HUMBOLDT FORUM RECHT
- Die juristische Internet-Zeitschrift an der Humboldt-Universität zu Berlin -

HFR 11/2006 ISSN 1862-7617 Wettbewerb

Professor Dr. Bernd Heinrich, Berlin

Aktuelle Probleme des Internetstrafrechts

Seit Anfang der neunziger Jahre entwickelte sich das Internet als weltweit und von jedem benutzbares neues Informations- und Kommunikationsmedium. Als Teildisziplin des Computerrechts formte sich daraufhin auch das Internetrecht sowie das Internetstrafrecht zu einem eigenen Rechtsgebiet. Letzteres zeichnet sich insbesondere dadurch aus, dass die verschiedenen neu auftretenden Problemkonstellationen (jedenfalls derzeit noch) mit den bisher vorhandenen Straftatbeständen gelöst werden müssen. Anhand mehrerer aktueller Problemfelder weist der Autor nach, dass dies durchaus möglich ist und an den Stellen, an denen sich Strafrechtslücken auftun, ein echtes Strafbedürfnis oftmals nicht existiert. Behandelt werden im Einzelnen: die rechtswidrige Erlangung von Daten (durch "Phishing", "Trojanische Pferde", "Brute-Force-Attacks" und "social engeneering"), Urheberrechtsverletzungen im Internet (insbesondere der Download urheberrechtlich geschützter Werke im Zuge so genannter "Tauschbörsen" und die Verwendung von urheberrechtlich geschützten Werken auf eigenen Web-Seiten), die Verabredung von Straftaten über das Internet und Sabotagehandlungen durch Ressourcenüberlastung ("E-Proteste" und "DDos-Attacken").

I. Begriffsbestimmung: Internetstrafrecht

1 Neue technische Entwicklungen bringen zumeist eine Vielzahl neuer rechtlicher Probleme mit sich. Zugleich lässt sich die Tendenz feststellen, dass neben den Erleichterungen, die technische Neuerungen dem einzelnen Menschen bescheren, sich alsbald auch Personen finden werden, welche die neuen technischen Möglichkeiten missbrauchen, um persönliche Vorteile hieraus zu ziehen, die ihnen nicht zustehen. Hierdurch kann der soziale Frieden in einer Weise gestört werden, dass der Ruf nach dem Strafrecht laut wird. Dabei stellt sich regelmäßig die Frage, ob die bestehenden Strafvorschriften ausreichen, die neuen Formen des Unrechts zu erfassen, oder ob der Gesetzgeber dazu aufgerufen ist, neue Straftatbestände zu schaffen. So hat die Erfindung des „Computers" nicht nur das Leben der Menschen in vielen Bereichen entscheidend verändert (und bereichert), sondern auch mit dem Bereich des „Computerrechts" ein ganz neues Rechtsgebiet eröffnet[1]. Dies wirkte sich auch auf das Strafrecht aus, da schon bald deutlich wurde, dass die geltenden Bestimmungen zwar viele, jedoch bei weitem nicht sämtliche Erscheinungsformen im Zusammenhang mit der Verwendung von Computern und elektronisch gespeicherten Daten erfassen konnten. Daher wurden durch das 2. WiKG[2] im Jahre 1986 mit den §§ 202a, 263a, 269, 303a, 303b StGB neue computerspezifische Straftatbestände ins StGB eingefügt. Inzwischen ist das Computer-[3] bzw. Multimediastrafrecht[4] auch als eigene Rechtsdisziplin anerkannt.

2 Seit Anfang der neunziger Jahre entwickelte sich das Internet als weltweit und von jedem benutzbares neues Informations- und Kommunikationsmedium. Als Teildisziplin des Computerrechts formte sich daraufhin auch das Internetrecht[5] zu einem eigenen Rechtsgebiet.

[1] Vgl. hierzu nur *Benning/Oberrath*, Computer- und Internetrecht, 2003; *Junker/Benecke*, Computerrecht, 3. Aufl. 2003; *Kilian/Heussen*, Computerrechtshandbuch, Loseblattsammlung, Stand: März 2005; *Nauroth*, Computerrecht für die Praxis, 2. Aufl. 1992; *Schneider*, Handbuch des EDV-Rechts, 3. Aufl. 2003; *Theis*, Computerrecht, 1997.
[2] Zweites Gesetz zur Bekämpfung der Wirtschaftskriminalität vom 15.5.1986, BGBl. 1986 I, S. 721.
[3] Vgl. hierzu nur *Hilgendorf/Frank/Valerius*, Computer- und Internetstrafrecht, 2005; *Marberth-Kubicki*, Computer- und Internetstrafrecht, 2005.
[4] Vgl. hierzu nur *Barton*, Multimedia-Strafrecht. Ein Handbuch für die Praxis, 1999.
[5] Vgl. hierzu nur *Benning/Oberrath*, Computer- und Internetrecht, 2003; *Härting*, Internetrecht, 2. Aufl. 2005; *Hoeren*, Grundzüge des Internetrechts, 2. Aufl. 2002; *Koch*, Internetrecht, 1998; *Köhler/Arndt*, Recht des In-

Auch bei der Benutzung dieses neuen Mediums zeigte sich schnell, dass es in vielfältigen Formen zu kriminellen Zwecken missbraucht werden konnte und auch missbraucht wurde. Erneut stellte sich die Frage, ob diese strafwürdigen Handlungen durch die bestehenden Strafvorschriften ausreichend geahndet werden können. Im Gegensatz zu den genannten computerspezifischen Straftatbeständen konnte dabei allerdings bislang auf die Schaffung eigener Straftatbestände verzichtet werden[6].

3 Wenn man heute vom „Internetstrafrecht"[7] spricht, muss man sich jedoch darüber im Klaren sein, dass es sich hierbei nicht um eine abgegrenzte Gruppe von Straftatbeständen, wie z.B. beim „Umweltstrafrecht" (§§ 324 ff. StGB) oder beim „Betäubungsmittelstrafrecht" (§§ 29 ff. BtMG) handelt. Vielmehr wird das „Internetstrafrecht", wie z.B. auch das „Arztstrafrecht", ausschließlich von seinem Gegenstand her definiert. Dabei werden aber die allgemeinen Straftatbestände – und eben keine Spezialtatbestände – zur Anwendung gebracht[8].

4 Da die einzelnen Probleme und Erscheinungsformen der Internetkriminalität vielschichtig sind, sollen im Folgenden nur einige der aktuellen und in ihrer rechtlichen Einordnung besonders umstrittenen Problemkonstellationen erörtert werden.

5 II. Aktuelle Problemkonstellationen

1. Die rechtswidrige Erlangung von Daten

a) „Phishing"

Unter „Phishing" versteht man die durch Täuschung herbeigeführte Erlangung fremder Daten, die im Internet als Identifikationsdaten verwendet werden können (Passwörter, PIN-Nummern, Kreditkartennummern, Accountdaten u.a.)[9]. Dabei kann das „Phishing", ein Kunstwort, welches aus den Namen „Password" und „Fishing" gebildet wurde, in mehreren Formen vorkommen. Üblicherweise erreicht den Internetnutzer eine E-Mail, die vermeintlich von seiner Bank oder einem sonstigen Vertragspartner stammt. In dieser wird er dazu aufgefordert, dem Absender sensible Daten, wie Passwörter oder Kreditkartennummern mitzuteilen, was durch die Rücksendung der E-Mail geschehen könne. Meist wird in der E-Mail angegeben, die Rücksendung diene der „Verifizierung" seiner Daten. Zu diesem Zweck (oder, besonders trickreich, mit der Argumentation, sich künftig besser gegen die Ausspähung seiner Daten schützen zu können), habe der Kunde ein (entweder im Anhang beigefügtes oder über einen in der E-Mail anzuklickenden Link erreichbares) Formular auszufüllen und zurückzusenden. In Wirklichkeit stammt die E-Mail von einem Täter, der mit der Bank bzw. dem Vertragspartner des Nutzers nichts zu tun hat, sondern eine falsche Identität vortäuscht, um die erlangten Daten zu kriminellen Zwecken verwenden zu können.

6 Insbesondere das Online-Banking ist vom „Phishing" betroffen[10]. Hier erlangt der Täter durch die Rücksendung der dem Nutzer von seiner Bank mitgeteilten Transaktionsnummer (TAN) die Möglichkeit, Banküberweisungen vom Konto des Betreffenden zu veranlassen. Während die spätere Veranlassung einer Banküberweisung durch die (unbefugte) Angabe einer fremden TAN den Straftatbestand des § 263a StGB unproblematisch er-

---

ternet, 4. Aufl. 2003; *Kröger/Gimmy*, Handbuch zum Internetrecht, 2. Aufl. 2002; *Strömer*, Online-Recht. Rechtsfragen im Internet, 3. Aufl. 2002.

[6] Geschaffen wurden lediglich Regelungen, welche die Strafbarkeit begrenzen, vgl. §§ 8 ff. Teledienstegesetz (TDG) und §§ 6 ff. Mediendienste-Staatsvertrag (MDStV).

[7] Vgl. hierzu nur *Hilgendorf/Frank/Valerius*, Computer- und Internetstrafrecht, 2005; *Malek*, Strafsachen im Internet, 2005; *Marberth-Kubicki*, Computer- und Internetstrafrecht, 2005; *Vetter*, Gesetzeslücken bei der Internetkriminalität, 2003.

[8] *Malek* (Fn. 7), Rn. 3.

[9] Vgl. zum „Phishing" *Hilgendorf/Frank/Valerius* (Fn. 3), Rn. 760 ff.; *Knupfer*, MMR 2004, 641; *Malek* (Fn. 7), Rn. 213; *Popp*, NJW 2004, 3517.

[10] *Malek* (Fn. 7) weist in Fn. 428 darauf hin, dass nach einer Mitteilung des hessischen Kriminalamtes allein im März 2004 ca. 200.000 solcher Phishing-E-Mails registriert wurden; weitere Zahlen bei *Popp*, NJW 2004, 3517.

füllt[11], ist die rechtliche Einordnung des bloßen „Abfischens" der Daten umstritten.

7 Zu denken ist hier in erster Linie an § 202a StGB, das „Ausspähen" von Daten. Diese Strafnorm setzt voraus, dass sich der Täter unbefugt Daten, die einerseits nicht für ihn bestimmt und andererseits gegen den unberechtigten Zugang besonders gesichert sind, verschafft. Dabei gelten als Daten (vgl. die Legaldefinition in § 202a Abs. 2 StGB) nur solche, die elektronisch, magnetisch oder sonst nicht unmittelbar wahrnehmbar gespeichert sind oder übermittelt werden. Die erste Alternative („gespeichert sind") scheidet im vorliegenden Zusammenhang regelmäßig aus, da sie voraussetzt, dass die ausgespähten Daten zuvor dauerhaft auf einem Datenträger fixiert wurden. Eine lediglich vorübergehende Speicherung im Arbeitsspeicher des Computers reicht hierfür nicht aus[12]. In den genannten Fällen des „Phishing" werden die eingegebenen Daten jedoch lediglich vom Tatopfer in das Formular eingegeben und – zumindest in der Regel – zuvor nicht dauerhaft, sondern nur vorübergehend im Arbeitsspeicher abgelegt[13].

8 Zu denken ist jedoch an die zweite Alternative des § 202a Abs. 2 StGB („übermittelt"). Dieses Merkmal soll gerade dazu dienen, Daten zu schützen, die sich in der Übermittlungsphase befinden[14]. Hierzu zählt auch die „Übermittlung" der Daten von der Tastatur in den Arbeitsspeicher des Computers[15]. Gibt das Tatopfer jedoch auf Aufforderung des Täters Daten in ein im Internet zur Verfügung stehendes Formular ein, welches er anschließend an den Täter in der irrigen Annahme übermittelt, es handle sich bei dem Empfänger um seine Bank bzw. seinen Vertragspartner, so greift der Täter gerade nicht in den Übermittlungsvorgang ein[16]. Denn die Daten werden vom Absender zielgerichtet an diejenige Adresse gesendet, an die er sie senden will. Insofern „verschafft" sich der Täter zwar die entsprechenden Daten dadurch, dass er durch die Täuschung des Absenders über die Identität des Empfängers die Verfügungsgewalt über die Daten erlangt[17], diese „Verschaffung" erfolgt jedoch – wenn auch täuschungsbedingt – mit Einverständnis des Absenders, der die Daten dem Täter hier ja gerade zielgerichtet übermittelt. Dies führt dazu, dass nach den Grundsätzen des tatbestandsausschließenden Einverständnisses bereits die Tatbestandsmäßigkeit des Verhaltens entfällt[18]. Konstruktiv kann dies entweder durch eine restriktive Auslegung des Merkmals „Sich-Verschaffen" (im Sinne von „gegen den Willen des Berechtigten" erfolgend), über das Merkmal „nicht für [den Täter] bestimmt" oder über das Merkmal „unbefugt" erreicht werden. Da das Merkmal des „Sich-Verschaffens" objektiv auszulegen und nicht vom Willen des Berechtigten abhängig gemacht werden sollte und das Merkmal „unbefugt" ein allgemeines Rechtswidrigkeitsmerkmal darstellt[19], ist der richtige Ansatzpunkt hier das Merkmal „nicht für [den Täter] bestimmt"[20]. Dabei kommt es dann – nach den Grundsätzen des tatbestandsausschließenden Einverständnisses – ausschließlich auf den „natürlichen Willen" des Absenders an, die entsprechenden Daten an die vorgesehene Adresse zu senden, die Motivation hierzu muss dagegen unbe-

[11] *Knupfer*, MMR 2004, 641 (642); Leipziger Kommentar zum Strafgesetzbuch (LK)-*Tiedemann*, 11. Aufl. 1992 ff., § 263a Rn. 56; *Malek* (Fn. 7), Rn. 213; Nomos-Kommentar zum Strafgesetzbuch (NK)-*Kindhäuser*, 2. Aufl. 2005, § 263a Rn. 57; *Popp*, NJW 2004, 3517 (3518); *Schönke/Schröder-Cramer/Perron*, Strafgesetzbuch, 27. Aufl. 2006, § 263a Rn. 14.

[12] *Frank* in: *Hilgendorf*, Informationsstrafrecht und Rechtsinformatik, 2004, S. 23 (32); *Hilgendorf/Frank/Valerius* (Fn. 3), Rn. 761; LK-*Tolksdorf* (Fn. 11), § 303a Rn. 4; *Welp*, CR 1992, 291 (293); a.M. *Hilgendorf*, JuS 1996, 509 (512); *Jessen*, Zugangsberechtigung und besondere Sicherung im Sinne von § 202a StGB, 1994, S. 53 f.; *Mühle*, Hacker und Computer-Viren im Internet, 1998, S. 63; Münchener Kommentar zum Strafgesetzbuch (MüKo)-*Graf*, 2003, § 202a Rn. 16; differenzierend *Schmitz*, JA 1995, 478 (480 f.).

[13] *Hilgendorf/Frank/Valerius* (Fn. 3), Rn. 761.

[14] *Hilgendorf/Frank/Valerius* (Fn. 3), Rn. 762.

[15] MüKo-*Graf* (Fn. 12), § 202a Rn. 16; *Hilgendorf/Frank/Valerius* (Fn. 3), Rn. 762.

[16] So im Ergebnis auch *Hilgendorf/Frank/Valerius* (Fn. 3), Rn. 762.

[17] *Tröndle/Fischer*, Strafgesetzbuch und Nebengesetze, 53. Aufl. 2006, § 202a Rn. 10.

[18] Vgl. hierzu (differenzierend) *Popp*, NJW 2004, 3517 (3518); zum tatbestandsausschließenden Einverständnis bei § 202a StGB auch LK-*Schünemann* (Fn. 11), § 202a Rn. 11, 18; MüKo-*Graf* (Fn. 12), § 202a Rn. 49, 52; a.M. *Tröndle/Fischer* (Fn. 17), § 202a Rn. 12, der hierin lediglich eine Einwilligung des Berechtigten sieht, die infolge der Täuschung unbeachtlich ist.

[19] *Schönke/Schröder-Lenckner* (Fn. 11), § 202a Rn. 11; *Tröndle/Fischer* (Fn. 17), § 202a Rn. 12.

[20] So auch *Schönke/Schröder-Lenckner* (Fn. 11), § 202a Rn. 11.

achtlich bleiben[21]. Zum gleichen Ergebnis kommt man mit Blick auf die amtliche Überschrift des § 202a StGB. Denn ein „Ausspähen" von Daten liegt dann nicht vor, wenn der Betroffene selbst dem Täter die erwünschten Daten durch die Rücksendung zur Verfügung stellt. Die Tatsache, dass der Absender über den tatsächlichen Empfänger getäuscht wird, ändert nichts daran, dass es sich bei der Absendung der Daten um einen freiwilligen Akt des Absenders handelt[22]. Schließlich kann in den genannten Fällen auch nicht davon gesprochen werden, dass der Täter – wie es der Tatbestand des § 202a StGB fordert – Daten erlangt, die gegen „unberechtigten Zugang besonders gesichert sind". Denn auch hier ist entscheidend, dass das Opfer die Daten ja gerade zielgerichtet – wenn auch täuschungsbedingt – an den Empfänger absendet, der zur Erlangung somit keine „Sicherung umgehen" oder fremde Übermittlungsvorgänge „anzapfen" muss[23]. Im Ergebnis scheidet daher eine Strafbarkeit nach § 202a StGB aus[24].

9 Ferner kann allein in der Aufforderung an den Nutzer, die sensiblen Daten zurückzusenden, noch kein Versuch des § 263a StGB (im Hinblick auf die später mittels der Daten veranlassten Kontobewegungen) gesehen werden[25]. Es fehlt hier an einem „unmittelbaren Ansetzen zur Tatbestandsverwirklichung" (§ 22 StGB), da das Erfragen der Daten, das spätere Übermitteln der Daten und vor allem die anschließende Überweisung unter Angabe der TAN zeitlich regelmäßig auseinander fallen. Die Vornahme der späteren Überweisung erfordert zudem einen neuen Willensentschluss, weshalb die verschiedenen Handlungen keinen einheitlichen Lebensvorgang darstellen.

S. 127

10 Fraglich ist somit lediglich, ob in der täuschungsbedingten Absendung der sensiblen Daten die Vollendung eines Betruges, § 263 StGB, gesehen werden kann. Wie bei der Erörterung des § 202a StGB gezeigt, liegt der Schwerpunkt der Tathandlung hier nicht in einem Eingriff in technische Schutzmaßnahmen, sondern in der Täuschung des Tatopfers über den wahren Empfänger (und seine Absichten). Durch diese Täuschung unterliegt der Absender einem entsprechenden Irrtum (er denkt, er sende die Daten an seine Bank bzw. seinen Vertragspartner). Um zu einer Betrugsstrafbarkeit zu gelangen, müsste nun aber in der Absendung der Daten an den Täter eine „Vermögensverfügung" zu sehen sein, die als ungeschriebenes Tatbestandsmerkmal des Betruges in § 263 StGB hineinzulesen ist. Unter einer Vermögensverfügung ist ein Handeln, Dulden oder Unterlassen zu verstehen, welches tatsächlich auf das geschützte Vermögen einwirkt[26]. Der Täter erlangt durch die Kenntnis der sensiblen Daten die Möglichkeit, Vermögensdispositionen im Hinblick auf das geschützte Vermögen des Opfers vorzunehmen. Insoweit wird bereits durch die Offenbarung der Daten das Vermögen des Tatopfers gefährdet (es hängt nunmehr lediglich noch vom Täter ab, ob und wann er die entsprechende Überweisung veranlasst). Fraglich ist jedoch, ob in dieser Gefährdung bereits ein Vermögensschaden zu erblicken ist. Zwar wird die Rechtsfigur der „schadensgleichen Vermögensgefährdung" im Rahmen des § 263 StGB weithin anerkannt[27] und hierin ein Vermögensschaden erblickt. Die Grenzen sind jedoch fließend. Im Ergebnis ist hier eine restriktive Auslegung geboten, da eine Ausweitung dieser Rechtsfigur zu einer Vorverlagerung der Betrugsstrafbarkeit führen und eine zu weitgehende Anerkennung einer Vermögensgefährdung als Schaden den Betrug contra legem von einem Verletzungsdelikt in ein Gefährdungsdelikt umgestalten würde. Schon von daher ist jedenfalls in denjenigen Fällen, in denen der Täter durch eine Handlung im

---

[21] Vgl. zum tatbestandsausschließenden Einverständnis und die Behandlung eines diesbezüglichen Irrtums *Heinrich*, Strafrecht Allgemeiner Teil Band I, 2005, Rn. 440 ff.
[22] *Frank* in: *Hilgendorf* (Fn. 12), S. 23 (33); *Hilgendorf/Frank/Valerius* (Fn. 3), Rn. 762; a.M. wohl *Knupfer*, MMR 641 (642), der davon ausgeht, § 202a StGB verlange nur, dass objektiv ein besonderes Zugangshindernis bestehe, auf die Frage, wie dieses überwunden werde, komme es nicht an, sodass auch eine täuschungsbedingte Weitergabe durch den Berechtigten hier erfasst sei.
[23] So auch *Hilgendorf/Frank/Valerius* (Fn. 3), Rn. 763.
[24] *Frank* in: *Hilgendorf* (Fn. 12), S. 23 (33); *Hilgendorf/Frank/Valerius* (Fn. 3), Rn. 760 ff.; differenzierend *Popp*, NJW 2004, 3517 (3518); vgl. auch *Jessen* (Fn. 12), S. 197; a.M. *Knupfer*, MMR 2004, 641 (642); *Tröndle/Fischer* (Fn. 17), § 202a Rn. 12.
[25] *Malek* (Fn. 7), Rn. 213; vgl. auch *Schönke/Schröder-Cramer/Perron* (Fn. 11), § 263a Rn. 21.
[26] *Schönke/Schröder-Lenckner/Perron* (Fn. 11), § 263 Rn. 55.
[27] Vgl. BGHSt 21, 112 (113); BGHSt 23, 300; *Schönke/Schröder-Lenckner/Perron* (Fn. 11), § 263 Rn. 145.

Vorfeld sich erst die Möglichkeit verschafft, später durch einen deliktischen Akt auf das Vermögen des Tatopfers zuzugreifen, in der Vorbereitungshandlung noch kein strafbarer Betrug zu sehen, da die Vermögensschädigung erst im tatsächlichen Zugriff auf das Vermögen zu sehen ist[28]. Dies ergibt sich ferner aus einer weiteren Überlegung. Im subjektiven Bereich muss der Täter die Absicht haben, sich durch die Tathandlung unmittelbar zu bereichern. An dieser Unmittelbarkeit fehlt es in denjenigen Fällen, in denen der Schaden erst durch einen weiteren deliktischen Akt eintreten soll, der durch den Täuschungsakt lediglich vorbereitet wird[29]. Auch insoweit ist eine Tatbestandserfüllung also nicht gegeben. Im Ergebnis stellt daher das „Abfischen" des Passworts lediglich eine insoweit straflose Vorbereitungshandlung dar. Durch die Erlangung der sensiblen Daten ist daher keine Strafbarkeit wegen Betruges begründet[30].

11 Letztlich ließe sich noch daran denken, bereits im Zusenden der E-Mail eine strafbare Handlung nach § 269 StGB (Fälschung beweiserheblicher Daten) zu sehen[31]. Denn die E-Mails erwecken beim Empfänger den Eindruck, als habe sich seine Bank oder ein sonstiger Vertragspartner auf Grund des bestehenden Vertragsverhältnisses an ihn gewandt. Dann aber müsste die E-Mail im Rechtsverkehr wie eine Urkunde anzusehen sein. Bei Wahrnehmung der Daten – etwa in Form eines Briefes – müsste also eine unechte Urkunde vorliegen, die vom Täter zur Täuschung im Rechtsverkehr hergestellt und an den Empfänger übersandt wurde. Dies ist jedoch zweifelhaft. Zwar würde ein entsprechendes Schreiben den Eindruck erwecken, als wäre es von der Bank oder einem sonstigen Vertragspartner abgesandt worden, sodass sowohl eine verkörperte Gedankenerklärung als auch eine Ausstellererkennbarkeit vorliegen. Fraglich ist jedoch, ob ein solches Schreiben, in welchem der Empfänger lediglich von seiner Bank aufgefordert wird, ihr zur Überprüfung gewisse Unterlagen zu übersenden bzw. seine Geheimnummern zu nennen, den Beweis für eine rechtlich erhebliche Tatsache erbringen soll. An dieser „Beweisfunktion" dürfte es aber regelmäßig fehlen, da durch das Schreiben weder rechtsverbindlich erklärt wird, dass eine vertragliche Beziehung besteht, noch der Kunde zu einem bestimmten Verhalten (eventuell unter Androhung von Sanktionen) rechtsverbindlich bestimmt werden soll. Vielmehr läge hierin lediglich eine unverbindliche Aufforderung, Überprüfungsmaßnahmen zu ermöglichen. Damit könnte ein solches Schreiben aber keinen „Beweis" für eine rechtserhebliche Tatsache liefern und wäre insoweit nicht als Urkunde anzusehen. Dann aber muss auch eine Strafbarkeit nach § 269 StGB ausscheiden. Eine solche kommt lediglich dann in Frage, wenn der Täter später unter Verwendung der erlangten Geheimnummer anstatt des Kunden Transaktionen mit der Bank bzw. einem anderen Vertragspartner vornimmt und dabei den Eindruck erweckt, er sei der Berechtigte. In diesem Fall ist dann § 269 StGB von § 263a StGB abzugrenzen.

S. 128

12 Schließlich ist noch an eine Strafbarkeit nach den §§ 44 Abs. 1, 43 Abs. 2 Nr. 1, Nr. 4 BDSG zu denken. Hiernach macht sich strafbar, wer unbefugt personenbezogene Daten, die nicht allgemein zugänglich sind, erhebt oder verarbeitet (§ 43 Abs. 2 Nr. 1 BDSG) oder deren Übermittlung durch unrichtige Angaben erschleicht (§ 43 Abs. 2 Nr. 4 BDSG), wenn er dabei gegen Entgelt oder in der Absicht handelt, sich oder einen anderen zu bereichern oder einen anderen zu schädigen. Bei der Tat handelt es sich nach § 44 Abs. 2 BDSG um ein Antragsdelikt. Personenbezogene Daten sind nach § 3 Abs. 1 BDSG Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person. Hierzu zählen nicht nur der Name der betreffenden Person, sondern auch sonstige als Namensersatz fungierende Angaben, die ausschließlich der Identifizierung der Person dienen, ohne im Übrigen irgendetwas über sie auszusagen. Insoweit zählen aber auch persönlich zugeteilte oder selbstgewählte Berechtigungskennzeichen,

[28] *Popp*, NJW 2004, 3517 (3518); a.M. *Hilgendorf/Frank/Valerius* (Fn. 3), Rn. 765.
[29] *Hecker*, JA 1998, 300 (300 f.); *Schönke/Schröder-Lenckner/Perron* (Fn. 11), § 263 Rn. 145; anders aber z.B. *Tröndle/Fischer* (Fn. 17), die bei Preisgabe der PIN eine Unmittelbarkeit annehmen, da durch die Handlung des Getäuschten die „wesentliche Zugriffsschwelle" bereits überschritten sei.
[30] *Popp*, NJW 2004, 3517 (3518); a.M. *Hilgendorf/Frank/Valerius* (Fn. 3), Rn. 765.
[31] So *Knupfer*, MMR 2004, 641 (642).

wie die PIN oder die TAN, zu den personenbezogenen Daten[32]. Sind diese Nummern als „personenbezogene Daten" anzusehen, dann erschleicht der Täter diese Daten durch die Absendung der fraglichen E-Mail. In dieser macht er insoweit „unrichtige Angaben", als er vortäuscht, er handle für die Bank bzw. einen sonstigen Vertragspartner des Nutzers. Schließlich ist auch das Tatbestandsmerkmal „erschleichen" weiter als die Tathandlung des § 202a StGB („Sich-Verschaffen"). Das Argument, der Nutzer würde die Daten dem Absender zwar täuschungsbedingt, aber insoweit dennoch freiwillig mitteilen, steht der Erfüllung dieses Tatbestandsmerkmals nicht entgegen. Selbst wenn man hierin eine Einwilligung nach § 4a BDSG sehen würde, wäre diese infolge der Täuschung unwirksam. Auch handelt der Täter hier regelmäßig, um sich – durch einen späteren Akt – zu Unrecht zu bereichern. Dennoch muss eine Strafbarkeit nach § 44 BDSG – obwohl vom Wortlaut her an sich erfüllt – bereits daran scheitern, dass der Anwendungsbereich des Gesetzes nicht betroffen ist. Nach § 1 Abs. 2 BDSG gilt das Gesetz nur für die Erhebung, Verarbeitung und Nutzung personenbezogener Daten durch öffentliche Stellen des Bundes, der Länder (mit gewissen Einschränkungen) und bestimmter nicht-öffentlicher Stellen, „soweit sie die Daten unter Einsatz von Datenverarbeitungsanlagen verarbeiten [...], es sei denn, die Erhebung, Verarbeitung oder Nutzung der Daten erfolgt ausschließlich für persönliche oder familiäre Tätigkeiten". Da es sich bei den geschädigten Internetnutzern aber regelmäßig nicht um solche Stellen, sondern um Privatpersonen handelt, scheidet die Anwendbarkeit des Bundesdatenschutzgesetzes (und daher auch die Strafbarkeit nach § 44 BDSG) aus.

13 ***b) „Trojanische Pferde"***

Vom strafrechtlichen Gesichtspunkt her weniger problematisch stellt sich die Erlangung fremder Passwörter oder anderer sensibler Daten durch die Installation eines so genannten „Trojaners"[33] dar. Hierunter versteht man ein selbstständiges Programm, welches von außen eingeschleust und ohne Wissen des Internetnutzers auf seinem Computer installiert wird. Dies ist in mehreren Formen denkbar: Entweder wird das Programm als Hilfs- oder Anwendungsprogramm getarnt und als solches installiert, ohne dass der Nutzer die Bedeutung des Programms als „Ausspähungsprogramm" erkennt. Eine andere Möglichkeit besteht darin, den „Trojaner" mittels eines Attachments einer E-Mail einzuschleusen und im Betriebssystem bzw. auf der Festplatte des Internetnutzers – ohne dessen Wissen – zu installieren. Das Programm verursacht zwar – im Gegensatz zu Viren – keinen unmittelbaren Schaden am betroffenen System, hat aber die Eigenschaft, dass es sämtliche, vom Nutzer eingegebenen Daten protokolliert und ohne dessen Wissen an den Täter weitersendet[34]. Durch die Installation eines „Trojaners" auf einem fremden Rechner und dem dadurch hervorgerufenen Weiterleiten von Daten ist der Tatbestand des § 202a StGB problemlos erfüllt. Zwar handelt es sich bei den weitergegebenen Daten in den überwiegenden Fällen nicht um solche, die i.S. des § 202a StGB dauerhaft „gespeichert" sind[35]. Hier greift jedoch die 2. Alternative des § 202a Abs. 2 StGB ein. Werden durch den „Trojaner" Eingabedaten, Passwörter oder die TAN, die das Tatopfer bei der Internetnutzung verwendet, an den Täter weitergeleitet, handelt es sich um Daten, die das Tatopfer an einen (anderen) Empfänger „übermittelt". In diesen Übermittlungsvorgang greift nun der Täter ein, indem er durch die Installation des „Trojaners" bewirkt, dass (auch) ihm die entsprechenden Daten übersandt werden. In diesen Fällen geschieht die Übermittlung der Daten an den Täter auch nicht durch einen willentlichen Akt des Geschädigten, sondern vollzieht sich im Hintergrund, wodurch die Voraussetzungen des § 202a StGB erfüllt sind[36]. Es liegt auch – anders als beim bloßen „Hacking"[37] – nicht nur eine bloße Überwin-

[32] *Dammann* in: *Simitis* (Hrsg.), Bundesdatenschutzgesetz, 6. Aufl. 2006, § 3 Rn. 10; hierzu auch *Gola/Schomerus*, Bundesdatenschutzgesetz, 8. Aufl. 2005, § 43 Rn. 23; a.M. allerdings *Popp*, NJW 2004, 3517 (3519, Fn. 6), der solche „persönlichen Zugangsdaten" als nicht erfasst ansieht.
[33] Vgl. zu den „Trojanischen Pferden" *Hilgendorf/Frank/Valerius* (Fn.3), Rn. 689; *Malek* (Fn. 7), Rn. 158; MüKo-*Graf* (Fn. 12), § 202a Rn. 64; *Schmid*, Computerhacken und materielles Strafrecht – unter besonderer Berücksichtigung von § 202a StGB, S. 169 ff.
[34] Vgl. hierzu *Haurand/Vahle*, RDV 1990, 128 (132); MüKo-*Graf* (Fn. 12), § 202a Rn. 64.
[35] *Hilgendorf/Frank/Valerius* (Fn. 3), Rn. 761.
[36] *Hilgendorf/Frank/Valerius* (Fn. 3), Rn. 762; *Malek* (Fn. 7), Rn. 158, 213; *Marberth-Kubicki* (Fn. 3), Rn. 60.
[37] Vgl. hierzu sogleich unten II 1c.

dung einer Zugangssperre ohne Kenntnisnahme von Daten vor, da der Täter durch die Übermittlung der fremden Zugangsdaten, welche ihm über den „Trojaner" zumeist per E-Mail übersandt werden, die Daten dauerhaft in seiner Verfügungsgewalt hat[38].

S. 129

14 ***c) Erlangung von Daten auf andere Weise***

Schließlich können sensible Daten auch auf andere Weise bekannt werden, wobei die Anwendung des § 202a StGB in vielen Fällen jedoch fraglich ist. Keine besondere kriminelle Energie erfordert z.B. das Erlangen von Passwörtern durch schlichtes Ausprobieren. So ist z.B. der Fall denkbar, dass ein Studierender auf Materialien eines fremden Hochschuldozenten, die dieser ausschließlich für seine Kursteilnehmer „ins Netz" gestellt und mit einem Passwort gesichert hat, zugreifen will und sich den Zugang dadurch verschaffen möchte, dass er als Passwörter allgemeingültige Begriffe (Name des Dozenten, der Veranstaltung etc.) eingibt, weil er sich erhofft, dadurch einen „Treffer" zu landen. Da § 202a StGB keine Versuchsstrafbarkeit kennt, wäre lediglich dann an eine Strafbarkeit (wegen eines vollendeten § 202a StGB) zu denken, wenn der Täter tatsächlich das richtige Passwort errät und sich dadurch Zugang zu den Informationen verschafft. Andererseits hat der Gesetzgeber bewusst davon abgesehen, das so genannte „Hacking", d.h. das bloße Eindringen in fremde Systeme, unter Strafe zu stellen[39], sodass jedenfalls die Überwindung des ersten Passwortes beim Zugang zu einer EDV-Anlage nicht strafbar sein soll[40]. Überwindet der Betreffende jedoch das entsprechende Passwort und greift dann auch auf die jeweiligen Daten zu, verlässt er den Bereich des bloßen „Hacking" und verschafft sich die entsprechenden Daten, die mittels des „erratenen" Passworts gerade gegen unberechtigten Zugang besonders gesichert waren[41]. Insoweit überschreitet er aber die Schwelle zum strafbaren Verhalten. Dabei ist es nicht erforderlich, dass der Täter die betreffenden Daten dauerhaft auf einem Speichermedium fixiert[42], ausreichend ist vielmehr die bloße Kenntnisnahme des durch das Passwort gesicherten Textes[43]. Zuweilen wird allerdings eine Ausnahme für diejenigen Fälle gefordert, in denen das Passwort als „Allerweltsname" leicht zu erraten ist und daher keine effektive Sicherung darstellt[44]. Dem ist jedoch entgegen zu halten, dass auch in diesen Fällen der Berechtigte eine Zugangssperre gegen die unbefugte Benutzung errichtet hat, die bewusst überwunden wird. Ferner kann eine Abgrenzung dahingehend, welche Begriffe noch oder schon den Bereich der „Allerweltsnamen" verlassen, kaum gefunden werden (mit den entsprechenden Konsequenzen im Bereich des Irrtums) [45].

15 Die vorgenannten Überlegungen gelten im Übrigen auch (und erst recht), wenn der Täter das Passwort nicht mittels „Ausprobierens" im Einzelfall, sondern mittels eines eigens dafür vorgesehenen (Wortlisten-)Programms ermittelt[46]. Bei diesen so genannten. „Brute-Force-Attacks" werden zur Überwindung von Passwörtern im Internet im „Trial-and-Error-Verfahren" systematisch alle denkbaren Buchstaben und Zahlenkombinationen ausprobiert, bis die richtige Kombination gefunden wurde.

16 Schließlich ist noch an die Fälle zu denken, in denen der Täter das Passwort bzw. die PIN

---

[38] So auch *Ernst*, NJW 2003, 3233 (3237); *Hilgendorf/Frank/Valerius* (Fn. 3), Rn. 691; MüKo-*Graf* (Fn. 12), § 202a Rn. 51, 64; *Tröndle/Fischer* (Fn. 17), § 202a Rn. 10; a.M. *Binder*, RDV 1995, 116 (116 f.); *Schmid* (Fn. 33), S. 171.

[39] BT-Drucks. 10/5058, S. 28 f.; vgl. hierzu *Dannecker*, BB 1996, 1285 (1289); *Schnabl*, wistra 2004, 211 (213); *Tiedemann*, JZ 1986, 865 (870 f.)

[40] *Binder*, RDV 1995, 57 (60); *Hilgendorf/Frank/Valerius* (Fn. 3), Rn. 691; MüKo-*Graf* (Fn. 12), § 202a Rn. 63; *Lackner/Kühl*, Strafgesetzbuch mit Erläuterungen, 25. Aufl. 2004, § 202a Rn. 5; *Schmid* (Fn. 33), S. 162 f.; *Schmitz*, JA 1995, 478 (483); *Schönke/Schröder-Lenckner* (Fn. 11), § 202a Rn. 10; kritisch *Bühler*, MDR 1987, 448 (453); a.M. *Jessen* (Fn. 12), S. 181 ff.; *Tröndle/Fischer* (Fn. 17), § 202a Rn. 10.

[41] NK-*Kargl* (Fn. 11), § 202a Rn. 1, 13.

[42] So aber *Hauptmann*, jur-PC 1989, 215 (217 f.).

[43] *Binder*, RDV 1995, 57 (60).

[44] *V.Gravenreuth*, NStZ 1989, 201 (206); *Koch*, RDV 1996, 123 (126); LK-*Schünemann* (Fn. 11), § 202a Rn. 16; *Strömer* (Fn. 5), S. 358 f.

[45] Ebenfalls ablehnend im Hinblick auf qualitative Anforderung an Passwörter *Ernst*, NJW 2003, 3233 (3236).

[46] *Malek* (Fn. 7), Rn. 159; MüKo-*Graf* (Fn. 12), § 202a Rn. 63; *Schmid* (Fn. 33), S. 158.

oder TAN durch Täuschung oder durch Diebstahl erlangt (im betrieblichen Bereich hat sich hierfür der Begriff des „social-engineering" eingebürgert: Ein Informationsträger wird durch gezielte Manipulation zur Preisgabe von Kennwörtern veranlasst). Während die Erlangung durch Täuschung nach den oben genannten Grundsätzen[47] noch kein „Ausspähen" darstellt und daher nicht nach § 202a StGB strafbar sein kann, ist bei der Erlangung der sensiblen Daten durch Diebstahl (z.B. durch die Wegnahme von Notizbüchern) oder Erpressung zwar der Bereich strafbaren Verhaltens erreicht, fraglich ist jedoch, ob hier neben § 242 StGB (bzw. § 240 StGB oder §§ 253, 255 StGB) auch § 202a StGB anwendbar ist. Zwar erlangt der Täter auch hier unbefugt Daten, die nicht für ihn bestimmt sind (und die auch möglicherweise gegen unberechtigten Zugang besonders gesichert sind), er erlangt diese jedoch nicht durch die Überwindung der hierfür vorgesehenen Zugangssperre, sodass auch hier § 202a StGB ausscheidet.

S. 130

17 **2. Urheberrechtsverletzungen im Zusammenhang mit dem Internet**

Urheberrechtsverletzungen können in vielfacher Weise über das Medium des Internet begangen werden[48]. Ausgangspunkt für die strafrechtliche Beurteilung ist dabei § 106 UrhG, der die unerlaubte Vervielfältigung, Verbreitung und öffentliche Wiedergabe urheberrechtlich geschützter Werke unter Strafe stellt. Ein solches Werk liegt nach den §§ 1, 2 Abs. 2 UrhG dann vor, wenn es sich um eine persönliche geistige Schöpfung aus den Bereichen der Literatur, Wissenschaft oder Kunst handelt. Beispiele hierfür sind in § 2 Abs. 1 UrhG aufgezählt. Im vorliegenden Zusammenhang relevant sind insbesondere die in den dortigen Nummern 1, 2 und 6 genannten Sprachwerke, Werke der Musik oder Filmwerke. Daneben können aber auch multimediale Internet-Produktionen urheberrechtlichen Schutz genießen[49], wobei man hier zwischen den einzelnen Beiträgen, der Gesamtproduktion und der Programmierleistung (d.h. dem zu Grunde liegenden Computerprogramm) unterscheiden muss[50].

18 Tathandlungen sind die Vervielfältigung (§ 16 UrhG), die Verbreitung (§ 17 UrhG) und die öffentliche Wiedergabe (§ 15 Abs. 2 i.V. mit §§ 19 ff. UrhG). Der Tatbestand des § 106 UrhG ist jedoch dann ausgeschlossen, wenn es sich um einen „gesetzlich zugelassenen Fall" der Verwertung handelt[51]. Hierunter fallen sowohl die in §§ 44a ff. UrhG normierten „Schranken des Urheberrechts" als auch die Nutzung von Werken nach Ablauf der Schutzfrist (§ 64 ff. UrhG)[52] sowie die Verbreitung eines Werkes nach Erschöpfung des urheberrechtlichen Verbreitungsrechts (§ 17 Abs. 2 UrhG). Dagegen schließt die in § 106 UrhG genannte Einwilligung des Berechtigten nicht bereits den Tatbestand aus, sondern stellt lediglich einen Rechtfertigungsgrund dar[53].

---

[47] Vgl. oben II 1a.

[48] Vgl. hierzu *Boßmanns*, Urheberrechtsverletzungen im Online-Bereich und strafrechtliche Verantwortlichkeit der Internet-Provider, 2003; *Büchele*, Urheberrecht im World Wide Web, 2002; *Ensthaler/Bosch/Völker*, Handbuch Urheberrecht und Internet, 2002; *Evert*, Anwendbares Urheberrecht im Internet, 2005; *Hilgendorf/Frank/Valerius* (Fn. 3), Rn. 591 ff.; *Malek* (Fn. 7), Rn. 241 ff.; *Rademacher*, Urheberrecht und gewerblicher Rechtsschutz im Internet, 2003; *Sedlmeier*, Die Auslegung der urheberrechtlichen Straftatbestände bei Internet-Sachverhalten, 2003.

[49] *Härting/Kuon*, CR 2004, 527; *Malek* (Fn. 7), Rn. 245; *Sedlmeier* (Fn. 48), S. 22 ff.

[50] *Malek* (Fn. 7), Rn. 245.

[51] Dass die „gesetzlich zugelassenen Fälle" bereits den Tatbestand ausschließen ist nahezu unstreitig; vgl. *Dreier/Schulze-Dreier*, Urheberrechtsgesetz, Kommentar, 2. Aufl. 2006, § 106 Rn. 6; *Fromm/Nordemann-Vinck*, Urheberrecht, Kommentar, 9. Aufl. 1998, § 106 Rn. 3; *Hildebrand*, Die Strafvorschriften des Urheberrechts, 2001, S. 124; *Schricker-Vassilaki*, Urbeberrecht, Kommentar, 3. Aufl. 2006, § 106 Rn. 23; *Wandtke/Bullinger-Hildebrandt*, Praxiskommentar zum Urheberrecht, 2. Aufl. 2006, § 106 Rn. 21; *Weber*, Der strafrechtliche Schutz des Urheberrechts, 1976, S. 225 ff., 230; a.M. *Lampe* UFITA 83 (1978), 15 (30 f.).

[52] *Hildebrandt* (Fn. 51), S. 136 f.; *Möhring/Nicolini-Spautz*, Urheberrechtsgesetz, Kommentar, 2. Aufl. 2000, § 106 Rn. 4*; Wandtke/Bullinger-Hildebrandt* (Fn. 51), § 106 Rn. 22; a.M. (ungeschriebenes Tatbestandsmerkmal) *Erbs/Kohlhaas/Meurer*, Strafrechtliche Nebengesetze, Loseblattsammlung, Kommentierung des Urheberrechtsgesetzes, U 180, Stand: 1.9.1995, § 106 Rn. 2; *Fromm/Nordemann-Vinck* (Fn. 51), § 106 Rn. 2.

[53] *Dreier/Schulze-Dreier* (Fn. 51), § 106 Rn. 8; *Fromm/Nordemann-Vinck* (Fn. 51), § 106 Rn. 5; *Möhring/Nicolini-Spautz* (Fn. 52), § 106 Rn. 5; *Weber* (Fn. 51), S. 266; a.M. *Schricker-Vassilaki* (Fn. 51) § 106

19 ***a) „Illegale" Musiktauschbörsen im Internet***

Seit etlichen Jahren existieren so genannte „Musiktauschbörsen" im Internet, bei denen Privatpersonen untereinander einzelne Musikstücke (die als Musikwerke nach § 2 Abs. 1 Nr. 2 UrhG urheberrechtlichen Schutz genießen) in digitaler Form tauschen[54]. Diese Tauschbörsen beruhen im Wesentlichen auf zwei Modellen, die urheber(straf)rechtlich unterschiedlich zu beurteilen sind: das frühere *Client-Server-Modell* und das heutzutage zumeist verwendete *Peer-to-Peer-Modell*.

20 Beim früher häufiger anzutreffenden *Client-Server-Modell* ist zwischen den Tauschpartnern noch ein externer Server zwischengeschaltet. Die Beteiligten („Clients"; Kunden) legen die einzelnen Musikwerke als „Files" in digitaler Form auf dem externen Server ab („Upload"). Sowohl auf diesem Server als auch auf den Rechnern der einzelnen Beteiligten ist dabei eine spezielle „Tauschbörsen-Software" installiert. Auf dem Server werden die jeweiligen Dateien verwaltet und bereitgehalten. Hat nun ein weiterer Beteiligter, der selbst im Regelfall ebenfalls Musikwerke auf dem Server abgelegt und dadurch anderen zur Verfügung gestellt hat, Interesse an einem solchen Musikstück, kann er dieses abrufen und auf seinem eigenen Rechner installieren („Download"). Urheberrechtlich stellt sowohl der Upload als auch der Download eine „Vervielfältigung" i.S. des § 16 UrhG dar. Der Upload selbst ist zudem eine „öffentliche Wiedergabe" i.S. der § 15 Abs. 2 Nr. 2, § 19a UrhG, da das Werk hierdurch einer Vielzahl von im Einzelnen nicht bekannten Personen – und daher der „Öffentlichkeit" – zugänglich gemacht wird. Dagegen scheidet eine „Verbreitung" i.S. des § 17 UrhG aus, da eine solche voraussetzt, dass das Werk einem anderen *in körperlicher Form* zugänglich gemacht wird[55]. Da sowohl für die Vervielfältigungshandlungen als auch für das öffentliche Zugänglichmachen regelmäßig keine Erlaubnis des Urhebers oder des Nutzungsberechtigten vorliegt, sind diese Verhaltensweisen von § 106 UrhG tatbestandlich erfasst, sofern kein gesetzlich zugelassener Fall vorliegt. Ein solcher könnte aber im Hinblick auf die Vervielfältigung nach § 53 UrhG dann in Frage kommen, wenn es sich um eine solche zum privaten oder sonstigen eigenen Gebrauch handelt[56].

S. 131

21 Unter privatem Gebrauch wird allgemein der Gebrauch in der Privatsphäre zur Befriedigung rein persönlicher Bedürfnisse durch die eigene Person oder durch mit ihr durch ein persönliches Band verbundene Personen verstanden[57]. Umfasst sind neben dem Vervielfältigenden selbst auch der engste Freundes- und Familienkreis. Ein privater Gebrauch scheidet allerdings dann aus, wenn die Vervielfältigung unmittelbar oder mittelbar Erwerbszwecken dient. Betrachtet man die Tauschbörsen, so stellt zwar der Download regelmäßig eine solche private Vervielfältigung dar, sofern er ausschließlich dazu dient, die eigene Musiksammlung zu bereichern. Der Upload hingegen verlässt den Bereich des Privaten, da die Vervielfältigung nicht der Befriedigung eigener Bedürfnisse, sondern ausschließlich dazu dient, eine Kopie des Werkes der Öffentlichkeit zur Verfügung zu stellen. Im Hinblick auf den Download ist aber zu beachten, dass der Betreffende

Rn. 27 (Tatbestandsmerkmal); vgl. auch *Hildebrandt* (Fn. 51), S. 149 ff.; *Wandtke/Bullinger-Hildebrandt* (Fn. 51), § 106 Rn. 25, welcher der Einwilligung eine „Doppelnatur" zuschreibt.

[54] Vgl. zur strafrechtlichen Beurteilung solcher Musiktauschbörsen *Heghmanns*, MMR 2004, 14.

[55] BGH NJW 1963, 651 (652) – Fernsehwiedergabe von Sprachwerken; BT-Drucks. IV/270, S. 47 = UFITA 45 (1965), 240 (262); Heidelberger Kommentar zum Urheberrecht-*Dreyer*, 2004, § 17 Rn. 2; *Schricker-Loewenheim* (Fn. 51), § 17 Rn. 4.

[56] Allgemein zu § 53 UrhG *Ahrens*, ZUM 2000, 1029; *Collova*, UFITA 125, 53; *Flechsig*, GRUR 1993, 532; *Freiwald*, Die private Vervielfältigung im digitalen Kontext am Beispiel des Filesharing, 2003; *Kreutzer*, GRUR 2001, 193, 307; *Krüger*, GRUR 2004, 204; *Leupold/Demisch*, ZUM 2000, 379; *Loewenheim*, Dietz-FS 2001, S. 415; *Mönkemöller*, GRUR 2000, 663; *Schack*, ZUM 2002, 497; *Schaefer*, Nordemann-FS 1999, S. 191; *Schippan*, ZUM 2003, 678; *Schwenzer*, ZUM 1997, 478; *Ulmer-Eilfort*, Nordemann-FS 1999, S. 285

[57] BGH, GRUR 1978, 474 (475) – Vervielfältigungsstücke (in NJW 1978, 2596 nicht abgedruckt); *Dreier/Schulze-Dreier* (Fn. 51), § 53 Rn. 7; *Heinrich*, Die Strafbarkeit der unerlaubten Vervielfältigung und Verbreitung von Standardsoftware, 1993, S. 251; *Schricker-Loewenheim* (Fn. 51), § 53 Rn. 12.

nur einzelne Vervielfältigungsstücke, d.h. „einige wenige" Exemplare[58] herstellen darf, wobei der BGH in einer Entscheidung die Grenze bei sieben Exemplaren zog[59]. Letztere Voraussetzung dürfte bei den Musiktauschbörsen regelmäßig vorliegen, da eine Vervielfältigung zwar auf der Festplatte des Computers, einer externen Festpatte, einem MP3-Player oder weiteren Speichermedien denkbar ist, die Zahl von sieben im Normalfall aber kaum überschritten werden dürfte. Eine weitere einschränkende Voraussetzung besteht im Hinblick auf die private Vervielfältigung jedoch darin, dass gemäß § 53 Abs. 1 UrhG keine „offensichtlich rechtswidrig hergestellte Vorlage" für die private Vervielfältigung verwendet werden darf. Dieses – infolge mangelnder Bestimmtheit zumindest aus strafrechtlicher Sicht verfassungsrechtlich bedenkliche – Merkmal ist aber im vorliegenden Fall regelmäßig gegeben. Denn wie soeben festgestellt, bedeutet das Ablegen einer Kopie des Musikwerkes auf dem Server (Upload) in aller Regel die Herstellung einer Vorlage, deren Herstellungsakt (der Upload) gerade rechtswidrig war, da eine Einwilligung des Urhebers oder Nutzungsberechtigten in den seltensten Fällen vorlag und das Verhalten den Bereich des Privaten verlässt. Fraglich ist dann lediglich noch, ob es sich auch um eine „offensichtlich" rechtswidrig hergestellte Vorlage handelte. Diese Offensichtlichkeit dürfte jedenfalls dann gegeben sein, wenn es ausgeschlossen ist, dass das Einstellen in die Tauschbörse dem Willen des Urhebers oder Nutzungsberechtigten entsprach, was lediglich dann einmal der Fall sein kann, wenn unbekannte Interpreten oder Gruppen ihre Werke als „Freeware" in eine solche Tauschbörse einstellen, um ihren Bekanntheitsgrad zu steigern. Bis auf diese wenigen Fälle ist die Rechtswidrigkeit des Herstellungsaktes aber offensichtlich erkennbar, weshalb auch derjenige, der sich nach diesem Modell urheberrechtlich geschützte Musikwerke herunterlädt, eine strafbare unerlaubte Vervielfältigung begeht.

22 Das heute zumeist anzutreffende *Peer-to-Peer Modell* verzichtet hingegen auf das Dazwischenschalten eines externen Servers[60]. Es werden ausschließlich die – zumeist privaten – Rechner der einzelnen Beteiligten benutzt, wobei auf jedem Rechner gleichrangig sowohl Daten zur Verfügung gestellt werden als auch Daten von anderen Rechnern heruntergeladen werden können. Jeder, der sich an dem Tausch-Netzwerk beteiligt, ermöglicht also den anderen Beteiligten einen Zugriff auf Teile der Festplatte seines Computers und die dort abgelegten Musikwerke. Dies funktioniert allerdings nur dann, wenn der jeweils betreffende Anbieter „online" ist. Insoweit finden zumeist beide Vorgänge gleichzeitig statt: In der Zeit, in der ein Nutzer Werke von anderen Rechnern herunterlädt, stellt er gleichzeitig die bei ihm abgelegten Werke anderen zur Verfügung. Zwar existiert auch hier mitunter ein zentraler Server (z.B. bei „Napster"), der aber lediglich eine Indexfunktion erfüllt[61]: Hier wird lediglich eine Übersicht der von den Benutzern zurzeit bereitgestellten Musiktitel erstellt und ferner die Möglichkeit geschaffen, sich durch das Anklicken des jeweils gewünschten Titels mit dem jeweiligen Anbieter bzw. dem Rechner des Anbieters direkt in Verbindung zu setzen. Der Austausch der Musikwerke erfolgt dann jedoch nicht mehr über den vermittelnden Server, sondern direkt zwischen den Beteiligten. Teilweise wird aber sogar auf diesen zentralen (Index-)Server verzichtet (z.B. bei „Gnutella" oder „KaZaA") und bei einer Suchanfrage das gesamte Internet nach den gewünschten Musikfiles durchsucht[62]. Insofern wird bei diesem Modell – in beiden Varianten – stets nur *eine* Vervielfältigung i.S. des § 16 UrhG vorgenommen, die nun in aller Regel dem Anwendungsbereich des § 53 Abs. 1 UrhG unterfällt: Zum privaten Gebrauch wird eine digitale Vervielfältigung erstellt. Auch die Vorlage, d.h. die sich auf der Festplatte des Ausgangsrechners befindende Kopie des Musikwerkes muss nicht zwingend rechtswidrig hergestellt sein, da es vielfäl-

[58] BGH NJW 1978, 2596 (2597) = GRUR 1978, 474 (476) – Vervielfältigungsstücke; *Ulmer*, Urheber- und Verlagsrecht, 3. Aufl. 1990, § 64 I 3; *Schack*, Urheber- und Urhebervertragsrecht, 3. Aufl. 2005, Rn. 496; *Schricker-Loewenheim* (Fn. 51), § 53 Rn. 14; *Wandtke/Bullinger-Lüft* (Fn. 51), § 53 Rn. 10.
[59] BGH NJW 1978, 2596 (2597) = GRUR 1978, 474 (476) – Vervielfältigungsstücke; diese Grenzziehung war allerdings dem der Klage zu Grunde liegenden Klageantrag geschuldet.
[60] Vgl. zu diesem Modell *Abdallah/Gerke*, ZUM 2005, 368; *Kress*, Die private Vervielfältigung im Urheberrecht, 2004, S. 13 ff.; *Kreutzer*, GRUR 2001, 193 (194).
[61] Vgl. *Kreutzer*, GRUR 2001, 193 (195).
[62] Vgl. *Kreutzer*, GRUR 2001, 193 (195).

tige Möglichkeiten gibt, dass der Betreffende das Musikwerk in zulässiger Weise auf seiner Festplatte gespeichert hat. Dies kann beispielsweise dann der Fall sein, wenn er das Musikwerk ordnungsgemäß, z.B. durch Kauf einer CD, erworben und anschließend auf seine Festplatte gespeichert hat, um es von dort aus abzuhören oder zu sichern. Insoweit stellt auch dieser Vorgang zwar eine Vervielfältigung i.S. des § 16 UrhG dar, jedoch ist diese regelmäßig von § 53 Abs. 1 UrhG gedeckt, wenn sie nicht ausschließlich dazu dient, das Werk zu speichern, um es anderen zur Verfügung zu stellen. Kopiert nämlich der Betreffende das Werk von der gekauften CD auf seine Festplatte, um es auf diese Weise später anzuhören, liegt ein „klassischer" Fall der zulässigen Vervielfältigung zum privaten Gebrauch vor[63]. Doch selbst dann, wenn dies im Einzelfall nicht festgestellt werden kann und der Betreffende den Vervielfältigungsvorgang ausschließlich deswegen vorgenommen hat, um das Werk später anderen zur Verfügung zu stellen, so ist dieser Umstand jedenfalls nach außen nicht erkennbar. Es handelt sich somit nicht um eine „offensichtlich" rechtswidrig hergestellte Vorlage, weshalb eine zu privaten Zwecken vorgenommene Vervielfältigung dieses Werkes von § 53 UrhG gedeckt ist. Da somit die mittels einer Tauschbörse im *Peer-to-Peer-Modell* erlangten Musikstücke rechtmäßig hergestellte Privatkopien sind, können diese wiederum von anderen straflos, da über § 53 UrhG zugelassen, vervielfältigt werden. Strafbar bleibt somit lediglich das öffentliche Zugänglichmachen (als öffentliche Wiedergabe gemäß §§ 19a, 15 Abs. 2 Nr. 2 UrhG), indem der Benutzer die Werke auf seiner Festplatte anderen zur Verfügung stellt, nicht jedoch der Vorgang der Vervielfältigung.

S. 131

23 ***b) Kopieren von Texten zur Verwendung in eigenen wissenschaftlichen Arbeiten***

Insbesondere im Zusammenhang mit der universitären Ausbildung von besonderem Interesse ist die Kopie von Texten bzw. Textteilen aus Internetseiten zur Verwendung in eigenen wissenschaftlichen Arbeiten (Hausarbeiten, schriftliche Referate etc.). Fraglich ist, wann und ob hier eine Vervielfältigung oder Verbreitung vorliegt. Unter einer Vervielfältigung eines urheberrechtlich geschützten Werkes ist jede körperliche Festlegung eines Werkes zu verstehen, die geeignet ist, das Werk den menschlichen Sinnen auf irgendeine Weise mittelbar oder unmittelbar wahrnehmbar zu machen[64]. Nicht erfasst ist hingegen die unkörperliche Verwertung, die allerdings eine öffentliche Wiedergabe i.S. des § 15 Abs. 2 UrhG darstellen kann[65]. Dagegen versteht man unter einer Verbreitung, dass der Täter das Vervielfältigungsstück der Öffentlichkeit anbietet oder in den Verkehr bringt, wobei auch hier ein körperliches Werk oder Vervielfältigungsstück erforderlich ist, eine unkörperliche Weitergabe (etwa durch Versenden einer Datei) scheidet dagegen aus[66].

24 Bei der rechtlichen Bewertung kann man folgende Vorgänge unterscheiden: Das bloße Betrachten von Dateien auf dem Bildschirm stellt noch keine unerlaubte Vervielfältigung dar[67]. Hier kann lediglich, wie oben bereits angesprochen, eine Strafbarkeit nach § 202a StGB vorliegen, wenn die entsprechende Datei durch ein Passwort gesichert war, welches umgangen wurde.

25 Dagegen stellt das Ausdrucken von Web-Seiten oder hierüber zugänglichen Dateien[68] e-

[63] Vgl. *Heghmanns*, MMR 2004, 14 (16).
[64] BGHZ 17, 266 (269 f.) = GRUR 1955, 492 (494) – Grundig-Reporter; BGH GRUR 1982, 102 (103) – Masterbänder; BGH GRUR 1983, 28 (29) – Presseberichterstattung und Kunstwerkwiedergabe II, BGHZ 112, 264 (278) = NJW 1991, 1231 (1234) – Betriebssystem; *Fromm/Nordemann-Nordemann* (Fn. 51), § 16 Rn. 1; *Haberstumpf*, GRUR 1982, 142 (148); *Heinrich* (Fn. 57), S. 185; *Möhring/Nicolini-Kroitsch* (Fn. 52), § 16 Rn. 3; *Rehbinder*, Urheberrecht, 14. Aufl. 2006, Rn. 203; *Rupp*, GRUR 1986, 147; *Schricker-Loewenheim* (Fn. 51), § 16 Rn. 6; *Weber* (Fn. 51), S. 195.
[65] *Malek* (Fn. 7), Rn. 247
[66] BGH NJW 1963, 651 (652) – Fernsehwiedergabe von Sprachwerken; BT-Drucks. IV/270, S. 47 = UFITA 45 (1965), 240 (262); *Malek* (Fn. 7), Rn. 248; *Schricker-Loewenheim* (Fn. 51), § 16 Rn. 4.
[67] *Malek* (Fn. 7), Rn. 247; vgl. allerdings zur Frage, ob bereits das Laden der Datei in den Arbeitsspeicher des Computers, welches Voraussetzung für das Lesen der Datei darstellt, eine Vervielfältigung darstellt sogleich unten im Text.
[68] *Malek* (Fn. 7), Rn. 247.

benso wie deren dauerhafte Abspeicherung auf einem Datenträger (Diskette, CD-ROM, Festplatte)[69], eine urheberrechtlich relevante Vervielfältigung dar. Diese ist aber dann nicht tatbestandsmäßig, wenn ein gesetzlich zugelassener Fall vorliegt, was häufig anzunehmen sein dürfte, da die Vervielfältigung zumeist von § 53 UrhG (privater oder sonstiger eigener Gebrauch) gedeckt sein wird. Darüber hinaus ist – auf Rechtswidrigkeitsebene – immer auch an eine Einwilligung des Berechtigten zu denken. Denn wer Dateien mit eigenen urheberrechtlich geschützten Werken frei zugänglich, d.h. nicht durch ein Passwort geschützt, ins Internet stellt wird mit der Vervielfältigung durch einen Nutzer regelmäßig einverstanden sein[70]. Doch selbst wenn dies einmal nicht der Fall ist, kommt ein entsprechender Irrtum des Vervielfältigenden über das Vorliegen einer Einwilligung in Frage, sofern die entsprechende Datei nicht den deutlichen Hinweis enthält, dass eine Vervielfältigung untersagt ist. Dieser Irrtum schließt als Erlaubnistatbestandsirrtum die Schuld des Handelnden aus[71].

26 In diesem Zusammenhang noch interessant ist die seit langer Zeit umstrittene Frage, ob bereits die Speicherung im Arbeitsspeicher des Computers (RAM) eine urheberrechtlich relevante Vervielfältigungshandlung darstellen kann[72]. Dieser Streit dürfte sich inzwischen jedoch im positiven Sinne durch die im Jahre 2003 vorgenommene Klarstellung des Gesetzgebers[73] geklärt haben, der in § 16 Abs. 1 UrhG den Passus „gleichviel ob vorübergehend oder dauerhaft" einfügte und dadurch zu verstehen gab, dass auch die nur flüchtige, vorübergehende Vervielfältigung als Vervielfältigung anzusehen ist, die jedoch unter den Voraussetzungen des § 44a UrhG zulässig ist.

27 ***c) Verwendung von urheberrechtlich geschützten Werken auf der Web-Seite***

Oftmals kommt es vor, dass auf eigenen Webseiten entweder urheberrechtlich geschützte Werke oder Werkteile verwendet werden oder auf solche verwiesen wird. Festzuhalten ist hierbei, dass der bloße Verweis auf eine andere Web-Seite im Internet, selbst wenn sie mit Hilfe eines „Hyperlinks" geschieht, noch keine Vervielfältigung der dort niedergelegten Texte darstellt, sondern lediglich eine Zugangserleichterung bedeutet[74].

28 Bei der Verwendung urheberrechtlich geschützter Werke oder Werkteile auf der eigenen Web-Seite scheidet eine Verbreitung – wegen des Erfordernisses der Körperlichkeit – aus. Es liegt jedoch eine öffentliche Wiedergabe nach § 15 Abs. 2 UrhG in der Form des öffentlichen Zugänglichmachens nach § 19a UrhG vor, die regelmäßig der Einwilligung des Berechtigten bedarf.

S. 132

29 **3. Verabredung von Straftaten über das Internet**

Nicht selten kommt es vor, dass Personen das Internet als Kommunikationsmedium dafür nutzen, andere zur Begehung von Straftaten aufzufordern oder sich mit anderen zur Begehung von Straftaten zu verabreden. So fand auch die Kontaktaufnahme der Beteiligten im jüngst vom BGH entschiedenen Fall des „Kannibalen von Rothenburg"[75] über das In-

[69] *Ernst*, GRUR 1997, 592 (595); *Koch*, GRUR 1997, 417 (423); *Malek* (Fn. 7), Rn. 247; *Waldenberger*, ZUM 1997, 176 (179).
[70] Etwas anderes gilt nur dann, wenn der Anbieter deutlich zum Ausdruck gibt, dass er zwar mit dem Lesen oder Betrachten der Wort- oder Bilddateien, nicht aber mit dem Vervielfältigen einverstanden ist. Dies kann z.B. in der Weise geschehen, dass der Anbieter – auch durch technische Maßnahmen gesichert – eine „Nur-Lese-Version" ins Netz stellt (so z.B. der Bundesanzeiger-Verlag, der eine kostenlose „Nur-Lese-Version" des Bundesgesetzblattes zur Verfügung stellt.; vgl. http://frei.bundesgesetzblatt.de, zuletzt abgerufen am 31.8.2006).
[71] Vgl. hierzu nur *Heinrich*, Strafrecht Allgemeiner Teil Band II, 2005, Rn. 1128 ff.
[72] Vgl. hierzu u.a. AG Freising CR 1990, 55; *Bosak*, CR 2001, 176 (177); *Koch*, GRUR 1997, 417 (423); *Leupold*, CR 1998, 234 (239); *Schack*, JZ 1998, 753 (756).
[73] Gesetz zur Regelung des Urheberrechts in der Informationsgesellschaft vom 10.9.2003, BGBl. I 2003, S. 1774.
[74] BGH NJW 2003, 3406; *Koch*, GRUR 1997, 417 (430); *Malek* (Fn. 7), Rn. 247; *Schricker-Loewenheim* (Rn. 50), § 16 Rn. 24; vgl. auch *Schack*, MMR 2001, 9 (13), der hier allerdings eine mittelbare Täterschaft für möglich hält.
[75] BGHSt 50, 80; vgl. hierzu *Kudlich*, JR 2005, 342; *Otto*, JZ 2005, 799; *Schiemann*, NJW 2005, 2350.

ternet statt. Der Angeklagte beschäftigte sich, so die Sachverhaltsdarstellung im Urteil[76], ungefähr ab 1999 über das Internet immer stärker mit dem Thema Kannibalismus. Er stieß dabei auch auf eine Schlachtanleitung für den menschlichen Körper. Schließlich begann er, über Internetforen Männer zum Schlachten und Verspeisen zu suchen. Nach mehreren nicht im Sinne des Angeklagten zielführenden Kontakten stieß er schließlich im Internet auf sein späteres Opfer. Zuerst entwickelte sich zwischen ihnen eine Kommunikation durch E-Mails, bevor man sich persönlich traf und es schließlich zur – einverständlichen – Tötung des Opfers kam.

30 Vom strafrechtlichen Gesichtspunkt aus ist eine Vielzahl weiterer Konstellationen denkbar, wobei jeweils kennzeichnend ist, dass es sich bei den „Verabredungen" im Internet um Vorstufen der Deliktsbegehung handelt, bei denen stets fraglich ist, ob die Schwelle zur Strafbarkeit bereits überschritten ist. Allgemein ist hierzu jedoch zu bemerken, dass auch in diesen Fällen keine internetspezifischen Straftatbestände einschlägig sind, sondern vielmehr stets das allgemeine Strafrecht zur Anwendung kommt. Das Internet wird hier gleichsam nur als „Medium" benutzt, welches hinsichtlich der rechtlichen Beurteilung im Vergleich zu Zeitungsinseraten bzw. öffentlichen Aushängen oder brieflichen Kontakten kaum Unterschiede aufweist. Im Folgenden sollen einige Fallkonstellationen näher untersucht werden.

31 ***a) Bereitschaftserklärung zur Deliktsbegehung***

Als erstes ist die Frage zu untersuchen, ob ein strafrechtlich relevantes Verhalten bereits darin zu sehen ist, dass jemand sich – sei es über die eigene Web-Seite, sei es in Diskussionsforen – allgemein dazu bereit erklärt, für einen anderen Delikte zu begehen, sei es in direkter Form („Erledige Tötungsaufträge sicher und zuverlässig"), sei es verschlüsselt und nur für Eingeweihte erkennbar („Erledige schwierige Aufgaben in sensiblen Bereichen"). Anknüpfungspunkt ist hier § 30 Abs. 2. Var. 1 StGB. Hiernach muss sich der Täter dazu „bereit erklären" ein Verbrechen zu begehen, wobei unter einem Verbrechen nach § 12 Abs. 1 StGB rechtswidrige Taten zu verstehen sind, die im Mindestmaß mit einer Freiheitsstrafe von einem Jahr oder darüber bedroht sind. Da der Täter in diesem Fall über den in § 30 Abs. 2 StGB vorgenommenen Verweis auf § 30 Abs. 1 StGB nach den Vorschriften über den Versuch des Verbrechens bestraft wird und der Versuch nach § 23 Abs. 2 StGB lediglich milder bestraft werden kann (aber nicht werden muss) als die vollendete Tat, wäre es möglich, denjenigen, der sich z.B. zur Begehung eines Mordes bereit erklärt mit einer lebenslangen Freiheitsstrafe zu bestrafen. Schon von daher (und im Hinblick darauf, dass allein von einer solchen Äußerung doch eine recht geringe objektive Gefährlichkeit ausgeht), muss die Vorschrift restriktiv ausgelegt werden[77].

32 Erforderlich ist erstens ein gewisser Bindungswille. Die Erklärung muss dahin gehen, sich gegenüber dem Adressaten insoweit festzulegen, dass dieser ein späteres Abstandnehmen von der Tat als Wortbruch ansehen könnte[78]. Insoweit muss die Erklärung jedenfalls ernst gemeint sein[79] und der „Anbietende" darf sich nicht vorbehalten, im Einzelfall zu entscheiden, ob er einen Auftrag annimmt oder nicht. Schon deshalb wird in den meisten Fällen die lediglich abstrakt gehaltene Bereitschaftserklärung im Internet die Voraussetzung des § 30 Abs. 2 Var. 1 StGB nicht erfüllen. Fraglich ist ferner, ob und inwieweit sich das Bereit-Erklären auf eine konkrete Tat beziehen muss und ob die Erklärung gegenüber einer Mehrheit von Personen ausreichen kann, von denen man dann eine entsprechende Reaktion, d.h. ihrerseits ein entsprechendes Angebot erwartet. Da aber in den geschilderten Fällen (Bereitschaftserklärung über eine WebSeite oder im Chat-Room) weder die

[76] BGHSt 50, 80 (81 f.).
[77] *Bloy*, JZ 1999, 157; MüKo-*Joecks* (Fn. 12), § 30 Rn. 3; *Schönke/Schröder-Cramer/Heine* (Fn. 11), § 30 Rn. 1; *Schröder*, JuS 1967, 290 (290 f.).
[78] MüKo-*Joecks* (Fn. 12), § 30 Rn. 40; Systematischer Kommentar zum Strafgesetzbuch (SK)-*Hoyer*, Bd. 1. Allgemeiner Teil, 7. Aufl., Loseblattsammlung, Stand 2/2005, § 30 Rn. 37; kritisch NK-*Zaczyk* (Fn. 11), § 30 Rn. 34.
[79] RGSt 57, 243 (245); RGSt 60, 23 (25); RGSt 63, 197 (199); BGHSt 6, 346 (347); MüKo-*Joecks* (Fn. 12), § 30 Rn. 42; NK-*Zaczyk* (Fn. 11), § 30 Rn. 37; *Schönke/Schröder-Cramer/Heine* (Fn. 11), § 30 Rn. 27; SK-*Hoyer* (Fn. 78), § 30 Rn. 38.

entsprechende Tat noch derjenige feststeht, der dem Handelnden letztlich das Angebot zur Begehung eines Verbrechens unterbreiten soll, kann dies für ein Sich-Bereit-Erklären i.S. des § 30 StGB nicht ausreichen. Es handelt sich vielmehr lediglich um ein „Angebot", vergleichbar einer „invitatio ad offerendum" im Zivilrecht, bei dem der Handelnde nun seinerseits eine Reaktion seitens einer vorher für ihn noch nicht bestimmbaren Person erwartet. Unterbreitet ihm diese dann das konkrete Angebot, liegt hierin eine (versuchte) Anstiftung. Nimmt der zuvor „Werbende" dieses (nunmehr konkrete) Angebot an, ist § 30 Abs. 2 Var. 1 StGB erfüllt.

S. 133

33 ***b) Aufforderung zur Begehung von Straftaten***

Als nächstes zu untersuchen ist die umgedrehte Konstellation: Der Auftraggeber sucht über das Internet Personen, die gegen Entgelt für ihn tätig werden, wobei die „Angebote" wiederum direkt und für alle verständlich („Suche zuverlässige Person, die gegen Bezahlung meine Ehefrau tötet") oder aber verschlüsselt und nur für Eingeweihte erkennbar abgegeben werden können. Kommt es auf das Angebot hin zu einem entsprechenden Kontakt zwischen dem „Auftraggeber" und dem Täter, liegt in der nachfolgenden konkreten Absprache unzweifelhaft eine Anstiftung, sofern die Tat später durchgeführt wird, bzw. eine versuchte Anstiftung, wenn es nicht zu dieser Tat kommt, die allerdings nach § 30 Abs. 1 Var. 1 StGB wiederum nur dann strafbar ist, wenn es sich bei der geplanten Tat um ein Verbrechen handelt.

34 Fraglich ist allerdings, ob allein in dem ins Internet eingestellten „Angebot" an eine Vielzahl von Personen bereits eine versuchte Anstiftung nach § 30 Abs. 1 Var. 1 StGB zu sehen ist, sofern sich daraufhin niemand meldet oder es jedenfalls nicht zu einer weiteren konkreten Absprache kommt. Die erste Voraussetzung, an der eine Strafbarkeit hier regelmäßig scheitern wird, liegt darin, dass das „Angebot" die für die Tatbegehung unentbehrlichen Angaben enthalten muss[80] (eine Aufforderung „Wer tötet meine Ehefrau" reicht hierfür nicht aus). Allerdings ließen sich durchaus Fälle finden, in denen die Angaben hinsichtlich der konkret durchzuführenden Tat ausreichend sind (so kann der Täter z.B. dazu auffordern, an einem bestimmten Tag einen ganz bestimmten Politiker bei einer genau bezeichneten Veranstaltung zu töten und hierfür eine Belohnung in Aussicht stellen). Allerdings dürfte eine versuchte Anstiftung in diesen Fällen regelmäßig deswegen zu verneinen sein, da sich das „Angebot" im Internet entweder an die Öffentlichkeit oder jedenfalls an eine größere, individuell nicht bestimmbare Personengruppe richtet. Denn es ist anerkannt, dass der Adressat des Anstifters entweder eine bestimmte Person sein muss oder aber sich die (versuchte) Anstiftungshandlung an eine Mehrheit individuell feststellbarer Personen zu richten hat, aus der wenigstens eine sich zur Tatbegehung entschließen soll[81]. Insofern kann zwar die Aufforderung an eine konkrete Person (z.B. durch Versendung einer E-Mail) oder an mehrere konkrete Personen (z.B. durch Versendung einer E-Mail an mehrere Personen, die für den Absender jedoch im Einzelnen individualisierbar sein müssen) als (versuchte) Anstiftung angesehen werden, nicht aber eine Aufforderung in einem Chat-Room, in welchem eine unbestimmte Zahl von Personen teilnehmen (kann). Richtet sich insoweit das „Angebot" des Handelnden an eine unbestimmte Personengruppe, kommt allerdings eine Straftat nach § 111 StGB in Betracht[82].

35 ***c) Verabredung zur Deliktsbegehung***

Keine Besonderheiten sind zu verzeichnen, wenn sich Personen zur Deliktsbegehung über das Internet verabreden. Handelt es sich bei der geplanten Tat um ein Verbrechen (vgl. wiederum § 12 Abs. 1 StGB), so ist der Straftatbestand des § 30 Abs. 2 Var. 3 StGB ein-

[80] *Bloy*, JR 1992, 493 (496); *Geppert*, JURA 1997, 546 (551); *Kühl*, Strafrecht, Allgeminer Teil, 5. Aufl. 2005, § 20 Rn. 249; *Schönke/Schröder-Cramer/Heine* (Fn. 11), § 30 Rn. 19.
[81] BayObLG JR 1999, 81 (83); LK-*Roxin* (Fn.11), § 30 Rn. 24; MüKo-*Joecks* (Fn. 12), § 30 Rn. 28; *Schönke/Schröder-Cramer/Heine* (Fn. 11), § 30 Rn. 20; a.M. allerdings SK-*Hoyer* (Fn. 78), Vor § 26 Rn. 54 f.; § 30 Rn. 27.
[82] MüKo-*Joecks* (Fn. 12), § 30 Rn. 28; *Schönke/Schröder-Cramer/Heine* (Fn. 11), § 30 Rn. 20; a.M. allerdings *Dreher*, Gallas-FS 1973, S. 307 (321), .

schlägig. Voraussetzung ist hierfür, dass sich mindestens zwei Personen zur gemeinsamen mittäterschaftlichen Ausführung eines Verbrechens verabreden[83]. Dabei reicht es allerdings nicht aus, dass die gemeinsame Verabredung nur vage getroffen wird, vielmehr muss der Tatplan bereits rechtlich relevante Konturen angenommen haben[84].

36 ***d) Anleitung zur Begehung von Straftaten***

Eine weitere Möglichkeit strafbaren Verhaltens ist die ins Internet gestellte allgemein gehaltene Anleitung zur Begehung bestimmter Straftaten. Eine solche Anleitung kann wiederum verschiedene Formen annehmen. So ist es auch hier denkbar, dass lediglich Tipps dahingehend abgegeben werden, wie Straftaten leichter durchzuführen sind bzw. das Entdeckungsrisiko bei bereits begangenen Straftaten gesenkt werden kann. Auf der anderen Seite stehen konkrete Anleitungen zum Bau verbotener Gegenstände (z.B. Kriegswaffen oder „Molotow-Cocktails"[85]) oder von Tatwerkzeugen (z.B. „Virenbaukästen" zur Zerstörung fremder Computeranlagen).

37 Als erstes ist hier wiederum an eine Strafbarkeit wegen einer öffentlichen Aufforderung zu Straftaten, § 111 StGB, zu denken.

S. 134 - HFR 11/2006 S. 11 -

38 Darüber hinaus kommt bei einer Anleitung zur Herstellung verbotener Gegenstände (z.B. „Molotow"-Cocktails, deren Herstellung und Besitz nach § 52 Abs. 1 Nr. 1 i.V.m. § 2 Abs. 3 sowie Anlage 2 Abschnitt 1 Nr. 1.3.4 WaffG unter Strafe steht) oder von Tatwerkzeugen (z.B. „Virenbaukästen") eine Strafbarkeit wegen Beihilfe zum jeweils vom Haupttäter begangenen Delikt in Frage. Problematisch ist jedoch auch hier, dass die konkrete Tat, zu welcher der Betreffende Hilfe leistet, zum Zeitpunkt der Einstellung der Anleitung ins Internet weder hinsichtlich der die Tat begehenden Person, noch hinsichtlich Tatzeit und Tatort ausreichend konkretisiert ist, was einer Strafbarkeit regelmäßig entgegenstehen dürfte. Im Einzelnen ist im Hinblick auf die soeben angesprochenen Fälle jedoch zu differenzieren:

39 Im Hinblick auf die genannten „Molotow-Cocktails" ist zu beachten, dass die Anleitung oder Aufforderung zur Herstellung solcher (waffenrechtlich verbotener) Gegenstände bereits eine selbstständige Strafbarkeit nach § 52 Abs. 1 Nr. 4 i.V.m. § 40 WaffG begründet. Unter dem Begriff Anleitung versteht man hierbei die Vermittlung von Informationen, die dem Empfänger die Möglichkeit gibt, auf Grund der erworbenen Kenntnisse den entsprechenden Gegenstand selbst herzustellen. Unter einer Aufforderung[86] ist dagegen ein Verhalten zu verstehen, welches von einem anderen erkennbar die Herstellung der verbotenen Gegenstände (z.B. der angesprochenen „Molotow-Cocktails") verlangt.[87] Die Aufforderung muss sich nicht an einen individuellen Adressaten richten, sondern kann auch darin liegen, dass sie öffentlich in einer Versammlung oder durch Verbreiten von Schriften vor sich geht. Insoweit ist jedenfalls auch derjenige, der eine entsprechende Anleitung in eine Mailbox im Internet einstellt, die anderen Personen zugänglich ist, nach dieser Vorschrift strafbar. Bei einer bloßen Weiterleitung entsprechender Texte (per E-Mail oder Einstellung in eine Mailbox) ist jedoch einschränkend zu fordern, dass der Weiterleitende sich den Text zu eigen macht und daher auch selbst zur Herstellung des ver-

[83] BGH NStZ 1988, 406; BGH NStZ 1993, 137; *Jescheck/Weigend*, Lehrbuch des Strafrechts. Allgemeiner Teil, 5. Aufl. 1995, § 65 III 1; *Kühl* (Fn. 80), § 20 Rn. 252; *Roxin*, Strafrecht. Allgemeiner Teil Band II, 2003, § 28 Rn. 43; *Schönke/Schröder-Cramer/Heine* (Fn. 11), § 30 Rn. 25; SK-*Hoyer* (Fn. 78), § 30 Rn. 3, 46.
[84] *Kühl* (Fn. 79), § 20 Rn. 253; LK-*Roxin* (Fn. 11), § 30 Rn. 66; NK-*Zaczyk* (Fn. 11), § 30 Rn. 52; *Schönke/Schröder-Cramer/Heine* (Fn. 11), § 30 Rn. 25; a.M. *Jescheck/Weigend* (Fn. 83), § 65 III 1; vgl. auch *Dessecker*, JA 2005, 549 (551 f.).
[85] Bei diesen so genannten „Molotow-Cocktails" handelt es sich um mit Benzin, Benzin-Ölgemisch oder anderen leicht brennbaren Flüssigkeiten gefüllte Glasflaschen, die vor allem nach einem Wurf beim Auftreffen auf einen heißen Gegenstand zersplittern, wobei sich der dadurch freigewordene Brennstoff ohne Zuhilfenahme einer weiteren Zündvorrichtung entzündet.
[86] Zum Begriff des „Aufforderns" vgl. auch § 29 Abs. 1 Nr. 12 BtMG, § 23 VersammlG.
[87] RGSt 63, 170 (173).

botenen Gegenstandes anleitet[88]. Ist dies der Fall, kommt Idealkonkurrenz zur Strafvorschrift des § 111 StGB in Frage.

40 Im Hinblick auf die Anbieter so genannter „Virus Construction Kits" (Virenbaukästen), die sich dadurch auszeichnen, dass mit ihrer Hilfe auch technisch weniger begabte Personen in der Lage sind, einen funktionierenden Computervirus zu erzeugen, den sie später ins Netz stellen oder durch Versendung an konkrete Personen verbreiten[89], ist dagegen eine Beihilfe zur jeweils durch den späteren „Virenkonstrukteur" begangenen Haupttat zu prüfen. Bei dieser Haupttat handelt es sich regelmäßig um ein Delikt nach § 303a StGB bzw. § 303b StGB[90]. Fraglich ist hier allerdings – wie bereits oben angesprochen –, ob das bloße Zugänglichmachen solcher Informationen bzw. das Zurverfügungstellen der Virenbausteine über das Internet als „Hilfeleistung" i.S. des § 27 StGB angesehen werden kann. Dabei ist als erstes anzumerken, dass sich in dieser Konstellation das Problem der „schillernden" Rechtsfigur der neutralen Handlung und die Frage, ob und wie Alltagshandlungen zu einer Einschränkung der Beihilfestrafbarkeit führen können[91] nicht stellt, da das Einstellen solcher Virenbaukästen jedenfalls nicht als neutrale Handlung angesehen werden kann. Zielrichtung ist die Schädigung fremder Computersysteme, sodass ein eindeutiger „deliktischer Sinnbezug" gegeben ist[92]. Fraglich erscheint jedoch die Bestimmtheit der Haupttat. Denn der Gehilfe muss nicht nur zu einer vorsätzlich begangenen rechtswidrigen Tat eines anderen Hilfe leisten, er muss vielmehr diesbezüglich auch vorsätzlich handeln. Dabei muss der Gehilfenvorsatz im Hinblick auf die Haupttat zwar weniger konkret sein als bei der Anstiftung[93]. Dennoch muss aber die jeweilige Tat für den Gehilfen bei Erbringung seiner Hilfeleistung in gewissen Umrissen bekannt sein[94]. Dies ist in der vorliegenden Konstellation nicht anzunehmen, da demjenigen, der die Virenbaukästen im Internet zur Verfügung stellt, weder bekannt ist, welche Personen die entsprechende Seite aufrufen, noch wann dies geschieht. Auch weiß er nicht, wer sich wann welche Bausteine herunterlädt und vor allem wer wann und gegen wen einen entsprechenden Angriff richtet. Insofern erfüllt das Zurverfügungstellen von Virenbausteinen im Internet die Anforderung an eine strafbare Beihilfehandlung nicht[95].

S. 135

41 **4. Sabotage durch Ressourcenüberlastung**

a) Aufforderung zur Sabotage / E-Protest

Ein internetspezifisches Sonderproblem stellte sich jüngst in einem Fall, in dem der Täter öffentlich dazu aufforderte, an einem bestimmten Tag den Server einer bestimmten Firma (im konkreten Fall: der Lufthansa) durch eine Vielzahl von E-Mail Anfragen so zu überlasten, dass dieser zum Absturz gebracht werden und dadurch der Betrieb (hier: die Entgegennahme und Abbuchung elektronischer Flugbuchungen) jedenfalls kurzfristig nicht mehr möglich sein sollte[96]. In diesem Fall kommt eine Strafbarkeit wegen einer öffentlichen Aufforderung zu Straftaten nach § 111 StGB in Frage, was jedoch voraussetzt, dass die durch die Aufforderung Angesprochenen bei dem „Boykott" der fremden Web-Seite selbst eine Straftat begehen. Das AG Frankfurt[97] sah in diesem Verhalten eine strafbare Nötigung nach § 240 StGB, was jedoch unter mehreren Gesichtspunkten bedenklich ist. So kann schon der „Mausklick", mit welchem der Internetnutzer die entsprechende E-Mail

[88] BayObLG NJW 1998, 1087; kritisch hierzu auch *Gänßle*, NStZ 1999, 90.
[89] Vgl. hierzu *Malek* (Fn. 7), Rn. 181; *Vetter* (Fn. 7), S. 95 ff.
[90] LG Ulm CR 1989, 825 – Killerprogramm: *Eichelberger*, MMR 2004, 594 (595 f.); *Hilgendorf/Frank/Valerius* (Fn. 3), Rn. 201; *Malek* (Fn. 7), Rn. 174.
[91] Vgl. hierzu *Heinrich* (Fn. 71), Rn. 1330 ff.
[92] Vgl. *Malek* (Fn. 7), Rn. 181; differenzierend *Eichelberger*, MMR 2004, 594 (597).
[93] Vgl. *Heinrich* (Fn. 71), Rn. 1337.
[94] BGHSt 11, 66; vgl. ferner BGHSt 42, 135 (138); BGHSt 46, 107 (109).
[95] So auch *Vetter* (Fn. 7), S. 115; differenzierend *Eichelberger*, MMR 2004, 594 (597); a.M. *Malek* (Fn. 7), Rn. 181.
[96] Vgl. AG Frankfurt NStZ 2006, 399; vgl. hierzu die Anmerkungen bei *Gercke*, MMR 2005, 868; *Kraft/Meister*, K&R 2005, 458; zu dieser Problematik auch *Kraft/Meister*, MMR 2003, 366.
[97] Zustimmend allerdings *Kraft/Meister*, MMR 2003, 366 (370 f.).

absendet nur schwerlich als „Gewaltanwendung" i.S. des § 240 StGB angesehen werden. Abgesehen davon, ob eine derart geringe körperliche Kraftentfaltung (durch den Mausklick) bereits als „Gewalt" gewertet werden kann[98], ist die Annahme, eine physische Zwangswirkung auf das Leitungsnetz stelle jedenfalls eine mittelbare physische Zwangswirkung im Hinblick auf die übrigen Internetnutzer dar, denen dadurch der Zugriff auf die betreffende Web-Seite verwehrt wird, kaum nachvollziehbar[99]. Auch ist die Konstruktion einer Dreiecksnötigung – der Betreiber der Web-Seite werde durch die Gewalt gegenüber den ihm nahestehenden (potentiellen) Internetkunden selbst genötigt – ebenfalls fraglich. Insoweit scheidet eine Strafbarkeit nach § 240 StGB aus.

42 Es kommt allerdings eine Strafbarkeit nach §§ 303a, 303b StGB in Frage[100]. Hinsichtlich der Strafbarkeit wegen Datenveränderung, § 303a StGB, muss geprüft werden, ob das Merkmal des „Unterdrückens" von Daten bereits dann vorliegt, wenn dem Berechtigten die Daten lediglich vorübergehend und nicht auf Dauer entzogen werden (im konkreten Fall war die Benutzung der Web-Seite für etwa zwei Stunden nicht oder nur mit erheblichen Wartezeiten möglich). Hinsichtlich des Tatbestandsmerkmals des Unterdrückens ist jedoch anerkannt, dass eine dauerhafte Unterdrückung nicht erforderlich ist, sondern dass es ausreicht, wenn die Daten zeitweilig entzogen werden, sofern es sich nicht um einen ganz unerheblichen Zeitraum handelt[101]. Bei der Frage der Erheblichkeit des Zeitraums ist allerdings auch die tatsächlich erlittene Beeinträchtigung von entscheidender Bedeutung[102]. Jedenfalls dann, wenn der Verfügungsberechtigte, welcher in aller Regel der Betreiber der Web-Seite sein dürfte, nicht mehr auf seine eigenen Daten zugreifen kann, ist daher der Tatbestand erfüllt[103], sofern es sich nicht um einen ganz unerheblichen Zeitraum handelt[104]. Fraglich ist jedoch, ob dies auch im Hinblick auf Dritte gelten kann, die infolge der Überlastung nicht mehr auf die entsprechende Web-Seite zugreifen können. Da § 303a StGB jedoch lediglich den Verfügungsberechtigten vor der Veränderung seiner Daten schützen soll, ist diese Konstellation von der Strafnorm nicht erfasst[105]. Ferner ist zu berücksichtigen, dass die Tathandlungen der einzelnen Internutzer für sich gesehen für ein Unterdrücken von Daten nicht ausreichen, sodass eine Strafbarkeit nur durch eine Annahme einer mittäterschaftlichen Zurechung (§ 25 Abs. 2 StGB) der Tatbeiträge der übrigen „Boykotteure" möglich ist. Diesbezüglich müsste dann aber ein gemeinsamer Tatplan nachgewiesen werden.

43 Darüber hinaus gehend werden in den genannten Fällen aber auch die Voraussetzungen des § 303b StGB erfüllt sein. Sofern die Voraussetzungen des § 303a Abs. 1 StGB angenommen werden, liegt es nahe, dass hierdurch auch eine Datenverarbeitung, die für das betroffene Unternehmen von wesentlicher Bedeutung ist, gestört wird. Ferner kommt auch eine Strafbarkeit nach § 317 StGB in Frage, da die betroffenen Server Telekommunikationseinrichtungen in diesem Sinne darstellen (vgl. auch die Definition in § 3 Nr. 23 TKG).

S. 136

44 ***b) DDoS-Attacken***

In Ihrer Wirkung mit den vorgenannten „E-Protesten" vergleichbar sind die so genannten.

---

[98] AG Frankfurt NStZ 2006, 399; zustimmend *Kraft/Meister*, MMR 2003, 366 (370 f.); *dies.*, K&R 2005, 458 (459); das Urteil des AG Frankfurt wurde durch die Revisionsentscheidung des OLG Frankfurt vom 22.5.2006 – 1 Ss 319/05 (bisher unveröffentlicht; Fundstelle juris) aufgehoben.
[99] Zustimmend dagegen *Kraft/Meister*, K&R 2005, 485 (459).
[100] So auch *Gercke*, MMR 2005, 868; *Kraft/Meister*, MMR 2003, 366 (370 f.); ferner *Ernst*, NJW 2003, 3233 (3239).
[101] LK-*Tolksdorf* (Fn. 11), § 303a Rn. 27; NK-*Zaczyk* (Fn. 11), § 303a Rn. 8; *Schönke/Schröder-Stree* (Fn. 11), § 303a Rn. 4; a.M. *Altenhain*, JZ 1997, 752 (753 Fn. 17).
[102] *Vetter* (Fn. 7), S. 66.
[103] *Hilgendorf/Frank/Valerius* (Fn. 3), Rn. 197; *Vetter* (Fn. 7), S. 67 ff.
[104] Das OLG Frankfurt (Fn. 98) lehnte im vorliegenden Fall die Erheblichkeit bei einem Zeitraum von zwei Stunden ab.
[105] *Faßbender*, Angriffe auf Datenangebote im Internet und deren strafrechtliche Relevanz, 2003, S. 61; *Hilgendorf/Frank/Valerius* (Fn. 3), Rn. 197; *Kraft/Meister*, MMR 2003, 366 (373); *Vetter* (Fn. 7), S. 66 f.; a.M. *Ernst*, NJW 2003, 3233 (3238).

„DDoS-Attacken" (Distributed-Denial-of-Service-Attacken), deren rechtliche Einordnung umstritten ist[106]. Allgemein versteht man unter einer solchen DDoS-Attacke einen Angriff, der darauf abzielt, bestimmte Dateien zu löschen oder Dienste (z.B. den WWW-Server) in einer Weise zu blockieren, dass sie nicht mehr im Rahmen ihrer Anforderungen nutzbar sind[107]. Dabei können solche Angriffe in verschiedenen Formen vorkommen.

45 Eine Variante besteht darin, dass sich der Angreifer zuerst Zugang zu einer Vielzahl von fremden Rechnern im Internet verschafft, auf denen er die Programme für den Angriff installiert. Von einem separaten Rechner aus synchronisiert er dann die Angriffsprogramme in der Weise, dass von diesen aus gleichzeitig ein Angriff auf den attackierten Rechner stattfindet. Die Wirkungen entsprechen dann denen der vorgenannten „E-Proteste"[108], wobei der Unterschied darin besteht, dass der Angriff nur von einer Person ausgeht, die sich dazu aber einer Vielzahl fremder Rechner bedient. Hier kommt zuerst eine Strafbarkeit nach § 303a StGB wegen Datenveränderung in Frage[109]. Wird durch den massiven Zugriff auf eine Web-Seite deren Server überlastet, so kann dies dazu führen, dass die auf diesem Server verfügbaren Daten für einen gewissen Zeitraum nicht mehr erreichbar sind. Kann daher der Verfügungsberechtigte (d.h. der Betreiber der Web-Seite) nicht mehr auf seine eigenen Daten zugreifen, ist eine Datenunterdrückung gegeben[110], sofern es sich nicht um einen ganz unerheblichen Zeitraum handelt[111]. Dass möglicherweise Dritte (andere Internet-Nutzer) infolge der Überlastung nicht mehr auf die entsprechende Web-Seite zugreifen können, ist auch in der vorliegenden Konstellation strafrechtlich unbeachtlich, da § 303a StGB nur den Verfügungsberechtigten vor der Veränderung seiner Daten schützen soll[112]. Auch in den Fällen der „DDoS-Attacken" ist aber wiederum an eine Strafbarkeit nach § 303b StGB wegen Computersabotage[113] sowie nach § 317 StGB zu denken[114].

46 **III. Fazit**

Die Ausführungen haben gezeigt, dass sich durch die Entwicklung des Internet hin zu einem Massenkommunikationsmittel eine Vielzahl neuer (straf-)rechtlicher Probleme eröffnen, die jedoch mit den derzeit geltenden Strafbestimmungen weitgehend erfasst werden können. Dort, wo sich strafrechtliche Lücken auftun (wie im Bereich des „Phishing" oder dem Download urheberrechtlich geschützter Werke), muss man sich fragen, ob ein Strafrechtsschutz hier sinnvoll und gewollt ist oder ob der Gesetzgeber nicht besser damit fährt, den „fragmentarischen Charakter" des Strafrechts aufrecht zu erhalten und das Strafrecht nur dort einzusetzen, wo es als „ultima ratio" zwingend erforderlich ist, um sozialschädlichen Verhaltensweisen zu begegnen.

47 Lediglich kurz soll am Ende dieses Beitrages allerdings noch auf eine ganz neue Dimension hingewiesen werden, die das Medium des Internet in das deutsche Strafrecht trägt: Die Internationalisierung des Strafrechts und die Frage, ob und inwieweit Verhaltensweisen durch den nationalen Rechtsanwender sanktioniert werden sollen und dürfen, die einen wesentlichen Auslandsbezug aufweisen, sei es, dass sich die Handelnden oder die potenziellen Opfer im Ausland aufhalten, sei es, dass sich der Server, auf welchem die fraglichen Daten abgelegt wurden, im Ausland befindet. Kann eine Beleidigung eines australischen Staatsbürgers, begangen durch eine schriftliche Äußerung eines anderen Australiers, die in Australien auf einem dortigen Server abgelegt ist, vor deutschen Strafgerichten abgeurteilt werden, nur weil die entsprechende Web-Seite auch in Deutschland abgerufen werden kann? Gilt dies auch für einen Aufruf zum Mord? Spielt dabei die verwende-

[106] Vgl. hierzu *Faßbender* (Fn. 105); *Hilgendorf/Frank/Valerius* (Fn. 3), Rn. 724 f.; *Möller*, DuD 2000, 292; *Vetter* (Fn. 7), S. 51 ff.
[107] *Hilgendorf/Frank/Valerius* (Fn. 3), Rn. 724.
[108] Vgl. hierzu oben II 4 a).
[109] *Faßbender* (Fn. 105), S. 49 ff.; *Hilgendorf/Frank/Valerius* (Fn. 3), Rn. 725; *Vetter* (Fn. 7), S. 55 ff.
[110] *Faßbender* (Fn. 105), S. 60; *Hilgendorf/Frank/Valerius* (Fn. 3), Rn. 197; *Vetter* (Fn. 7), S. 67 ff.
[111] Vgl. hierzu bereits oben II 4 a).
[112] *Hilgendorf/Frank/Valerius* (Fn. 3), Rn. 197; *Vetter* (Fn. 7), S. 55 ff.; a.M. *Ernst*, NJW 2003, 3233 (3238).
[113] *Faßbender* (Fn. 105), S. 67 ff.; *Hilgendorf/Frank/Valerius* (Fn. 3), Rn. 725; *Vetter* (Fn. 7), S. 71 ff.
[114] *Hilgendorf/Frank/Valerius* (Fn. 3), Rn. 725.

te Sprache eine Rolle? All dies sind Fragen, zu denen schon vielfach Stellung genommen wurde, ohne dass bisher eine wirkliche Klärung erreicht wurde. Doch auch hier gilt die oben gewonnene Erkenntnis, dass das geltende Strafrecht in seinen dogmatischen Strukturen und ausformulierten Straftatbeständen in der Lage sein muss und auch in der Lage sein wird, diese neu auftretende Problematik einer zufrieden stellenden Lösung zuzuführen.

Zitierempfehlung: Bernd Heinrich, HFR 2006, S. 125 ff.