrbücher zugleich zu diesem Thema veröffentlicht wurden.⁵

¹ Der Beitrag stellt eine mit Anmerkungen versehene Fassung des gleichnamigen Vortrags vom 1. September 2007 auf der deutsch-türkischen Tagung „Das Strafrecht im deutsch-türkischen Rechtsvergleich“ dar. Die Vortragsform wurde beibehalten.

² Der Verfasser ist Wissenschaftlicher Mitarbeiter am Lehrstuhl für Strafrecht, Strafprozessrecht, Rechtstheorie, Informationsrecht und Rechtsinformatik (Prof. Dr. Dr. Eric Hilgendorf) an der Universität Würzburg.

³ Dabei handelt es sich um die Zeitschriften „Computer und Recht“, gestartet bereits 1985, die „Multimedia und Recht“ seit dem Jahre 1998 sowie die ein Jahr später erstmals veröffentlichte „Kommunikation & Recht“.

⁴ „JurPC“ (1989) sowie „Medien Internet und Recht“ (November 2005).

⁵ *Hilgendorf/Frank/Valerius*, Computer- und Internetstrafrecht. Ein Grundriss, Berlin/Heidelberg 2005; *Malek*, Strafsachen im Internet, Heidelberg 2005; *Marberth-Kubicki*, Computer- und Internetstrafrecht, München 2005.

B. Internetstrafrecht in der Gesetzgebung

I. Zweites Gesetz zur Bekämpfung der Wirtschaftskriminalität (2. WiKG) vom 15. Mai 1986

Die heutige Bedeutung und Eigenständigkeit des Internetstrafrechts ist zu einem nicht unerheblichen Maße den gesetzgeberischen Aktivitäten zu verdanken. Den Anfang machte das Zweite Gesetz zur Bekämpfung der Wirtschaftskriminalität (2. WiKG) vom 15. Mai 1986,⁶ das unter anderem erste spezielle computerstrafrechtliche Regelungen mit sich brachte. So wurden das Ausspähen von Daten im gleichnamigen § 202a dStGB sowie die Datenveränderung und die Computersabotage in den §§ 303a, 303b dStGB unter Strafe gestellt. Damit sollten – damals noch konzentriert auf den Schutz der Datenverarbeitung in Wirtschaft und Verwaltung – störende Eingriffe und Sabotageakte gegen Datenträger und Datenverarbeitungsanlagen bekämpft werden.

Zunehmend wurden Datenverarbeitungsanlagen auch zu Angriffen auf das Vermögen missbraucht. Um hier vor neuen elektronischen und computergestützten Angriffsformen zu schützen und damit einhergehende Strafbarkeitslücken zu beseitigen, wurde der Straftatbestand des Computerbetrugs (§ 263a dStGB) eingefügt sowie das Urkundsstrafrecht geändert bzw. erweitert (§§ 269, 270 dStGB: Fälschung beweisheblicher Daten; Täuschung im Rechtsverkehr bei Datenverarbeitung). Abgesehen vielleicht von den letztgenannten Urkundsdelikten ist die Bedeutung der 1986 neu eingeführten Normen des Kernstrafrechts stetig gestiegen und vermag zum Teil auch neue, zum damaligen Zeitpunkt noch gar nicht absehbare kriminelle Erscheinungsformen im Internet wie z.B. das Verwenden gehishter Daten bereits zu erfassen.

II. Informations- und Kommunikationsdienste-Gesetz (IuKDG) vom 22. Juli 1997

Speziell mit den Herausforderungen der modernen Informations- und Kommunikationstechnologie, vornehmlich dem Internet, beschäftigte sich sodann das Informations- und Kommunikationsdienste-Gesetz (IuKDG) vom 22. Juli 1997.⁷ Im Strafgesetzbuch selbst brachte es nur geringfügige Änderungen mit sich. So wurde die Besitzverschaffung bzw. der Besitz von kinderpornographischen Schriften auf Darstellungen wirklichkeitsnaher Geschehen erweitert. Damit sollte zunehmenden Beweisschwierigkeiten begegnet werden, da bei digital überarbeiteten Dateien kaum

⁶ BGBl. I, S. 721; allgemein zum 2. WiKG *Hilgendorf/Frank/Valerius*, in: Vormbaum/Welp (Hg.), Das Strafgesetzbuch, S. 258, 294 ff.; *Haft*, NStZ 1987, 6; *Lenckner/Winkelbauer*, CR 1986, 483; 654; 824; *Möhrenschlager*, wistra 1986, 128.

⁷ BGBl. I, S. 1870; allgemein zum IuKDG *Engel-Flechsigt/Maennel/Tettenborn*, NJW 1997, 2981; *Gounalakis/Rhode*, K&R 1998, 321; *Rofnagel*, NVwZ 1998, 1.

noch zwischen realem und fiktivem Ursprung unterschieden werden kann.⁸ Zudem wurde der Schriftenbegriff des Allgemeinen Teils als Tribut an die zunehmende Digitalisierung von Informationen um die Variante des Datenträgers (z.B. in Gestalt von Festplatten, CD-ROMs, USB-Sticks etc.) ergänzt, damit rechtswidrige Inhalte auch dann strafbar bleiben, wenn sie in digitalisierter, also unkörperlicher Form verbreitet werden.⁹

Ungleich wichtiger war aber eine andere Neuerung, die das Informations- und Kommunikationsdienste-Gesetz mit sich brachte. In der neu eingeführten Vorschrift des § 5 des Teledienstegesetzes (TDG) wurde in Deutschland erstmalig die Haftung der Internetprovider geregelt.¹⁰ Dabei handelte es sich um eine Querschnittsregelung, also eine Regelung, die nicht nur das Strafrecht, sondern sämtliche Rechtsgebiete betrifft. Dies entsprach dem Geiste des Informations- und Kommunikationsdienste-Gesetzes, das die Rahmenbedingungen für Informations- und Kommunikationsdienste generell regeln sollte und sich daher auf zahlreiche Rechtsgebiete auswirkte. Die Providerhaftung widmete sich dabei der zentralen Frage, inwieweit die Anbieter von Dienstleistungen im Internet für rechtswidrige Inhalte zur Verantwortung gezogen werden können. Hintergrund war, dass sich das Internet nur deswegen so rasch hatte ausbreiten und zum alltäglichen Kommunikationsmittel aufsteigen können, weil kommerzielle Unternehmen die notwendige Infrastruktur geschaffen und die einzelnen Nutzungsmöglichkeiten – seien es Webseiten, E-Mails, Nachrichtenforen oder IRC – erweitert bzw. allgemein zugänglich gemacht haben. Heutzutage sind daher bei fast jeder Datenübertragung im Internet ein oder mehrere Provider beteiligt, sei es, dass sie einem den Zugang zum Internet verschaffen, dass sie Speicherplatz für Webseiten oder Leitungen zur Datenübertragung zur Verfügung stellen.

Nun ist das Internet alles andere als ein Raum, der frei von rechtswidrigen, mitunter strafbaren Inhalten wäre. So kann sich jeder halbwegs versierte Nutzer binnen kurzer Zeit Zugriff verschaffen auf Foren mit beleidigenden Äußerungen, auf rechtsextremistische Webseiten mit rassistischem, volksverhetzendem Inhalt oder auch auf kinderpornographische Bild- und Videodateien. Ohne Provider wären weder der Abruf noch die Verbreitung solcher rechtswidriger Inhalte möglich, so dass sich die Frage nach ihrer Verantwortung stellt. Die Brisanz des Themas kann an dem

⁸ BT-Drs. 13/7385, S. 60; 13/7934, S. 41.

⁹ BT-Drs. 13/7385, S. 36.

¹⁰ Allgemein zur Providerhaftung *Hilgendorf/Frank/Valerius* (Fn. 5), Rn. 274 ff.; *Valerius* in: BeckOK-StGB, 8. Edition 2009, Lexikon des Strafrechts: Providerhaftung; eingehend *Kessler*, Zur strafrechtlichen Verantwortlichkeit von Zugangs Providern, Berlin 2003.

international beachteten Urteil im Fall „CompuServe“ verdeutlicht werden, auf den noch zurückzukommen sein wird.¹¹

Die Regelung in § 5 TDG (nunmehr §§ 7 ff. TMG) bestimmte, dass in erster Linie den Anbieter des rechtswidrigen Inhalts (sog. Content-Provider), bei Veröffentlichungen auf Webseiten also z.B. deren Betreiber, die volle Verantwortung trifft. Alle anderen Provider hingegen, die etwa lediglich den Zugang zum Internet ermöglichen (sog. Access-Provider) oder den Speicherplatz für rechtswidrige Inhalte anbieten (sog. Host-Service-Provider), haften nur unter bestimmten, nach ihrer Einflussmöglichkeit auf die fraglichen Inhalte abgestuften Voraussetzungen. Dieses abgestufte Haftungsmodell besteht auch heute noch fort; Einzelfragen wie z.B. die Haftung für Hyperlinks auf Webseiten oder die Haftung für Suchmaschinen sind jedoch nach wie vor ungeklärt – und das trotz oder auch wegen zweier zwischenzeitlicher Änderungen der Verantwortlichkeitsregeln.¹²

III. Weitere Gesetzesänderungen

Neben diesen beiden wesentlichen Gesetzesänderungen gab es Ende 2003 noch kleinere Anpassungen im Computer- und Internetstrafrecht, mit denen der Gesetzgeber auf neue technische Errungenschaften und die fortschreitende Digitalisierung reagierte. Unter anderem wurde durch das Sexualdelikteänderungsgesetz vom 27. Dezember 2003¹³ der – neu nummerierte – § 184c dStGB (Verbreitung pornographischer Darbietungen durch Rundfunk, Medien- oder Teledienste; inzwischen § 184d dStGB) erweitert, wonach nunmehr nicht nur die Verbreitung pornographischer Live-Darstellungen im Rundfunk, d.h. im Hörfunk und Fernsehen, sondern auch in Medien- und Telediensten wie z.B. dem Internet erfasst werden konnte.

Wenige Tage zuvor fügte das 35. Strafrechtsänderungsgesetz vom 22. Dezember 2003 in die Vorschrift des § 263a dStGB zum Computerbetrug die Absätze 3 und 4 ein,¹⁴ womit bestimmte Tathandlungen in Verbindung mit Computerprogrammen

¹¹ Siehe unten C. I.

¹² Gesetz über rechtliche Rahmenbedingungen für den elektronischen Geschäftsverkehr (Elektronischer Geschäftsverkehr-Gesetz; EGG) vom 20. Dezember 2001 (BGBl. I, S. 3721) sowie das Gesetz zur Vereinheitlichung von Vorschriften über bestimmte elektronische Informations- und Kommunikationsdienste (Elektronischer-Geschäftsverkehr-Vereinheitlichungsgesetz; ElGvG) vom 26. Februar 2007 (BGBl. I, S. 179). Vgl. dazu auch unten II. 5. b) a.E.

¹³ Gesetz zur Änderung der Vorschriften über die Straftaten gegen die sexuelle Selbstbestimmung und zur Änderung anderer Vorschriften (BGBl. I, S. 3007).

¹⁴ 35. Strafrechtsänderungsgesetz zur Umsetzung des Rahmenbeschlusses des Rates der Europäischen Union vom 28. Mai 2001 zur Bekämpfung von Betrug und Fälschung im Zusammenhang mit unbaren Zahlungsmitteln (35. StrÄndG; BGBl. I, S. 2838).

sanktioniert werden, sofern sie einen Computerbetrug vorbereiten. Mit der Ausdehnung der Strafbarkeit auf gewisse Vorbereitungshandlungen setzte der Gesetzgeber die Vorgaben eines Rahmenbeschlusses des Rates der Europäischen Union¹⁵ in nationales Recht um.

*IV. 41. Strafrechtsänderungsgesetz zur Bekämpfung
der Computerkriminalität (41. StrÄndG) vom 7. August 2007*

Umfassendere Umgestaltungen brachte wiederum das erst heute vor drei Wochen in Kraft getretene 41. Strafrechtsänderungsgesetz vom 7. August 2007 zur Bekämpfung der Computerkriminalität¹⁶ mit sich, das ebenfalls einen europäischen Hintergrund aufzuweisen hat. Durch die Revision der bestehenden Vorschriften zum Computer- und Internetstrafrecht sollten bestehende Strafbarkeitslücken geschlossen werden, welche die rasanten Fortschritte im Bereich der Informationstechnologie offenbarten und bereits zum Gegenstand europäischer Dokumente erhoben wurden, namentlich dem Übereinkommen des Europarates zur Datennetzkriminalität vom 23. November 2001 (Convention on Cybercrime)¹⁷ sowie dem am 24. Februar 2005 verabschiedeten Rahmenbeschluss des Rates der Europäischen Union über Angriffe auf Informationssysteme.¹⁸

Im deutschen Strafrecht führten die europäischen Vorgaben insbesondere zu Änderungen der Vorschriften über das Ausspähen von Daten (§ 202a dStGB) und die Computersabotage (§ 303b dStGB) sowie zu dem neuen Straftatbestand über das Abfangen von Daten (§ 202b dStGB). Außerdem wurden zahlreiche Vorbereitungshandlungen inkriminiert, im Einzelnen zum Abfangen und Ausspähen (§ 202c dStGB), zur Veränderung von Daten (§ 303a Abs. 3 dStGB) sowie zur Computersabotage (§ 303b Abs. 5 dStGB).

Die vorgenommenen Änderungen haben unter anderem einen größeren Schutz der elektronischen Kommunikation zur Folge. So schützt der neue Straftatbestand über das Abfangen von Daten vor jeglichem Einblick in elektronische Datenübertragungen, z.B. bei dem Versand von E-Mails, Gesprächen mittels der Voice-IP-Technologie oder auch nur bei dem simplen Austausch beliebiger Dateien. Dieser Schutz gilt unabhängig

¹⁵ Vgl. Art. 3 und 4 des Rahmenbeschlusses des Rates der Europäischen Union vom 28. Mai 2001 zur Bekämpfung von Betrug und Fälschung im Zusammenhang mit unbaren Zahlungsmitteln (ABl. EG Nr. L 149 vom 2. Juni 2001, S. 1).

¹⁶ BGBl. I, S. 1786.

¹⁷ SEV Nr. 185.

¹⁸ ABl. EU Nr. L 69 vom 16. März 2005, S. 67.

davon, ob die transferierten Daten gegen unberechtigten Zugang besonders gesichert sind oder nicht. Insbesondere das Abfangen von Daten in ungeschützten WLAN-Netzen ist demnach nunmehr strafbar.

Des Weiteren sind durch die Erweiterung des Straftatbestandes der Computersabotage in § 303b dStGB auch Denial of Service-Angriffe eindeutig erfasst.¹⁹ Über ihre Strafbarkeit bestand zuvor Streit, nicht unwesentlich hervorgerufen durch eine recht junge, später noch zu erörternde Entscheidung des OLG Frankfurt am Main.²⁰

Letztlich wurde nach kontroversen Diskussionen auch das sogenannte Hacking, d.h. das bloße Verschaffen eines Zugangs zu Daten (z.B. durch das Knacken eines Passworts) unter Strafe gestellt. Hintergrund war, dass Hacking-Angriffe in letzter Zeit sowohl in ihrer Anzahl als auch in der Raffiniertheit ihrer Durchführung (z.B. durch Schnüffelsoftware, Key-Logging-Trojaner u.ä.) zugenommen hatten.²¹ Beibehalten wurde indes das Erfordernis, dass die Daten gegen unberechtigten Zugang besonders gesichert sein müssen. Die Überwindung einer solchen besonderen Zugangssperre manifestiert zugleich die strafwürdige kriminelle Energie des Täters.²²

V. Zusammenfassung

Blickt man auf die bisherigen Gesetzgebungsakte im Computer- und Internetstrafrecht zurück, so lässt sich dem Gesetzgeber insgesamt eine recht gute Arbeit bescheinigen. Hervorzuheben ist insbesondere das 2. WiKG, mit dem sich der Gesetzgeber – bei aller berechtigten Einzelkritik an dem Gesetz – beeindruckend frühzeitig mit der Materie des Computerstrafrechts beschäftigte. Dass die damaligen Regelungen gleichwohl eine gewisse Zukunftssicherheit aufwiesen, wird nicht nur daran deutlich, dass sich zahlreiche kriminelle Erscheinungsformen des Internets dadurch erfassen ließen, sondern auch daran, dass sich internationale Regelungen wie z.B. die bereits erwähnte Convention on Cybercrime des Europarates nicht unerheblich an der deutschen Gesetzgebung orientiert haben.

¹⁹ Vgl. BT-Drs. 16/3656, S. 13.

²⁰ Siehe unten C. IV.

²¹ Vgl. BT-Drs. 16/3656, S. 9.

²² BT-Drs. 16/3656, S. 10.

1. Ausweitung der Strafbarkeit im Internet

Allerdings werfen die jüngsten Gesetzgebungsakte auf dem Gebiet des Computer- und Internetstrafrechts zunehmend Fragen und Bedenken auf, wie sich exemplarisch an dem 41. Strafrechtsänderungsgesetz vom 7. August dieses Jahres illustrieren lässt. So ist insbesondere zu beobachten, dass der Gesetzgeber die Strafbarkeit zunehmend ausweitet. Damit ist nicht die notwendige Einführung neuer Straftatbestände gemeint, um die durch Errungenschaften des Fortschritts entstandenen Strafbarkeitslücken zu schließen, sondern die erhebliche Ausdehnung des Anwendungsbereichs der Strafvorschriften auch auf Vorbereitungshandlungen (z.B. die Programmierung von Software, deren Zweck die Begehung einer Straftat ist). Ein weiterer Beleg für diese Tendenz im Computer- und Internetstrafrecht ist die Regelung der (über das Strafrecht freilich hinausreichenden) Providerhaftung.

Die Providerhaftung stellt zwar an sich eine Verantwortlichkeitsbeschränkung dar. Von Nöten ist sie allerdings nur infolge eines weitreichenden, im Computer- und Internetbereich mittlerweile für selbstverständlich gehaltenen Verantwortungsverständnisses: Da sich der unmittelbar Verantwortliche für die Begehung strafwürdigen Unrechts (also z.B. derjenige, der rechtswidrige Inhalte im Internet veröffentlicht) oftmals nicht greifen lässt – dies gilt im Internet nicht zuletzt aufgrund von Ermittlungsproblemen infolge seines grenzüberschreitenden Charakters und der Flüchtigkeit der übertragenen Daten –, wird zunehmend versucht, andere Personen zur Verantwortung zu ziehen. Veranschaulicht ausgedrückt: Gestern war nur der Urheber rechtswidriger Dateien strafbar, heute ist es bereits der Provider, der den Zugang dazu vermittelt oder den Speicherplatz dafür anbietet, morgen ist es vielleicht schon der Nutzer, der den rechtswidrigen Inhalt lediglich betrachtet. So ist in Deutschland gemäß § 184b Abs. 4 Satz 2 dStGB etwa bereits der bloße Besitz einer kinderpornographischen Datei strafbar, mag dieser auch unvorsätzlich – etwa beim Surfen auf unverdächtigen Webseiten – erlangt worden sein.

Die Ausweitung der Verantwortlichkeit im Internet mag insoweit begrüßenswert sein, als dadurch begangenes Unrecht überhaupt geahndet werden kann. Allerdings darf der – leichte und angenehme – Rückgriff auf lediglich mittelbar Verantwortliche nicht die – schwere und erfolgsunsichere – Suche nach dem eigentlichen Täter ersetzen. So ist niemandem geholfen, wenn bei der Tötung eines Menschen nicht der Totschläger für seine Tat belangt wird, sondern nur derjenige, der ihm die Waffe verkauft hat. Durch die Ausdehnung der strafrechtlichen Verantwortlichkeit darf der Gesetzgeber also nicht seine eigene Verantwortlichkeit zur Bekämpfung der Computerkriminalität abwälzen. Mit einer Konzentration auf die strafrechtliche Verfolgung von Providern und Nutzern – anstatt auf die Sanktionierung der eigentlichen Urheber rechtswidriger Inhalte oder

krimineller Erscheinungsformen – werden eher die Symptome als die Ursachen bekämpft.

2. Europäisierung des Strafrechts

Ein zweiter Aspekt, der anhand der letzten gesetzgeberischen Akte beobachtet werden kann, ist die zunehmende Internationalisierung, vornehmlich Europäisierung des Strafrechts.²³ Obwohl etwa im Staatenbund der Europäischen Union die Mitgliedstaaten nur zurückhaltend Kompetenzen im Strafrecht abgeben, werden die europäischen Einflüsse stetig größer. Dies gilt nicht zuletzt bei der Suche nach einer Lösung für neue internationale Herausforderungen, vorliegend etwa kriminelle Handlungen in einem nicht an staatliche Grenzen gebundenen Kommunikationsnetz wie das Internet. Hier sind zunehmend Versuche grenzüberschreitender Kooperation zu verzeichnen, die in völkerrechtlichen Abkommen enden. Im Bereich der Computerkriminalität ergingen etwa – wie bereits erwähnt – sowohl ein entsprechendes Übereinkommen des Europarates (Convention on Cybercrime vom 23. November 2001)²⁴ als auch ein erst Jahre später verabschiedeter Rahmenbeschluss des Rates der Europäischen Union über Angriffe auf Informationssysteme.²⁵ Letzterer orientierte sich bis ins Detail an dem Europaratsübereinkommen, blieb aber in seinen Vorgaben deutlich hinter diesem zurück.

Das kürzlich in Kraft getretene 41. Strafrechtsänderungsgesetz dient der Umsetzung dieser beiden europäischen Rechtsdokumente, ist aber nicht das erste Beispiel für europäische Einflüsse auf dem Gebiet des Internetstrafrechts. So ließen sich die Änderungen der Regelung zur Providerhaftung durch das Gesetz über rechtliche Rahmenbedingungen für den elektronischen Geschäftsverkehr (Elektronischer Geschäftsverkehr-Gesetz; EGG) vom 20. Dezember 2001²⁶ auf eine Richtlinie zurückführen,²⁷ welche die Normierung der Providerverantwortlichkeit in den Mitgliedstaaten der Europäischen Gemeinschaften harmonisieren wollte. Ferner beruhte

²³ Allgemein zum europäischen Strafrecht *Hecker*, Europäisches Strafrecht, 2. Aufl., Berlin/Heidelberg 2007; *Satzger*, Die Europäisierung des Strafrechts, Köln 2001; *Valerius* in: BeckOK-StGB (Fn. 10), Lexikon des Strafrechts: Europäisches Strafrecht; *Dannecker*, Jura 2006, 95; *Eisele*, JA 2000, 991, 992 ff.; *Hecker*, JA 2007, 561, 562 ff.

²⁴ Siehe Fn. 17.

²⁵ Siehe Fn. 18.

²⁶ BGBl. I, S. 3721.

²⁷ Richtlinie 2000/31/EG des Europäischen Parlaments und des Rates über den elektronischen Geschäftsverkehr vom 8. Juni 2000 (ABl. EG Nr. L 178 vom 17. Juli 2000, S. 1).

die angesprochene Ausweitung der Strafbarkeit des Computerbetrugs auf Vorbereitungshandlungen auf einem Rahmenbeschluss der Europäischen Union.²⁸

Die Beteiligung vieler Staaten an einem gemeinsamen Gesetzeswerk hat allerdings zwangsläufig zur Folge, dass die von allen getragenen Regelungen zumeist nur den kleinsten gemeinsamen Nenner bilden und einige Fragen offen bleiben müssen. Dies gilt insbesondere dann, wenn die Einigung – wie etwa bei Rahmenbeschlüssen der Europäischen Union – eine Umsetzungspflicht der Mitgliedstaaten begründet. Beispielhaft veranschaulicht werden kann dies an der international umstrittenen Frage der Bekämpfung rassistischer Äußerungen im Internet, in der sich weder in dem Rahmenbeschluss der Europäischen Union noch in dem Übereinkommen des Europarates eine Einigung findet. Der Europarat hat immerhin ein Zusatzprotokoll zur Convention on Cybercrime in die Wege geleitet,²⁹ das aber von deutlich weniger Staaten als das Hauptübereinkommen unterzeichnet wurde.

Übereinkommen zur Bekämpfung der Cyberkriminalität sind also zwar äußerst begrüßenswert und zukunftsweisend, dürfen aber weder für die internationale Staatengemeinschaft noch für den nationalen Gesetzgeber das Ende der Bemühungen darstellen. Vielmehr dürfen sich die einzelnen Staaten nicht mit dem gemeinsam begonnenen Weg begnügen, sondern müssen diesen ggf. auch allein fortsetzen, um auf neue oder bestehende Herausforderungen durch das Internet augenblicklich zu reagieren. Ein aktuelles Gegenbeispiel für fehlende Bemühungen des deutschen Gesetzgebers zeigt die Neuregelung der Providerhaftung, die durch Gesetz vom 26. Februar 2007³⁰ in das neue Telemediengesetz überführt wurde. Der Gesetzgeber übernahm die bisherigen Vorschriften zur Verantwortlichkeit von Providern unverändert, obwohl in den vergangenen Jahren einige Fragen, wie insbesondere zur Haftung für Hyperlinks, aufgeworfen wurden. Zwar wurde ein Änderungsbedarf nicht kategorisch verneint, gleichwohl blieb der Gesetzgeber aber im Hinblick auf einen anstehenden Evaluierungsbericht der Europäischen Kommission untätig.³¹ Die Trumpfkarte der Europäisierung verkommt somit zu einer Aussetzkarte für den Gesetzgeber.

²⁸ Siehe Fn. 15.

²⁹ Zusatzprotokoll vom 28. Januar 2003 zum Übereinkommen über Computerkriminalität betreffend die Kriminalisierung mittels Computersystemen begangener Handlungen rassistischer und fremdenfeindlicher Art (SEV Nr. 189).

³⁰ Gesetz zur Vereinheitlichung von Vorschriften über bestimmte elektronische Informations- und Kommunikationsdienste (Elektronischer-Geschäftsverkehr-Vereinheitlichungsgesetz; ElGVG); BGBl. I, S. 179.

³¹ BT-Drs. 16/3078, S. 11.

C. Internetstrafrecht in der Rechtsprechung

I. Fall „CompuServe“

Kommen wir zum zweiten Hauptteil des Vortrages und wenden uns der Rechtsprechung zu. Auch hier sind einige bedeutende Ereignisse zu verzeichnen, die zum Teil über die Grenzen Deutschlands hinaus Aufmerksamkeit erlangten. Der wohl erste spektakuläre Internetfall, über den ein deutsches Strafgericht zu entscheiden hatte, war der Fall „CompuServe“, nach dem Namen des Angeklagten auch als Fall „Somm“ bekannt. Felix Somm war Geschäftsführer der CompuServe GmbH (im Folgenden: CompuServe Deutschland), einer Tochtergesellschaft der in den Vereinigten Staaten ansässigen CompuServe Incorporated (im Folgenden: CompuServe USA), für welche die CompuServe Deutschland hierzulande Kunden gewann und Einwahlknoten für den Internetzugang bereitstellte. CompuServe USA unterhielt nun auf US-amerikanischem Territorium einige Server, auf denen Newsgroups abgespeichert wurden. Einige dieser Gruppen enthielten Bilddateien mit kinderpornographischem Inhalt, frei zugänglich von Dritten dort hinterlegt und somit von jedermann (auch in Deutschland) abrufbar. Während es für CompuServe USA ohne Weiteres möglich war, die betreffenden Newsgroups zu sperren bzw. deren Inhalte zu löschen, hatte die CompuServe Deutschland keinen direkten Zugriff auf die Server und konnte lediglich auf die betreffenden Dateien hinweisen, verbunden mit der Bitte um Sperrung oder Löschung.

Aufgrund dieses Sachverhalts verurteilte das Amtsgericht München den Angeklagten Felix Somm am 28. Mai 1998 unter anderem wegen mittäterschaftlicher Verbreitung pornographischer Schriften zu einer Freiheitsstrafe von zwei Jahren auf Bewährung.³² Das Gericht verwehrte der CompuServe Deutschland die weitgehende Haftungsprivilegierung des damals noch jungen § 5 Abs. 3 TDG für Access-Provider mit dem formalen Argument, dass die CompuServe Deutschland keine eigenen Kunden habe, denen sie den Zugang zum Internet gewähre. Während insoweit also strikt zwischen CompuServe Deutschland auf der einen und CompuServe USA auf der anderen Seite unterschieden wurde, zeigte sich ein anderes Bild bei der Einordnung von CompuServe Deutschland als Host-Provider. Hier war auf einmal nicht mehr von Bedeutung, dass der Speicherplatz für die rechtswidrigen Inhalte von CompuServe USA zur Verfügung gestellt wurde und dass auch nur CompuServe USA die Möglichkeit hatte, die Inhalte zu löschen. Vielmehr wurden der CompuServe Deutschland sowohl der Providerstatus als auch die Löschungsmöglichkeit von CompuServe USA zugerechnet. Der Strafrichter kam demzufolge zu dem Ergebnis, dass CompuServe

³² AG München NJW 1998, 2836 mit Anmerkung *Hoeren*, NJW 1998, 2792; MMR 1998, 429 mit Anmerkung *Sieber*; CR 1998, 500 mit Anmerkung *Moritz*; K&R 1998, 406 mit Anmerkung *Eichler*.

Deutschland ein Host-Provider sei, der, da die Voraussetzungen der Haftungserleichterung nach dem damaligen § 5 Abs. 2 TDG nicht erfüllt waren, für die abgespeicherten pornographischen Inhalte verantwortlich sei.

Das Urteil führte in der Computer- und Internetbranche zu Entsetzen und stieß in der juristischen Welt zu Recht auf Empörung und einhellige Ablehnung. Jenseits der inhaltlich nicht mehr vertretbaren Begründung des Urteils, die hier nur angerissen werden konnte, waren nicht zuletzt deren äußere Begleitumstände mehr als zweifelhaft, angefangen von einem fraglichen Ermittlungsgebaren der Justizbehörden im Vorfeld bis hin zu einem – selbst bei zutreffender Begründung – äußerst hohen Strafmaß für einen nicht strafrechtlich in Erscheinung getretenen Angeklagten und schließlich einer Verurteilung, obwohl selbst die Staatsanwaltschaft sich in der Hauptverhandlung von den Argumenten der Verteidigung und den gehörten Sachverständigen überzeugen ließ und Freispruch beantragte. Der Imageverlust für die deutsche Wirtschaft und nicht zuletzt die deutsche Justiz waren nicht unerheblich und konnten durch den Freispruch von Felix Somm im Berufungsverfahren vor dem Landgericht München am 17. November 1999³³ nur unvollständig behoben werden.

II. Fall „Toebe“

Für ähnliche Aufregung sorgte das Urteil des Bundesgerichtshofs vom 12. Dezember 2000³⁴ im Fall „Toebe“. Toebe war ein australischer Staatsangehöriger, der auf einer frei zugänglichen Webseite im Internet englischsprachige Artikel veröffentlichte, in denen er den Holocaust an jüdischen Bürgern durch das NS-Regimes bestritt. Die Artikel stellte er von Australien aus auf einen dort gelegenen Server, von wo aus sie weltweit, d.h. auch von Nutzern aus Deutschland, abgerufen werden konnten.

Der Bundesgerichtshof verurteilte den Angeklagten unter anderem wegen Volksverhetzung gemäß § 130 Abs. 1 und Abs. 3 dStGB. Zwar ist unstrittig, dass die Äußerungen des Angeklagten diesen Straftatbestand verwirklichen. Problematisch war jedoch, ob und ggf. unter welchen Voraussetzungen das deutsche Strafrecht auf Veröffentlichungen im Internet überhaupt anwendbar ist. Der Bundesgerichtshof kam zu dem Ergebnis, dass die Anwendbarkeit deutschen Strafrechts gerechtfertigt sei, und verwies auf den besonderen Bezug volksverhetzender Online-Publikationen zur

³³ LG München NJW 2000, 1051 mit Anmerkung *Kühne* NJW 2000, 1003; MMR 2000, 171; CR 2000, 117 mit Anmerkung *Moritz*; K&R 2000, 193 mit Anmerkung *Barton*.

³⁴ BGHSt 46, 212. Eingehend zum Fall Toebe *Körber*, Rechtsradikale Propaganda im Internet. Der Fall Töbe, Berlin 2003.

Bundesrepublik, begründet durch die leidbringende Geschichte Deutschlands und die Einzigartigkeit des Holocaust.³⁵

Die Konsequenzen der Entscheidung sind äußerst bedenklich. Ist auch auf Internetinhalte auf ausländischen Servern – und somit letztlich unabhängig vom Standort des Servers – das deutsche Strafrecht anwendbar, begründet dies eine Allzuständigkeit der deutschen Justizbehörden zur Überwachung des Internets, und zwar unter Zugrundelegung der deutschen Strafrechtsvorschriften als weltweitem Maßstab.³⁶ Abgesehen von der darin liegenden Oktroyierung eigener kultureller Wertvorstellungen, die nicht gerade einen Ausdruck der Achtung anderer Staaten und ihrer Rechtsordnungen darstellt, erscheinen die Folgen dieser Entscheidung vor allem dann als fraglich, wenn auch andere Staaten ihre nationalen Maßstäbe als für die gesamte Welt verbindlich erklärten. Jeder Betreiber einer Webseite würde sich dadurch einem erhöhten Strafbarkeitsrisiko ausgesetzt sehen, weil im Internet veröffentlichte Inhalte letztlich nur dann unbedenklich wären, wenn sie dem kleinsten gemeinsamen Nenner des in allen Staaten Erlaubten entsprächen. Nicht unerwartet stieß daher auch diese Entscheidung auf weitgehende Ablehnung in der Rechtswissenschaft sowie auf Unverständnis im Ausland.

III. Kinderpornographie im Internet

Zum Abschluss sei noch auf zwei weitere Entscheidungen zum Internetstrafrecht eingegangen, deren Beachtung eher auf das Inland beschränkt blieb. In einer Entscheidung vom 27. Juni 2001³⁷ hatte der Bundesgerichtshof über die Strafbarkeit des Anbietens kinderpornographischer Dateien im Internet zu befinden. In den Urteilsgründen unterlaufen dem Bundesgerichtshof technische Ungenauigkeiten, die sich auch auf die rechtliche Betrachtung des Falles auswirken. So wird versäumt, hinreichend zwischen den gespeicherten Daten und dem Datenspeicher zu trennen, also zwischen den (unkörperlichen) Inhalten auf der einen und dem (körperlichen) Inhaltsträger auf der anderen Seite. Diese Unterscheidung hat im deutschen Strafrecht Tradition und kommt in dem sog. Schriftenbegriff des § 11 Abs. 3 dStGB zum Ausdruck, der allen Äußerungsdelikten zugrunde liegt. Demnach sind Schriften alle Darstellungen wie etwa Abbildungen, Bild- und Tonträger sowie *Datenspeicher*; allen Darstellungen ist ihre Eigenschaft als körperlicher Gegenstand gemein. Anknüpfend an

³⁵ BGHSt 46, 212 (220 ff.).

³⁶ *Hilgendorf/Frank/Valerius* (Fn. 5), Rn. 249 ff.; *Hilgendorf*, NJW 1997, 1873 (1878); *Koch*, GA 2002, 703 (707); *Lagodny*, JZ 2001, 1198 (1200).

³⁷ BGHSt 47, 55.

diese Differenzierung wird bei den Äußerungsdelikten regelmäßig zwischen den Tathandlungen des Verbreitens und des Zugänglichmachens unterschieden. Die Verbreitung erfordert die (körperliche) Weitergabe einer Schrift, beim Zugänglichmachen dagegen genügt die (unkörperliche) Wahrnehmung ihres Inhalts.

Der Bundesgerichtshof verwischte in seiner Begründung die Unterscheidung zwischen Inhalt und Inhaltsträger, indem er ausführt, dass auch Daten (vorliegend digitalisierte Photos) Datenspeicher im Sinne des § 11 Abs. 3 dStGB seien.³⁸ Dass diese Differenzierung beseitigt wird, wirkt sich sodann auf die Auslegung der Tathandlung des Verbreitens aus. Da Daten mangels Körperlichkeit nicht verbreitet werden können, aber als Schrift nach Auffassung des Bundesgerichtshofs verbreitet werden können müssen, kommt er zu der Schlussfolgerung, dass der Verbreitensbegriff im Internet nicht mehr passe und einer Erweiterung bedürfe, die auf das Merkmal der Körperlichkeit verzichtet. Ausreichend sei nach diesem spezifischen Verbreitensbegriff daher, dass eine Datei auf dem Rechner des Internetnutzers ankomme und dieser die Möglichkeit des Zugriffs habe.³⁹

Was zeigt die zu Recht vielfach kritisierte,⁴⁰ wenngleich von der herrschenden Lehre ohne inhaltliche Auseinandersetzung übernommene Auffassung des Bundesgerichtshofs? Zum einen schienen zumindest damals Computer und Internet noch geheimnisvolle Unbekannte zu sein, deren Funktionsweise – wie die Vermischung von Daten und Datenspeicher zeigt – dem Senat nicht ganz geläufig war. Diese Unbekannten schienen zudem unheimlich zu sein oder zumindest skeptisch beäugt zu werden, denn ansonsten lässt sich kaum erklären, dass der Bundesgerichtshof die traditionelle Unterscheidung zwischen Zugänglichmachen des Inhalts und Verbreiten des Inhaltsträgers einfach aufgibt, obwohl dies überhaupt nicht nötig gewesen wäre. Schließlich hätte der Angeklagte bereits nach der Variante des Zugänglichmachens ebenso bestraft werden können, so dass sich der Bundesgerichtshof mit dem Verbreitensbegriff überhaupt nicht hätte auseinandersetzen müssen. Dass und wie er es gleichwohl tat, deutet auf einen gewissen Aktionismus hin, insbesondere wenn man bedenkt, dass hier derselbe Senat entschied, der nur ein halbes Jahr zuvor das weitreichende Urteil im Fall „Toeben“ gefällt hatte.

³⁸ BGHSt 47, 55 (58).

³⁹ BGHSt 47, 55 (59).

⁴⁰ *Hilgendorf/Frank/Valerius* (Fn. 5), Rn. 412 ff.; *Gercke*, MMR 2001, 678; *Kudlich*, JZ 2002, 310; *Lindemann/Wachsmuth*, JR 2002, 206.

IV. Online-Demonstrationen im Internet

Das jüngste und abschließende Beispiel aus der Rechtsprechung beschäftigte sich mit Online-Demonstrationen im Internet. Der Angeklagte rief zu einem sog. Cyber-Sit-in gegen die Deutsche Lufthansa AG auf, um gegen ihre Beteiligung an Abschiebungen von Personen ohne Aufenthaltsrecht zu protestieren. Mit Hilfe einer speziellen Software wurde am Tag der Hauptversammlung der Lufthansa für die Dauer von zwei Stunden so oft auf ihre Webseite zugegriffen, dass die Rechenkapazität des Webservers überlastet wurde und Anfragen potentieller Nutzer und Kunden erfolglos blieben. Durch diesen technisch sog. „Denial of Service“-Angriff kam es neben dem Imageverlust der Lufthansa zu einem materiellen Schaden in Höhe von knapp 48 000 EUR.

Das Amtsgericht Frankfurt am Main bewertete den Cyber-Sit-in als Nötigung gemäß § 240 Abs. 1 dStGB und verurteilte daher den Angeklagten am 1. Juli 2005⁴¹ wegen öffentlicher Aufforderung zu einer Straftat nach § 111 dStGB zu einer Geldstrafe von 90 Tagessätzen. Ausführungen zu einer eventuellen Strafbarkeit wegen des technischen Charakters des „Denial of Service“-Angriffs ließ die Entscheidung völlig vermissen. In der Revision hob das Oberlandesgericht Frankfurt am Main das Urteil mit Entscheidung vom 22. Mai 2006⁴² auf und sprach den Angeklagten frei. Eine Strafbarkeit wegen Nötigung wurde unter Verweis auf die Parallelen zur – in Deutschland nicht ohne Weiteres strafbaren – Sitzblockade abgelehnt, ebenso eine Strafbarkeit wegen Datenveränderung bzw. Computersabotage gemäß §§ 303a f. dStGB.

Die beiden Entscheidungen könnten kaum gegensätzlicher sein. Während die erste Instanz relativ kurz die Besonderheiten einer virtuellen Demonstration behandelte, ging das Revisionsgericht äußerst ausführlich darauf ein. Während die erste Instanz die technische Seite des Cyber-Sit-ins überhaupt nicht ansprach, bemühte sich das Oberlandesgericht auch hier um eine hinreichende Darstellung. Während das Amtsgericht die Strafbarkeit des Angeklagten mühelos bejahte, schien das Oberlandesgericht sichtbar bemüht, eine Verurteilung des Angeklagten mit allen Mitteln zu vermeiden. Auch wenn die Begründung des Oberlandesgerichts nicht nur aus diesem Gesichtspunkt in einigen Punkten angreifbar ist,⁴³ so ist die Entscheidung zumindest insoweit zu begrüßen, als sie sich den Besonderheiten sozialinadäquater Verhaltensweisen im Internet mit der gebotenen Sorgfalt und Ausführlichkeit widmet.

⁴¹ AG Frankfurt am Main MMR 2005, 863 mit Anmerkung *Gercke*.

⁴² OLG Frankfurt am Main MMR 2006, 547 mit Anmerkung *Gercke*.

⁴³ Ausführlich *Valerius*, in: Hilgendorf (Hg.), Dimensionen des IT-Rechts, Berlin 2008, S. 19 ff. Zur Thematik auch *Eichelberger*, DuD 2006, 490; *Kitz*, ZUM 2006, 730; *Klutzny*, RDV 2006, 50; *Kraft/Meister*, K&R 2005, 458.

V. Zusammenfassung

Die vorgestellten Entscheidungen zeigen, dass die Rechtsprechung noch keinen sicheren Umgang mit dem Internet als neuer Informations- und Kommunikationstechnologie gefunden hat. Vielfach bereiten schon Funktionsweise und Charakterzüge des Internets den Fachgerichten nach wie vor Probleme, was dazu verleitet, bestehende rechtliche Grundsätze der bisherigen, weder digitalisierten noch vernetzten Welt ohne Not aufzugeben, zu verändern oder zu erweitern, anstatt zu versuchen, die neuen Herausforderungen darunter zu subsumieren. Dabei ist das Internet entgegen landläufiger Etikettierung keine neue, eigenständige oder virtuelle Welt, sondern Teil der bestehenden, realen Welt.

Von den dogmatischen Problemen abgesehen ist zudem festzuhalten, dass zwischen der Rechtsprechung und dem Internet noch kein völlig unvoreingenommenes Verhältnis besteht. Bislang war der Rechtsprechung überwiegend eine gewisse Skepsis gegenüber dem Internet und der damit verbundenen, leider nicht geringen Missbrauchsgefahr anzumerken, die sich auch auf Inhalt und Begründung der Entscheidungen auszuwirken schien. Einen eher erfreulichen Lichtblick stellt insoweit die Entscheidung des OLG Frankfurt am Main dar, die jedoch ihrerseits über das Ziel hinausschießt und allzu bereitwillig eine Strafbarkeit des Angeklagten im konkreten Fall verneint. Immerhin lässt die Entscheidung auf eine allmähliche Trendwende in der Rechtsprechung und auf der Problematik gerecht werdende Entscheidungen in der Zukunft hoffen.

D. Fazit

Das Internetstrafrecht in Deutschland stellt ein Rechtsgebiet dar, das sowohl auf eine Vielzahl gesetzgeberischer Akte als auch auf zahlreiche, nicht immer unumstrittene Entscheidungen zurückblicken kann. Obwohl Gesetzgebung und Rechtsprechung das Gebiet schon weitgehend erschlossen haben, warten am Horizont – dem steten Fortschritt geschuldet – viele neue Herausforderungen, angefangen von der Änderung technischer Grundlagen wie die fortschreitende Konvergenz der Medien bis hin zur strafrechtlichen Behandlung neuer Angriffsformen im Internet.

Wer diese Herausforderungen meistern will, muss über die (ggf. auch nur gefühlte) Strafwürdigkeit des jeweiligen Einzelfalls hinausschauen und sich um Regeln bemühen, die verallgemeinerungsfähig und möglichst unabhängig von den stetem Wandel unterworfenen technischen Besonderheiten des konkreten Verhaltens sind. Die eingangs erwähnte, bereits etablierte rechtswissenschaftliche Subdisziplin des Internetstrafrechts kann durch eine weiterhin kritische, aber auch lösungsorientierte Begleitung neuer Akte der Gesetzgebung sowie neuer Entscheidungen der Rechtsprechung einen nicht

unerheblichen Beitrag dazu leisten und dadurch zugleich Bedeutung und Stellenwert des Internetstrafrechts in Deutschland weiter erhöhen.

Almanya`da Internet Ceza Hukuku¹

Dr. Brian Valerius²

Übersetzt von: Rabia Ünlü, LL.M.Eur.

A. Giriş

Almanya`da internet suçları o denli geniş bir alan ki, bunu kısa bir tebliğ ile her yönden ele alamayız ama en azından önemli noktalara değinebiliriz. Fazla ayrıntılara girmemek şartıyla genel bir bakışa zamanımızın yeteceğini düşünüyorum. Yasama ve uygulamadan örnekler sunmak, geçmişte ve bugün durumun nasıl olduğu ve gelecekte nelerin olabileceği hakkında genel bir fikir oluşturabilecektir.

İktibas yoluyla kabul edilen internet ceza hukukuna ilişkin yasal düzenlemelere bakılacak olursa, bu konuların derinden ilgilenmeye değer oldukları ortadadır. Halihazırda aynı konuyla ilgili internetin özel hukuk ve kamu hukukundaki düzenlemelerinin de dikkate alındığı en az üç basılı³ ve en az iki online dergileri⁴ düzenli olarak çıkarılmaktadır.

Geçen yıllar içerisinde internet medya ve enformasyon ceza hukuku alanında ihtisaslaşmış kürsüler artmıştır. Sonunda 2005 yılında 3 farklı ders kitabının yayınlanmasıyla⁵ internet ceza hukuku, ceza hukuku ana bilim dalının bir alt bilim dalı haline gelmiştir.

B. İnternet Ceza Hukukuna İlişkin Yasal Düzenlemeler

I. 15 Mayıs 1986 tarihli 2. Ekonomik Suçların Önlenmesiyle İlgili Kanun (2. WiKG)

Bugün internet ceza hukukunun anlamı ve bağımsız bir bilim dalı olmasının sebebi, geniş çapta gerçekleştirilen yasama faaliyetleridir. Bilgisayar ceza hukukundaki ilk özel

¹ Dipnotların dahil edildiği bu tebliğ, 1 Eylül 2007 tarihinde “Alman- Türk Ceza Hukuku Karşılaştırması” adlı sempozyumda sunulan tebliğin aynısıdır.

² Yazar Würzburg Üniversitesi Hukuk Fakültesi, Ceza hukuku, Ceza Usul Hukuku, Hukuki Teori, Enformasyon Hukuku, Bilişim Hukuku (Prof. Dr. Dr. Hilgendorf) kürsüsünde Asistandır.

³ Söz konusu dergiler ilk olarak 1985 yılında yayınlanan „Computer und Recht“, 1998 yılında yayınlanan „Multimedia und Recht“ ve hemen bir yıl sonra ilk kez yayınlanan „Kommunikation & Recht“dir.

⁴ “JurPC“ (1989) ve „Medien Internet und Recht“ (kasım 2005).

⁵ Hilgendorf/Frank/Valerius, Computer- und Internetstrafrecht. Ein Grundriss, Berlin/Heidelberg 2005; Malek, Strafsachen im Internet, Heidelberg 2005; Marberth-Kubicki, Computer- und Internetstrafrecht, München 2005.

hükümleri içeren 15 Mayıs 1986 tarihli⁶ 2. Ekonomik Suçların Önlenmesiyle İlgili Kanun bu anlamda bir başlangıç sayılmaktadır. Böylelikle Al.CK. § 202a'ya göre, verilerde casusluk, aynı Kanunun § 303a ve § 303b uyarınca verilerin değiştirilmesi ve bilgisayar sabotajı suç sayılmaktadır. Bu maddeler ile özellikle ekonomik ve idari alanlardaki bilgi işlemlerin korunmasının ön planda tutulmasından dolayı, bilgi depolama ve bilgi işlem cihazlarına yönelik dış müdahaleler ve sabotaj eylemleri önlenmek istenmiştir.

Bilgi işlem cihazları aracılığıyla mal varlığına karşı yapılan saldırılar giderek artmaktadır. Elektronik ve bilgisayar destekli yeni saldırı şekillerini önlemek ve oluşabilecek kanun boşluklarını gidermek amacıyla bilgisayar suçları ceza hükümlerine eklenmiştir ve evrakta sahtecilikle ilgili ceza hükümleri değiştirilerek genişletilmiştir (Al.CK. § 269 ve § 270 maddelerinde yer alan ve delil niteliği taşıyan belgelerde sahtecilik ile bilgi işlem yoluyla hukuki işlemlerde sahtecilik). Söz konusu evrakta sahtecilikle ilgili hükümlerin yanı sıra, 1986 yılında Al.CK.'a yeni konulan normların önemi giderek artmaktadır ve bu normlar özellikle „Phishing“in sayesinde alınan belgelerin kullanımı gibi o dönemde henüz mümkün olmayan yeni internet suçlarını da kısmen kapsamaktadır.

II. 22 Temmuz 1997 Tarihli Enformasyon ve İletişim Hizmetleri Kanunu

22 Temmuz 1997 tarihli Enformasyon ve İletişim Hizmetleri Kanunu⁷, internet ortamına öncelik vererek özellikle modern enformasyon ve iletişim teknolojisindeki zorluklara karşı durmaktadır. Bu Kanun, Alman Ceza Kanunu'nda sadece küçük değişikliklere sebep olmuştur. Örneğin çocuk pornografisi içerikli yazı ve görüntülerin satın alınması veya bunlara sahip olunması, gerçeğe yakın görüntüler ifadesiyle değiştirilerek genişletilmiştir. Dijital ortamda yapılan işlemlerin kaynağının reel ya da fiktif olduğunun neredeyse ayırt edilememesinden dolayı oluşan ve giderek artan ispat zorlukları böylelikle önlenmeye çalışılmıştır.⁸ Bilgilerin giderek dijitalleşmesi nedeniyle Ceza Kanunu'nun genel hükümlerinde veri taşıyan tüm araçlar (örneğin salt okunur bellek, CD- Rom, USB Stick gibi) suçun kanuni unsuruna dahil edilmiştir ve böylelikle

⁶ BGBl. I, S. 721; allgemein zum 2. WiKG *Hilgendorf/Frank/Valerius*, in: Vormbaum/Welp (Hg.), Das Strafgesetzbuch, S. 258, 294 ff.; *Haft*, NStZ 1987, 6; *Lenckner/Winkelbauer*, CR 1986, 483; 654; 824; *Möhrenschlager*, wistra 1986, 128.

⁷ BGBl. I, S. 1870; allgemein zum IuKDG *Engel-Flechsing/Maennel/Tettenborn*, NJW 1997, 2981; *Gounalakis/Rhode*, K&R 1998, 321; *Rofnagel*, NVwZ 1998, 1.

⁸ BT-Drs. 13/7385, S. 60; 13/7934, S. 41.

dijital ortamında yayınlanan hukuka aykırı yayınlar, cismi nitelikte olmasalar da, cezalandırılabilirlerdir.⁹

Enformasyon ve İletişim Hizmetleri Kanunu'nun getirdiği bir diğer yenilik ise Tele Hizmetler Kanunu'nun 5. maddesinde yer verilen internet sistem sağlayıcılarının cezai sorumluluklarının düzenlenmesiydi.¹⁰ Söz konusu yenilik disiplinlerarası bir düzenleme olup, sadece ceza hukukunu değil tüm hukuk dallarını etkilemektedir. Bu durum, enformasyon ve iletişim hizmetlerinin genel olarak düzenlemeyi ve tüm hukuk dallarına etki etmeyi öngören Enformasyon ve İletişim Kanunu'nun yapısına uygun düşen bir özelliktir. Bu maddeyle hukuka aykırı bir içerikten dolayı, internet hizmet sağlayıcılarının cezai sorumlulukları da düzenlenmiştir. Ticari şirketlerin gerekli olan altyapısını sağladığından ve web sayfası, elektronik posta, haberleşme forumları veya sohbet etme şeklindeki farklı kullanım olanaklarını sunarak herkesçe kullanılabilir hale getirdiğinden, internet gündelik yaşamda kullanılan bir iletişim aracı olarak hızla yaygınlaşmıştır. Artık internet ortamındaki her türlü verilerin aktarılmasında bir veya birden fazla sunucunun internet bağlantısını sağlamak, web sayfalarına gereken hafızanın sağlanması veya verilerin taşınması için gerekli kablo ağının kullanımına sunmak gibi katkıları bulunmaktadır.

Şu an, internet cezalandırılabilir içeriklerin ve ayrıca hukuka aykırılıkların dahi bulunmadığı bir ortam olmalıyken durum farklıdır. Az çok bilgi sahibi olan her kullanıcı kısa bir süre içerisinde hakaret içerikli ifadelerin yer aldığı forum sayfalarına, ırkçı veya halkı kışkırtıcı içeriklere sahip aşırı sağcı web sitelerine veya fotoğraf ve video şeklindeki çocuk pornografisi içerikli sayfalara ulaşabilmektedir. Bu tür yasadışı yayınlar, hukuki sorumlulukları tartışmalı servis sağlayıcılar olmazsa, ne ulaşılabilir ne de yayınlanabilir. "CompuServe" davasında verilen uluslararası geçerli karar, hassas sayılan bu konuya en iyi örnektir.¹¹

Tele Hizmetler Kanunu'nun 5. maddesindeki düzenlemeye göre yasadışı içerikli web sayfalarını yayınlayan içerik sağlayıcısı (Content-Provider) öncelikle sorumlu olacaktır. Bunun dışında, internet bağlantısını sağlayan erişim sağlayıcı (Access-Provider) veya yasadışı yayınlar için gerekli hafızayı sunan yer sağlayıcı (Host-Provider) gibi diğer tüm sağlayıcılar, sadece belirli koşullarda ve yayınlara etki etme gücüne göre hukuken sorumlu tutulabilmektedirler. Bu derecelendirilmiş sorumluluklar prensibi bugün de kabul edilmektedir. Web sayfalarına yerleştirilen bağlantılar veya arama motorlarından

⁹ BT-Drs. 13/7385, S. 36.

¹⁰ İçerik sağlayıcısının sorumluluğu ile ilgili genel olarak *Hilgendorf/Frank/Valerius* (Dipnot 5), Rn. 274 ff.; *Valerius* in: BeckOK-StGB, 8. Edition 2009, Lexikon des Strafrechts: Providerhaftung; ayrıntılı bilgi için *Kessler*, Zur strafrechtlichen Verantwortlichkeit von Zugangs Providern, Berlin 2003.

¹¹ Bkz. aşağıda C. I.

dolayı hukuki sorumlulukların nasıl olacağı konusu, buna ilişkin kuralların iki defa değiştirilmesine rağmen, hala tartışmalıdır.¹²

III. Diğer Yasa Değişiklikleri

Teknik gelişmelere ve dijitalleşme sürecine cevap vermeye çalışan yasa koyucu, 2003 yılının sonlarına doğru, bilgisayar ve internet ceza hukuku alanında bu iki büyük değişikliklerinin yanı sıra birkaç küçük değişiklikler de yapmıştır. Al.CK.'nın, radyo, televizyon, ve tele hizmetler aracılığıyla pornografik yayınlar yapılmasını düzenleyen § 184c (artık § 184d), 27 Aralık 2003 tarihli Cinsel Suçlarla İlgili Maddelerin Değiştirilmesi Kanunu ile¹³ genişletilmiş ve canlı pornografik yayınların sadece radyo veya televizyon üzerinden değil, internet gibi medya ve tele hizmetler aracılığıyla yapılmasını da kapsar hale getirilmiştir.

Bundan birkaç gün önce 22 Aralık 2003 tarihli 35. Ceza Kanunu Değişikliği ile İlgili Kanun ile bilgisayar dolandırıcılığıyla ilgili § 263a'nın 3. ve 4. fıkralarının eklenmesiyle,¹⁴ bilgisayar suçlarının hazırlığında kullanılacak olan her türlü programlarla ilgili eylemleri de suç haline getirilmiştir. Kanun koyucunun hazırlık aşamasındaki eylemlere, suç niteliği kazandırması ile Avrupa Birliği Konseyi'nin çerçeve kararı¹⁵ ulusal hukuk sistemine uyarlanmıştır.

IV. 7 Ağustos 2007 Tarihli, Ceza Kanununda 41. Değişiklik Kanunu

Bilgisayar suçlarının önlenmesi konusunda geniş çapta değişiklikleri beraberinde getiren 7 Ağustos 2007 tarihli ve 3 hafta önce yürürlüğe girmiş olan Ceza Kanunu'un 41. Değişiklik Kanunu,¹⁶ Avrupa hukuku menşelidir.

Enformasyon teknolojisinin hızlı gelişimiyle oluşan ve 23 Kasım 2001 tarihli Avrupa Konseyi Siber Suç Sözleşmesi¹⁷ ile 24 Şubat 2005 tarihli Avrupa Birliği Konseyi'nin

¹² 20 Aralık 2001 tarihli Elektronik Ortamda Gerçekleştirilen Ticari İşlemlerin Hukuksal Çerçeve Koşullarına İlişkin Kanununda (Elektronik ortamda ticari işlemler kanunu) (Elektronischer Geschäftsverkehr-Gesetz; EGG) (BGBl. I, S. 3721) ve 26 Şubat 2007 tarihli Elektronik Ortamda Gerçekleştirilen Enformasyon ve İletişim Hizmetleriyle İlgili Uyum Kanunu (Elektronischer-Geschäftsverkehr-Vereinlichungsgesetz; ElGVG) (BGBl. I, S. 179). Ayrıca bkz. II. 5. b) a.E.

¹³ Cinsel Özgürlüğüne Karşı İşlenen Suçlarla İlgili Düzenlemelerin Değiştirilmesiyle İlgili Kanun ve diğer yeni düzenlemelerle ilgili kanun (BGBl. I, S. 3007).

¹⁴ Avrupa Konseyinin Nakit Olmayan Ödemelerde Dolandırıcılığın Önlenmesine Dair 28 Mayıs 2001 tarihli Çerçeve Kararı'nın Ceza Kanunu'nun Uyumlaştırılmasına Dair 35. Değişiklik Kanunu (35. StrÄndG; BGBl. I, S. 2838).

¹⁵ Karşılaştırınız m.3 ve 4 Avrupa Konseyinin Nakit Olmayan Ödemelerde Dolandırıcılığın Önlenmesine Dair 28 Mayıs 2001 tarihli Çerçeve Kararı (ABl. EG Nr. L 149 vom 2. Juni 2001, S. 1).

¹⁶ BGBl. I, S. 1786.

¹⁷ SEV Nr. 185.

Bilgi Sistemlerine Saldırılarla İlgili Çerçeve Kararı'na konu olan bilgisayar ve internet ceza hukukundaki düzenlemelerin revizyonuyla cezalandırılabilirlik alanındaki boşluklar giderilmeye çalışılmıştır.¹⁸

Avrupa hukuku düzenlemeleri bağlamında Alman ceza hukukunda yapılan veri casusluğu (§ 202a Al.CK.), bilgisayar sabotajı (§ 303b Al.CK.) suçlarındaki değişiklikler yanında, verilerin kontrol edilmesine ilişkin yeni bir suç tipi de yaratılmıştır. Bunların yanı sıra kontrol ve casusluk (§ 202c Al.CK.), verilerin değiştirilmesi (§ 303a/3 Al.CK.) ve bilgisayar sabotajı (§ 303b/5 Al.CK.) gibi suçların hazırlık hareketleri de suç sayılmıştır.

Yapılan kanun değişiklikleri elektronik iletişim alanında daha fazla koruma sağlayacaktır. Şöyle ki, verilerin kontrol edilmesiyle ilgili yeni suç tipi, e-mail yoluyla yazışmalar, "Voice-IP" teknolojisiyle yapılan görüşmeler veya belgelerin gönderilmesi gibi her türlü elektronik veri aktarımlarının izlenmesine karşı korumaktadır. Bu tarz bir koruma, gönderilen verilerin haksız bir dış müdahaleye karşı özellikle korunup korunmadığından bağımsız gerçekleştirilmektedir.

Al.CK. § 303b'deki bilgisayar sabotajı suçu, unsurları genişletildikten sonra, servis kullanımını engelleme (Denial of Service) türünde saldırıları da kapsamaktadır.¹⁹ Bu tür saldırıların suç olup olmaması konusu özellikle Frankfurt am Main Yüksek Eyalet Mahkemesinin verdiği ve ileride ayrıntılarını sunacağım bir karardan sonra tartışmalıydı.²⁰

Örneğin şifrenin kırılarak verilere izinsiz ulaşılması anlamına gelen "Hacking" olayının dahi suç olarak tanımlanması uzun tartışmalar neticesinde kabul edilmiştir. Son zamanlarda sayısı giderek artan ve zamanla gitgide kusursuzlaşan (örneğin ispiyon programlar, key logging veya truva atlarıyla) programlar buna sebep olmuştur.²¹ Verilere izinsiz ulaşılmasının engellenmesi gerektiği konusundaki zorunluluk ise hala güncelliğini korumaktadır. Verilere ulaşmanın böylesine zorlaştırılması, aynı zamanda failin cezalandırılabilir suç enerjisini açığa vurmaktadır.²²

¹⁸ ABl. EU Nr. L 69 vom 16. März 2005, S. 67.

¹⁹ Vgl. BT-Drs. 16/3656, S. 13.

²⁰ Bkz. aşağıda C. IV.

²¹ Vgl. BT-Drs. 16/3656, S. 9.

²² BT-Drs. 16/3656, S. 10.

V. Özet

Şimdiye kadar bilgisayar ve internet ceza hukuku alanında yapılan yasalara bakacak olursak, yasa koyucunun toplamda iyi işler başardığı aşınadır. Yasa koyucu, Ekonomik Suçların Önlenmesiyle İlgili 2. Kanun ile, her ne kadar detayda eleştirilse de, bilgisayar ceza hukuku alanında oldukça erken davranmıştır. Yapılan bu düzenlemelerin gelecek için tedbir niteliği taşımaktadır. Çünkü Alman kanunlarındaki düzenlemeler hem sayısız farklı şekillerdeki internet suçlarını kapsamakta hem de Avrupa Konseyi'nin Siber Suç Sözleşmesi gibi farklı uluslararası düzenlemelere yön vermiştir.

1. İnternette Cezai Sorumluluk Alanının Genişletilmesi

Bu yıl yapılan 4 Ağustos tarihli Ceza Kanununun 41. Değişiklik Kanunu ile, bilgisayar ve internet ceza hukuku alanında yapılan yeni düzenlemeler, yeni sorulara ve endişelere sebebiyet vermektedir. Bir yandan kanun koyucunun suç oluşturacak unsurları arttırdığı gözlemlenmektedir. Bunu sadece teknolojik gelişmelerle oluşan kanun boşluklarını gidermek amacıyla, yeni suç unsurları tanımlayarak değil, aynı zamanda ceza kanununun uygulama alanını hazırlık aşamasına kadar (örneğin bir suç işlemek amacıyla yapılan programlar gibi) genişleterek yapmaktadır. Bilgisayar ve internet ceza hukuku alanındaki bu eğilimin bir diğer göstergesi ise internet sunucularının (ceza hukukunun dışına da taşan) cezai sorumluluklarıdır.

Aslında internet sunucularının cezai sorumluluğu, sınırlı bir sorumluluk olarak ortaya çıkmaktadır. Fakat bu durum bilgisayar ve internet alanında genel olarak kabul edilen bir sorumluluk anlayışıdır. Cezai sorumluluk gerektiren haksız bir olay karşısında, özellikle de sınır ötesi karakteri nedeniyle soruşturması zor olan ve internet ortamında aktarılan verilerin çabuk silinebilir niteliğinden dolayı, doğrudan sorumlu olan faili (örneğin internet ortamında hukuka aykırı yayın yapan kişiyi) bulmak neredeyse mümkün olmadığından, cezai sorumluluk giderek başka kişilere aktarılmaya çalışılmaktadır. Durumu somutlaştırmak gerekirse: Daha önce sadece hukuka aykırı verileri yükleyen kişi cezalandırılabilirken, artık erişim sağlayıcı ve yer sağlayıcı gibi sunucular, gelecekte de belki hukuka aykırı içeriğe sahip sayfaları sadece izleyen internet kullanıcısı, fail konumuna getirilecektir. Almanya'da örneğin çocuk pornografisi içeren verilerin bilgisayarda bulunması, her ne kadar bunlar internetteki çocuk pornografisi konusunda bir şüphe taşımayan sayfalarda gezinirken istem dışı yüklenmiş olsa da cezalandırılmaktadır.

Bir hukuka aykırılığın takip edilebilmesi açısından internette sorumluluk alanının genişletilmiş olması olumlu bir gelişmedir. Fakat zor ve belirsiz olan asıl faili bulmak yerine, kolay ulaşılabilen dolaylı yoldan sorumlu olanları bulmakla yetinmemek gerekir.

Şöyle ki, bir cinayet olayında sadece silahı satan kişiyi yakalayıp suçu işleyen asıl failin üzerine gitmemek, kimseye fayda sağlamayacaktır. Yani kanun koyucunun cezai sorumluluk alanını genişletmesi, bilgisayar suçlarının önlenmesiyle ilgili sorumluluğundan kurtulduğu anlamına gelmemektedir. Asıl failerin cezalandırılması yerine sistem sağlayıcılarıyla kullanıcıların cezai takibatı üzerinde durmakla suçun kaynağı değil, semptomları önlenmeye çalışılmaktadır.

2. Ceza Hukukunun Avrupa Hukukuyla Uyumlaştırılması

Son zamanlarda yapılan yasa değişikliklerindeki bir diğer husus ise ceza hukukunun giderek uluslararası hukukla, özellikle Avrupa hukukuyla uyumlaştırılmasıdır.²³ Üye devletlerin ceza hukuku alanındaki yetkilerini Avrupa Birliği'ne sınırlı olarak devretmesine rağmen, Avrupa'nın etkisi giderek artmaktadır. Bu durum sadece internet gibi sınırlara bağlı olmayan bir iletişim ağında gerçekleştirilen suçlarda değil aynı zamanda uluslararası platformda alınması gereken önlemler söz konusu olduğunda da görülmektedir. Uluslararası sözleşmelerle neticelenen bu konulardaki sınırötesi işbirliği arayışı giderek artmaktadır. Bilgisayar suçluluğu alanında, yukarıda bahsetmiş olduğum gibi, hem Avrupa Konseyi'nin oluşturduğu bir sözleşme mevcuttur (23 Kasım 2001 tarihli Siber Suç Sözleşmesi)²⁴ hem de bir kaç yıl sonra İletişim Sistemlerine Karşı Saldırılarla ilgili Avrupa Birliği Konseyi'nin kabul ettiği bir çerçeve kararı yürürlüğe konmuştur.²⁵ Fakat bu çerçeve kararı her ne kadar Avrupa Konseyi'nin oluşturduğu sözleşmeye dayandırılmış olsa da, çerçeve kararı daha kısıtlı konularda düzenlemelere yer vermiştir.

Bu iki Avrupa hukuku belgesinin kısa süre önce yürürlüğe giren 41. Ceza Kanununda Değişiklik Kanunu ile iç hukukuna uyarlanması, Avrupa hukukunun internet ceza hukuku alanında görülen ilk etkisi olduğu söylenemez. Avrupa Topluluklarının üye devletlerindeki internet sunucularının sorumluluklarını uyumlaştırmak isteyen yönergeye²⁶ dayanan 20 Aralık 2001 tarihli Elektronik Ortamda Gerçekleştirilen Ticari İşlemlerin Hukuksal Çerçeve Koşullarına İlişkin Kanun'da (Elektronik Ortamda Ticari İşlemler Kanunu; EGG)²⁷ yapılan değişiklik ile internet sunucularının sorumlulukları değişmiştir. Bunun dışında bilgisayar dolandırıcılığının cezalandırılabilirliği hazırlık

²³ Ceza Hukukuyla ilgili genel olarak *Hecker*, *Europäisches Strafrecht*, 2. Aufl., Berlin/Heidelberg 2007; *Satzger*, *Die Europäisierung des Strafrechts*, Köln 2001; *Valerius* in: *BeckOK-StGB* (Dipnot 10), *Lexikon des Strafrechts: Europäisches Strafrecht*; *Dannecker*, *Jura* 2006, 95; *Eisele*, *JA* 2000, 991, 992 ff.; *Hecker*, *JA* 2007, 561, 562 ff.

²⁴ Bkz. Dipnot 17.

²⁵ Bkz. Dipnot 18.

²⁶ Richtlinie 2000/31/EG des Europäischen Parlaments und des Rates über den elektronischen Geschäftsverkehr vom 8. Juni 2000 (ABl. EG Nr. L 178 vom 17. Juli 2000, S. 1).

²⁷ BGBl. I, S. 3721.

aşamasına kadar genişletilmiş olması, Avrupa Birliği Konseyi'nin başka bir çerçeve kararına²⁸ dayanmaktadır.

Birçok ülkenin ortak bir hukuk düzenini oluşturuyor olmaları, kabul edilen her düzenlemenin sadece en alt seviyede ortak noktada buluşmalarını ve birçok soruları açık bırakmalarını beraberinde getirmektedir. Bu durum özellikle Avrupa Birliği Konseyi'nin çerçeve kararlarında olduğu gibi, üye ülkelerin kendi iç hukukuna uyarlama zorunluluğu olduğu durumlarda da ortaya çıkmaktadır. Somut bir örnek vermek gerekirse, internet ortamında ırkçı söylemlere karşı önlem alma konusunda, ne Avrupa Birliği Konseyi'nin çerçeve kararında ne de Avrupa Konseyi sözleşmesinde, eşitlik sağlanamamıştır. Avrupa Konseyi, Siber Suç Sözleşmesi'ne ek olarak²⁹ çok daha az sayıda ülkeler tarafından kabul edilen bir protokol hazırlamıştır.

Siber Suç Sözleşmesi açıkça takdire değerdir ve gelecek vaad etmektedir, ancak ne uluslararası devletler topluluğu için ne de ulusal kanun koyucu için, verdikleri çabanın son durağı olmamalıdır. İnternetin getirmiş olduğu tehlikeler karşısında anında harekete geçebilmek için, ülkeler, diğerleriyle birlikte başlanan yolda ilerlemekle yetinmeyip, gerektiğinde tek başında önlemler alabilmelidir. Alman kanun koyucusunun bu yönde olmayan çabalarına güncel bir örnek olarak, internet sunucularının cezai sorumluluklarını değiştirilmeden aynen aktardığı 26 Şubat 2007 tarihli Yeni Medya Yoluyla Haberleşme Yasasını³⁰ burada örnek olarak göstermek mümkündür. Son yıllarda bağlantı linkleriyle ilgili cezai sorumluluk gibi bir çok konuda sorunlu alanlar olmasına rağmen, Alman kanun koyucusu var olan düzenlemeleri aynen aktarmakla yetinmiştir. Bir değişikliğin yapılması gerektiği konusunda her ne kadar karşı çıkmamış olsa da kanun koyucu yakın zamanda çıkarılacak olan Avrupa Komisyonunun Gelişme Raporunu³¹ da göz ardı ederek, herhangi bir harekette bulunmamıştır. Bu da avrupalılaştırma yolunda kanun koyucunun bu konuda sınıfta kaldığını göstermektedir.

²⁸ Bkz. Dipnot 15.

²⁹ 28 Ocak 2003 tarihli Avrupa konseyi Siber suç sözleşmesine internet ortamında ırkçı söylemlere karşı önlem alma konusundaki ek protokol (SEV Nr. 189).

³⁰ Bir takım elektronik enformasyon ve iletişim hizmetleriyle ilgili düzenlemelerinin uyumlaştırılması hakkındaki kanunu (Elektronischer- Geschäftsverkehr- Vereinheitlichungsgesetz; ElGVG); BGBl. I, S. 179.

³¹ BT-Drs. 16/3078, S. 11.

C. Mahkeme kararlarında İnternet Ceza Hukuku

I. "CompuServe" Davası

Tebliğimin ikinci ana bölümünde bir kaç örnek karardan bahsedeceğim. Bu alandaki örnek kararlarda kısmen Almanya dışında da yankı yapan önemli hususlar gözlemlenmektedir. "CompuServe" ya da davalının ismiyle de bilinen Somm davası Alman ceza mahkemelerinde görülen ve internetle ilgili ilk olağanüstü davadır.

Felix Somm, Amerikan Birleşik Devletlerinde kurulmuş olan CompuServe Incorporated'in (ileride CompuServe ABD diye bahsedilecek) şubesi olarak faaliyet gösteren ve Almanya'da internet erişimini sağlayan sistemin pazarlığını yapan CompuServe GmbH (ileride CompuServe Almanya diye bahsedilecektir) şirketinin yöneticisidir. CompuServe ABD kendi ülke topraklarında haber gruplarının kaydedildiği bir kaç server işletmekteydi. Bu gruplardan bir kaçında çocuk pornografisi içerikli resim dosyaları üçüncü şahıslar tarafından yüklenmiş bulunmakta olup, herkes tarafından (Almanya'dan da) görüntülenebilmekteydi. CompuServe ABD için ilgili haber gruplarını kapatmak ve içeriklerini silmek bir sorun teşkil etmezken CompuServe Almanya'nın doğrudan sunuculara ulaşması mümkün olmayıp sadece ilgili belgeleri bildirip kapatılmasını ve silinmesini talep edebilmektedir.

Bu durum karşısında Münih Yerel Mahkemesinin 28 Mayıs 1998 tarihinde vermiş olduğu kararla Felix Somm, pornografik içerikli belgelerin yayılması suçuna iştirak etmekten, iki yıl şartlı hapis cezasına³² çarptırıldı. Mahkeme vermiş olduğu bu kararla CompuServe Almanya'nın internet erişimini sağlayan, kendisine ait bir müşteri kitlesine sahip olmadığı gerekçesine dayanan ve erişim sağlayıcıya imtiyazlı sorumluluk hakkı tanıyan Tele Hizmetler Kanunu'nun 5/3 maddesinin uygulanmasını kabul etmemiştir. CompuServe Almanya ile CompuServe ABD iki farklı şirket olarak ele alınmış olsa da CompuServe Almanya'yı ayrı bir yer sağlayıcı olarak kategorize edilmiştir. Bu noktada CompuServe ABD'nin yasadışı içerikli belgelerin saklanması sağlanmasının ve onları silmenin sadece kendi imkanı dahilinde olduğunun bir önemi kalmamıştır. CompuServe Almanya'ya hem internet sunucusu statüsü verilmiştir hem de aslında CompuServe ABD'nin imkanı dahilinde olan ilgili sayfaları silme sorumluluğu da yüklenmiştir. Ceza mahkemesi hakiminin ulaştığı sonuca göre, CompuServe Almanya bir yer sağlayıcı olup, Tele Hizmetler Kanunu'nun 5/3 maddesi uyarınca cezayı hafifleten sebeplerinin bulunmamasından dolayı kaydedilen pornografik içerikli sayfalardan CompuServe Almanya sorumludur.

³² AG München NJW 1998, 2836 mit Anmerkung *Hoeren*, NJW 1998, 2792; MMR 1998, 429 mit Anmerkung *Sieber*; CR 1998, 500 mit Anmerkung *Moritz*; K&R 1998, 406 mit Anmerkung *Eichler*.

Verilen karar, bilgisayar ve internet alanında ve hukuk dünyasında haklı olarak tepkilere yol açmıştır. Sadece kısaca değindiğimiz kararın gerekçe kısmının hukuki dayanaklardan uzak olması değil, aynı zamanda da davanın her aşamasında yapılan hatalar, şüphe uyandırmaktadır. Kaldı ki adli mercilerin yürütmüş olduğu soruşturma aşaması, gerekçesi hukuken kabul edilebilir olsa dahi, daha önce hiç bir suç işlememiş birisi için verilmiş olan cezanın çok yüksek olması ve savcının dahi, duruşma sırasında savunma makamının getirilen argümanlar ve bilirkişi raporları neticesinde fikrini değiştirmiş olmasından sonra, beraat talep etmiş olmasına rağmen mahkumiyet kararı verilmiştir. Alman ticaret anlayışı ile Alman adalet sisteminin imajı bundan dolayı zarar görmüştür ve kararın, Münih Eyalet Mahkemesi tarafından 17 Kasım 1999³³ tarihinde bozulmuş olması da bu zararı tamamen telafi edememiştir.

II. “Toebeben” Davası

12 Aralık 2000 tarihinde Federal Yüksek Mahkeme’nin, “Toebeben” davasında vermiş olduğu karar³⁴ benzer tepkilere yol açmıştır. Avustralya vatandaşı olan Toebeben, herkes tarafından erişilebilir bir web sayfasında nasyonal sosyalist rejiminin Yahudi vatandaşlarına yapmış olduğu soykırımın gerçekleşmediğine dair fikirleri içeren İngilizce makaleler yayınlamıştır. Bu makaleleri Avustralya’da bulunan bir server üzerinden yayınlamış, dünyanın her yerinden, dolayısıyla Almanya’dan da yayınları görüntülenebilmektedir.

Federal Yüksek Mahkeme kararında davalıyı Al.CK. § 130/1 ve 3 uyarınca ırkçı söylemlerinden yargılamıştır. Bu eylemle suç unsurunun oluşmuş olduğu tartışılmaz olmakla birlikte, Al.CK.’nin internetteki yayınlarda hangi koşullarla uygulanıp uygulanamayacağı konusu problemlidir. Mahkemenin görüşüne göre Al.CK.’nin uygulanabilirliğinin hukuki dayanağı, söz konusu internet yayınlarının Almanya’nın acılı tarihi ve benzeri görülmemiş soykırımla ilgili ırkçı propaganda içermesidir.³⁵

Kararının sonuçları oldukça endişe vericidir. Eğer yabancı server kaynaklı internet yayınlarının içeriklerine Al.CK. uygulanabiliyorsa, Alman adli mercilerinin Alman ceza hukuku düzenlemelerini dünya çapında bir ölçek³⁶ olarak temel alarak internetteki tüm yayınları denetleme hakkına sahip olduğu sonucu çıkarılabilir. Kendi kültürel değerlerinin tüm değerlerin üstünde gösterilmiş olmasını ve bunun diğer tüm ülkelerin

³³ LG München NJW 2000, 1051 mit Anmerkung *Kühne* NJW 2000, 1003; MMR 2000, 171; CR 2000, 117 mit Anmerkung *Moritz*; K&R 2000, 193 mit Anmerkung *Barton*.

³⁴ BGHSt 46, 212. Eingehend zum Fall Toebeben *Körber*, Rechtsradikale Propaganda im Internet. Der Fall Töben, Berlin 2003.

³⁵ BGHSt 46, 212 (220 ff.).

³⁶ *Hilgendorf/Frank/Valerius* (Dipnot 5), Rn. 249 ff.; *Hilgendorf*, NJW 1997, 1873 (1878); *Koch*, GA 2002, 703 (707); *Lagodny*, JZ 2001, 1198 (1200).

değerlerine ve hukuk sistemine yapılmış bir saygısızlık olmasını bir yana bırakacak olursak, kararın sonuçları, özellikle diğer ülkelerin, kendi ulusal ölçütlerinin tüm dünyada geçerli olduğunu deklere etmeleri halinde büyük sorunlar doğuracaktır. İnternette yayınlanan sayfaların her ülkede kabul edilebilir seviyede içeriklere sahip olmadığı sürece, bir web sayfası sunucusu her zaman bir yaptırımın uygulanacağı tehlikesiyle karşı karşıya kalacaktır. Bu nedenle hukuk dünyası bu kararı kabul etmemiştir ve dış ülkeler bu karara anlam verememiştir.

III. İnternette Çocuk Pornografisi

Son olarak etkisini ülke çapında göstermiş olan internet ceza hukuku alanında iki karara daha değinmek istiyorum. Federal Yüksek Mahkeme 27 Haziran 2001 tarihinde, çocuk pornografisi içeren belgelerin internette yayınlanmasının cezalandırılabilirliğini karara³⁷ bağlamıştır. Vermiş olduğu kararın gerekçesinde, davanın hukuki değerlendirilmesini de etkileyecek olan bazı teknik belirsizlikler mevcuttur. Şöyle ki, sunulan verilerle, verilerin yüklendiği alan arasındaki ayırım, yani (soyut olan) içerik ile bu içeriğin yüklendiği (somut olan) içerik taşıyıcısı, yani veri tabanı arasındaki fark yeteri kadar belirgin değildir. Bu ayırım Al.CK.'nda bir gelenek olarak kabul görmüştür ve her türlü ifade suçlarında uygulama alanı bulan Al.CK. § 11/3 ile de pekiştirilmiştir. Kaydedilmiş her türlü resim, ses ve veri dosyaları ve veri tabanı bu maddeye göre yazılı bir metindir ve her şekliyle somut bir nesne olduğu kabul edilmektedir. Buna ek olarak ifade suçu oluşturan fiillerde genelde “dağıtım” ile “erişilebilir hale getirme” arasında ayırım yapılmaktadır. Dağıtımda metnin (somut olarak) elden ele verilmesi gerekmektedir, yazılı metnin erişilebilir hale getirilmesinde ise somut bir fiil gerekmemektedir ve sadece erişilebilir olması yeterlidir.

Mahkeme vermiş olduğu kararın gerekçesinde, verilerin de (bu durumda dijital fotoğrafların) Al.CK. § 11/3'e göre, bir veri tabanı olarak tanımlayarak içerik ile içerik taşıyıcısı yani veri tabanı arasındaki farkı ortadan kaldırmıştır. Bu farkın ortadan kalkması, suçu oluşturan fiilin, dağıtım şeklinde gerçekleştirildiği hususuna da etki etmektedir. Mahkeme, verilerin somut olarak elden ele dağıtılması mümkün olmadığına göre, dağıtım teriminin internette gerçekleştirilen fiillere uymadığını ve somut olma şartını geçersiz sayarak, anlamının genişletilmesi gerektiğini savunmaktadır. Spesifik anlamda dağıtım fiili bir belgenin internet kullanıcısı tarafından erişilebilir olması halinde tamamlanması yerterli olacaktır.³⁸

³⁷ BGHSt 47, 55.

³⁸ BGHSt 47, 55 (59).

Mahkemenin haklı olarak eleştirilere³⁹ uğramış olan ve genelde kabul gören görüşten tamamen ayrılan bu anlayışı, bize neyi göstermektedir? Öncelikle zamanında bilgisayar ve internetin gizemli birer yabancı araç olduğu sonra, veri ile veri tabanı arasındaki farkın gözetilmediğinden de anlaşıldığı üzere, bilgisayar ve internetin ne şekilde çalıştığı konusu da mahkeme heyeti tarafından pek bilinmemekteydi. Bu iki bilinmeyen husus, ürkütücü gelmiş olmalı ya da en azından şüpheyle yaklaşılmalı gerekir ki, yoksa Federal Mahkemenin içeriği erişilebilir hale getirmekle, içerik sağlayıcının dağıtımındaki geleneksel farkı, gerekli olmasına rağmen, gözardı etmiştir. Sonuçta sanık, içeriğin erişilebilir hale getirmiş olmaktan aynı yaptırımla karşılaşacaktı ve Mahkeme dağıtım terimiyle hiç bu kadar uğraşmak durumunda kalmayacaktı. Yine de bu şekilde uğraşmış olmasının göz boyama şeklinde bir hareket niteliğinde olduğu kesindir, özellikle de bu heyetin altı ay önce geniş çapta tepkilere yol açan “Toebe” davasında karar veren heyet olması dikkate alındığında.

IV. İnternette Online-Gösteriler

En son örnek karar ise internette online gösterilerle alakalıdır. Davalı Lufthansa A.Ş.’nin oturum izni olmayan kişilerin sınırdışı edilmesindeki katkılarını protesto etmek amacıyla bir “Cyber-Sit-In” çağrısında bulunulmuştur. Lufthansa A.Ş.’nin iki saatlik Genel Kurul toplantısının yapıldığı günde özel bir program aracılığıyla web sayfası o kadar fazla yüklendi ki webserver işlem kapasitesini aştı ve potansiyel müşterilerin istekleri cevapsız kaldı. Bu şekilde gerçekleştirilen “servis kullanımını engelleme saldırısı” neticesinde Lufthansa’nın önemli bir imaj kaybına uğramasının yanı sıra 48.000 Avro değerinde maddi bir kayba da uğramıştır.

Frankfurt am Main Sulh Mahkemesi, siber oturum eylemini, Al.CK. § 240/1 gereğince Al.CK. § 111’de belirtilen suça teşvik nedeniyle 1 Temmuz 2005 tarihinde⁴⁰ davalıya 90 gün hapse tekabül eden para cezasına mahkum etmiştir. Kararda gerçekleştirilen bu servis kullanımını engelleme saldırısının, teknik açıdan cezaya tabi tutulması hiç irdelenmemiştir. Frankfurt am Main Yüksek Eyalet Mahkemesi 22 Mayıs 2006 tarihinde⁴¹ kararı bozarak davalıyı serbest bırakmıştır. Almanya’da her ne şekilde olursa olsun bir oturum eyleminin cezalandırılmasına rağmen, Mahkeme yapılan fiilin oturum eylemine teşvik olmadığını ve Al.CK. § 303a ve diğer ilgili maddeleri gereğince

³⁹ *Hilgendorf/Frank/Valerius* (Dipnot 5), Rn. 412 ff.; *Gercke*, MMR 2001, 678; *Kudlich*, JZ 2002, 310; *Lindemann/Wachsmuth*, JR 2002, 206.

⁴⁰ AG Frankfurt am Main MMR 2005, 863 mit Anmerkung *Gercke*.

⁴¹ OLG Frankfurt am Main MMR 2006, 547 mit Anmerkung *Gercke*.

de bilgisayar sabotajı veya veri değiştirilmesi şeklinde bir suçun da söz konusu olmadığına karar vermiştir.

Her iki karar birbiriyle son derece çelişmektedir. İlk derece mahkemenin, bir gösteri şeklinin özelliklerini sadece kısaca ele alırken, ikinci derece mahkemesi bu hususu ayrıntılarıyla incelemiştir. Yine ilk derece mahkemesi siber oturum eyleminin teknik yanına hiç değinmemesine karşın, Yüksek Eyalet Mahkemesi burada da ayrıntılı bir incelemeyi seçmiştir. Yerel Mahkeme davalıya bir yaptırımın uygulanması gerektiğini savunurken Yüksek Eyalet Mahkemesi her ne pahasına olursa olsun bir cezanın öngörülmesini engellemeye çalışmış gibi görünmektedir. Bu anlamda Yüksek Eyalet Mahkemesinin vermiş olduğu kararın gerekçesi eleştirilebilse de,⁴² internet ortamında gerçekleştirilen sosyal içerikli davranışları gerekli hassasiyeti göstererek detaylarla inceleme yapmış olması olumlu karşılanmalıdır.

V. Özet

Örnek olarak sunmuş olduğum bu kararlar, yeni bir enformasyon ve iletişim aracı olarak internetin içtihat tarafından henüz sağlam zeminlere oturtulmadığının göstergesidir. Çoğu zaman internetin işleyişiyle yapısı, uzman mahkemelerde sorun teşkil etmektedir ve mahkemelerin ortaya çıkan bu durumdan meydana gelen yeni güçlükleri bir alt kategoride toplamak yerine, şimdiye kadar ne dijitalleştirilmiş ne de ağ bağlantısına sahip olan dünyanın var olan hukuki temel ilkelerini bırakmalarını, değiştirmelerini ya da genişletmelerini istemektedirler. Bu arada internet uzunca bir süre yapılan nitelermeye rağmen yeni bağımsız ya da görsel bir dünya olmayıp varolan gerçek dünyanın bir parçasıdır.

Dogmatik problemleri bir tarafa bırakacak olursak, içtihat ile internet arasında karşılıklı olarak tamamen önyargılardan arınmış bir ilişki bulunmamaktadır. Bu zamana kadar içtihat, internete ve internetin kötüye kullanımına elverişliliği karşısında şüpheyle yaklaşmakta ve bu da içtihatların içeriğine ve gerekçesine yansımaktaydı. Frankfurt am Main Yüksek Eyalet Mahkemesinin vermiş olduğu karar bu anlamda sevindiricidir, fakat amacını aşarak sanığın cezalandırılması gereğini somut olayda kaldırılmasını kabul etmemektedir. Bu karar içtihatla, eğilimin farklı yönde geliştiğinin bir göstergesidir ve bundan sonra sorunlara çözüm getirecek kararlarının verileceği yönünde umut vermektedir.

⁴² Ayrıntılar için bkz.: *Valerius*, in: Hilgendorf (Hg.), Dimensionen des IT-Rechts, Berlin 2008, S. 19 ff. Zur Thematik auch *Eichelberger*, DuD 2006, 490; *Kitz*, ZUM 2006, 730; *Klutzny*, RDV 2006, 50; *Kraft/Meister*, K&R 2005, 458.

D. Sonuç

İnternet ceza hukuku, Almanya'da hem çok sayıdaki yasama faaliyetine hem de her zaman tartışmasız olmayan sayısız karara neden olan bir hukuk alanı niteliğindedir. Yasama ve içtihadın bu alanda gerekenleri geniş ölçüde yerine getirmiş olmalarına rağmen, gelecekte sürekli gelişmenin getirdiği birçok yeni güçlükler bulunmaktadır ve bunlar, iletişim araçlarının birbirine yaklaşmasından, internetteki yeni saldırı formlarının ceza hukukunca ele alınmasına kadar olan ve haberleşme ağlarının işletilmesi gibi teknik temeldeki değişikliklerle başlamıştır.

Kim bu güçlükleri çözmek isterse, somut olaydaki cezalandırılabilirliğe bakmak ve genelleştirilmeye yatkın ve mümkün olduğunca somut davranışın ortaya konulan teknik özelliklerinin sürekli değişiminden bağımsız bir biçimde kurala bağlamak zorundadır. Girişte belirtilen, hukuk biliminin alt disiplin olan internet ceza hukuku, gelecekteki eleştirel, ama çözüme yönelik yeni kanunlar ve yeni içtihatlarla bu konuda önemli bir katkıda bulunabilir ve aynı zamanda Almanya'da internet ceza hukukunun anlam ve önemini yükseltebilir.