ZIS
Zeitschrift für Internationale Strafrechtsdogmatik
http://www.zis-online.com

AUSGABE 8-9/2012
S. 395 - 485
7. Jahrgang

Inhalt

ISSN
1863-6470

Einführung zur Sonderausgabe der ZIS: Cybercrime & Cyberjustice

Von Dr. **Christoph Burchard**, LL.M. (NYU), München*

Diese Sonderausgabe der ZIS geht aus der Tagung „Cybercrime: Ein deutsch-türkischer Strafrechtsdialog“ hervor, die vom 12. bis 15. Oktober 2011 an der Bilgi Universität in Istanbul, Türkei, stattfand. Erst eine Vielzahl von Unterstützern ermöglichte dieses internationale Format, insbesondere die Bilgi Universität Istanbul, die Anwaltskammer Istanbul, der türkische Strafrechtsverein, die Deutsche Landesgruppe der AIDP e.V.[1] sowie all jene deutschen Forschungsinstitutionen, Ministerien und Kanzleien, die die Reisekosten ihrer Referenten übernommen haben. Auf Einladung der Jeunes Pénalistes der deutschen und türkischen Landesgruppe der Association Internationale de Droit Pénal (AIDP) diskutierten angesehene Wissenschaftler, Praktiker sowie der wissenschaftliche Nachwuchs aus Deutschland, der Türkei und dem europäischen Ausland über ein Thema, das aufgrund seiner Aktualität und Brisanz just vor wenigen Tagen den Deutschen Juristentag[2] beschäftigt hat, im Jahr 2014 den Gegenstand des XIX. AIDP-Weltkongresses[3] („Informationsgesellschaft und Strafrecht“) bilden wird, und hier mit den plakativen Schlagworten „Cybercrime & Cyberjustice“ zusammengefasst wurde.

Dass diese Chiffren randunscharf sind, liegt in der Natur der Sache bzw. der damit angesprochenen, globalisierten Phänomenbereiche: Im Zusammenspiel von Informationstechnologie und Datenverarbeitung einerseits sowie von (potentiell) sozialschädlichem Verhalten und Strafrechtspflege andererseits entwickelt sich stetig „Neues“. Dabei ist das „Cyber“ zugleich Problem und Lösung. Es wird zum Problem, wenn z.B. Straftaten durch oder auf informationstechnische Systeme verübt werden, sei es, dass die Unbedarftheit der Nutzer im Umgang mit diesen ausgenutzt wird (Stichwort: Phishing), sei es, dass hochspezialisiertes Insiderwissen zum Einsatz kommt (Stichwort: Stuxnet). Das „Cyber“ verheißt aber auch Lösungen, insbesondere für eine Kriminalpolitik, die sich zusehends als Politik der effektiven inneren Sicherheit (miss-)versteht, wenn etwa Strafakten in Zukunft ausschließlich elektronisch geführt werden sollen oder gar der globalen bzw. zumindest europäisch-regionalen Vernetzung der Sicherheits- und Strafverfolgungsbehörden samt ihrer Datenbanken das Wort geredet wird.

Für einen rechtsstaatlichen Umgang mit „Cybercrime & Cyberjustice“ gibt es keine Patentrezepte. Gleichwohl sei hier an zwei Selbstverständlichkeiten erinnert, die im nationalen und internationalen Diskurs freilich mitunter in Vergessenheit zu geraten scheinen: Zum ersten ist vor einer Überschätzung und einseitigen Überlastung des Strafrechts bei der Bewältigung von Cybercrime zu warnen. Der Rückgriff auf das Strafrecht muss, auch und gerade im Einzelfall, ein legitimes Ziel verfolgen und verhältnismäßig sein; insofern gilt es, die Grenzen strafwürdiger bzw. strafbedürftiger Verhaltensweisen aufs Neue zu vermessen und ggf. nichtstrafrechtliche Regelungen in Betracht zu ziehen. Überdies ist der Gemeinplatz „Gelegenheit macht Diebe“ umzuformulieren in „Sicherheitslücken machen Cyberkriminelle“; diese Sicherheitslücken, die vom Nutzer häufig nicht gesehen werden, sind durch Information und Prävention zu schließen. Zum zweiten ist staatliche, europäische oder internationale Herrschaft, die sich vermittels Cyberjustice vollzieht, datenschutzrechtlich einzugrenzen und datenschutztechnisch abzusichern. Dass gilt insbesondere, wenn Zwangs- bzw. Ermittlungsmaßnahmen rein „virtuell“ erfolgen (Stichwort: Rasterabgleich von Datensätzen, z.B. von Kreditkartendaten). Ein blindes Vertrauen in staatliche Datenverarbeitung und Datenverarbeitungssysteme widerspräche allen europäischen Rechtsstaatsidealen.

Die folgenden Beiträge bilden die hohe rechtliche wie technische Komplexität sowie die große thematische Bandbreite von „Cybercrime & Cyberjustice“ vorzüglich ab. Zunächst wird die Strafbarkeit einzelner Cyber-Verhaltensweisen aus verschiedenen Perspektiven näher untersucht (*Heger*, *Eisele*, *Hoffmans*, *Seidl*, *Cekin*, *Oglakcioglu*, *Schuhr*), um sodann strafanwendungsrechtlich hinterfragt (*Wörner*) und aus der Sicht der Verteidigung eingeordnet zu werden (*Groß*). Im Anschluss wird der Einsatz informationstechnischer Systeme im Rahmen und zur Effektuierung der Strafverfolgung kritisch reflektiert (*Rettenmaier/Palm*, *Brodowski*, *Vogel*).

Mein Dank gilt der AIDP, unter deren Trägerschaft sich in Istanbul ein echter Dialog über Grenzen hinweg und über die akuten, grenzüberschreitenden Herausforderungen an das Strafrecht entwickeln konnte. Abschließend möchte ich mich nochmals ganz herzlich bei Ass.-Prof. Dr. *Ragip Bariş Erman* von der Bilgi Universität Istanbul, Türkei, sowie seinem Team bedanken. Nur durch seinen unermüdlichen Einsatz konnte die Istanbuler Konferenz jener Erfolg werden, der sich in dieser ZIS-Sonderausgabe widerspiegelt. Damit geht die Hoffnung einher, dass der deutsch-türkische Strafrechtsdialog auch in Zukunft weitere Früchte tragen wird.

* *Christoph Burchard* ist Akad. Rat a.Z. und habilitiert sich am Lehrstuhl für Strafrecht, Strafprozessrecht und Wirtschaftsstrafrecht, Prof. *Dr. Joachim Vogel*, RiOLG, Ludwig-Maximilians-Universität, München.

[1] Mehr Informationen zu Aufbau und Programm finden sich online unter http://www.aidp-germany.de.

[2] Vgl. das Gutachten von *Sieber* für den 69. djt mit dem Thema „Straftaten und Strafverfolgung im Internet“.

[3] Mehr Informationen finden sich online unter http://www.penal.org.

Strafbarkeit von Glücksspielen, Sportwetten und Hausverlosungen via Internet im Lichte des Europarechts*

Von Prof. Dr. **Martin Heger**, Berlin**

I. Einleitung

Glücksspiele und auch (Sport-)Wetten sind kein neues Phänomen. Dass es dabei nicht immer mit rechten Dingen zugegangen ist, zeigen nicht nur mediale Aufbereitungen wie der Film „Der Clou“ (1973). Auch wenn überall in der Welt mondäne Casino-Bauten den Anschein vollkommener Legalität dieses Gewerbes vermitteln, war und ist es doch seit jeher auch ein Tummelplatz der Halb- und Unterwelt. Glücksspiele fanden nicht nur im grellen Licht der Kronleuchter statt, sondern immer schon auch in abgedunkelten Hinterzimmern. Und der Glanz großer Pferderennen mit riesigen Wettumsätzen an den Totalisatoren kann nicht verdecken, dass in allen Teilen der Welt auf alle möglichen Ereignisse Wetten platziert werden können. Dabei waren nicht nur diese Wetten vielfach illegal; vielmehr kam es auch immer wieder zu Manipulationen der bewetteten Ereignisse. Die Geschichte des „Clou“ ist nicht bloße Fiktion. Das zeigt schon der Blick auf den sog. „Spätwetten“-Fall des Bundesgerichtshofs,[1] dem die gleiche Konstellation zugrunde lag: Zeitverschiebungen bei der Mitteilung des Rennausgangs sollten zu manipulierten Pferdewetten ausgenutzt werden. Derzeit haben in der Realität manipulierte Fußballwetten weltweit Hochkonjunktur. In Deutschland steht dafür symbolisch – aber längst nicht mehr allein – der Fall „Hoyzer“[2] und in Italien ermittelt die Staatsanwaltschaft derzeit ebenfalls wegen betrügerisch manipulierter Fußballwetten.[3]

II. Internationale Vermittlung

Nicht neu ist es auch, dass dabei Gelder von einem in ein anderes Land transferiert, ja sogar kriminelles Kapital „gewaschen“ wird. Heute wie vor hundert Jahren engagieren sich beispielsweise Russlands Reiche an den Roulette-Tischen der Cote d‘Azur wie der Riviera. Aus Sicht des Glücksspielrechts wie des Glücksspielstrafrechts ist das kein besonderes Problem, denn nach dem Territorialitätsprinzip (§§ 3, 9 StGB) ist das Recht anzuwenden, das am Tatort – d.h. dem Casinostandort – gilt. Hier kann die Polizei kontrollieren, können Razzien durchgeführt, Verdächtige verhaftet werden etc.

Allerdings gab es auch schon in früheren Jahrzehnten Vermittlungsbüros für Sportwetten weltweit. So konnten Wetten in einem Land platziert werden, seit die Ergebnisse z.B. eines Pferderennens via Fernsprecher (Telefon) übermittelt werden konnten. Davon leben ja auch der Plot des „Clou“ wie der Sachverhalt der „Spätwetten“. Vereinfacht wurde dies dann, als im Fernsehen Pferderennen aus aller Welt in ein Wettbüro übertragen wurden. Damit stellte sich bereits die Frage, ob etwa die Vermittlung einer Wette auf ein dortiges Ereignis ins Ausland im Inland nach inländischem Recht verboten und strafbar sein kann.

Diese Situation hat sich inzwischen durch das Internet massiv verändert.[4] Nunmehr kann sich jeder Spieler nicht nur frei über nahezu alle Sportereignisse informieren (um dann allerdings an seinem Standort eine Wette zu platzieren); er kann sich auch an Wett- und Glücksspielangeboten via Internet von überall beteiligen.[5] Vereinfacht wird dies freilich weiterhin vielfach durch Wettbüros, die in allen deutschen Städten vor allem ausländische Wettangebote an deutsche Kunden vermitteln und dabei natürlich das Internet als Kommunikationsmittel nutzen.

III. Das deutsche Strafrecht als Grenze

Beidem – der Beteiligung am Glücksspiel im Internet wie auch der Vermittlung von ausländischen Wettangeboten in Sportwettbüros – steht derzeit das deutsche Strafrecht entgegen. Strafbar ist nach § 284 Abs. 1 StGB nämlich das Veranstalten eines Glücksspiels, wozu von der ganz h.M. in Deutschland auch Sportwetten nach festen Quoten („Oddset-Wetten“) gezählt werden,[6] ohne staatliche Konzession,[7] und zwar auch dann, wenn das Angebot von einem ausländischen Anbieter kommt und Deutsche daran von Deutschland aus nur – z.B. via Internet – teilnehmen können.[8] Renn- und Sportwetten aufgrund eines vom Veranstalter festgelegten Spielplans (Toto) unterfallen als Lotterien i.S.v. § 287 StGB

---

* Um Nachweise erweiterter Vortrag, der im Oktober 2011 an der Bilgi-Universität Istanbul gehalten worden ist. – Die im Zuge des Glücksspieländerungsstaatsvertrags, der seit Juli 2012 in allen Bundesländern mit Ausnahme Schleswig-Holsteins gilt, vereinbarten Änderungen des Glücksspiel- und Sportwettrechts sowie die derzeit abweichende Rechtslage in Schleswig-Holstein sind eingefügt worden; eine umfassende Analyse der derzeit „noch im Fluss befindlichen“ Rechtslage (insbesondere in Schleswig-Holstein) war im Format dieses Vortrags nicht möglich.

** Der *Verf.* lehrt Strafrecht, Strafprozessrecht, europäisches Strafrecht und neuere Rechtsgeschichte an der Humboldt-Universität zu Berlin.

[1] BGHSt 16, 120.

[2] BGHSt 51, 165. Dazu ausführlich *Koch*, Betrug bei der Sportwette, 2007, passim.

[3] Dazu *Ferragina*, Betrügereien im Profifußball in Deutschland und Italien, 2012, passim.

[4] Dazu grundsätzlich *Mintas*, Glücksspiele im Internet, 2009, passim; *Volk*, Glücksspiel im Internet, 2005, passim.

[5] Zu Internet-„Auktionen“ als strafbares Glücksspiel gem. § 284 StGB vgl. den gleichnamigen Beitrag von *Rotsch/Heissler*, ZIS 2010, 403.

[6] BGH NStZ 2003, 372 (373); BGH NStZ 2007, 151 (153); *Fischer*, Strafgesetzbuch und Nebengesetze, Kommentar, 59. Aufl. 2012, § 284 Rn. 10. A.A. noch LG Bochum NStZ-RR 2002, 170, und AG Karlsruhe-Durlach NStZ 2001, 254: Geschicklichkeitsspiel.

[7] Dazu nur *Lackner/Kühl*, Strafgesetzbuch, Kommentar, 27. Aufl. 2011, § 284 Rn. 12.

[8] *Krehl*, in: Laufhütte/Rissing-van Saan/Tiedemann (Hrsg.), Strafgesetzbuch, Leipziger Kommentar, Bd. 10, 12. Aufl. 2008, § 284 Rn. 20a.

ebenfalls dem deutschen Glücksspielstrafrecht (§§ 284 ff. StGB).[9] Da aber Deutschland nur die Veranstaltung eines Glücksspiels zumindest mit einer Zugangsmöglichkeit – wie bei Angeboten im Internet – auch im Inland konzessionieren kann (und nicht etwa Glücksspielangebote im Ausland ohne jede Erstreckung auch in das Inland), ist es im Lichte des deutschen Strafrechts straflos, im Ausland ein nicht unmittelbar vom Inland zugängliches Glücksspiel nach dortigem Recht legal zu betreiben (§ 7 Abs. 2 Nr. 1 StGB macht die Anwendbarkeit deutschen [Glücksspiel-]Strafrechts von der Tatortstrafbarkeit abhängig). Monacos Casinos müssen sich also nicht um eine deutsche Konzession bemühen und deutsche Staatsbürger können im Fürstentum sanktionslos ihr Vermögen aufs Spiel setzen.

Seit 1998 strafbar ist jede Werbung in Deutschland für ein solches öffentliches Glücksspiel, d.h. ein Glücksspiel- oder Wettangebot, das nicht durch deutsche Stellen konzessioniert ist (§§ 284 Abs. 4, 287 Abs. 2 StGB).[10] Damit ist nicht gemeint, dass generell – etwa zum Schutz vor Spielsucht – Werbung für Glücksspiele in Deutschland bei Strafe verboten sein soll. So ist es nicht strafbar, für in Deutschland konzessionierte Glücksspiel- und Wettangebote vor allem des Deutschen Toto-/Lotto-Blocks Werbung zu machen; inzwischen halten sich deutsche Anbieter freilich mit Werbung zurück, weil sie fürchten, anderenfalls mit dem Europarecht in Konflikt zu geraten.

Nicht strafbar ist es allerdings weiterhin, im Inland für nicht nach deutschem Recht zu konzessionierende Glücksspielangebote Werbung zu machen, weil in § 284 Abs. 4 StGB ausdrücklich nur die Werbung für in Abs. 1 und 2 unter Strafe gestellten unerlaubten Glücksspiele erfasst ist; erfasst ist damit eigentlich nur die Werbung für im Ausland abgehaltene Glücksspiel- und Wettangebote, sofern sich ein Spieler aus dem Inland via Telekommunikationseinrichtungen (Telefon, Fax, vor allem aber heute Internet) daran beteiligen kann.[11] Wer also im Anzeigenteil einer deutschen Zeitschrift darauf hinweist, dass man in Monaco wunderbar sein Glück herausfordern kann, steht nicht mit einem Fuß im Gefängnis. Die Strafbarkeit wegen Werbung für Glücksspiel, Sportwette und Lotterie ist vielmehr eine Antwort des deutschen Gesetzgebers auf die Möglichkeit einer Teilnahme an im Ausland abgehaltenen Glücksspielen insbesondere via Internet.

Schließlich strafbar ist die Beteiligung an einem unerlaubten Glücksspiel (§ 285 StGB). Unerlaubt ist das Glücksspiel wiederum bereits dann, wenn es an einer deutschen staatlichen Konzession dafür fehlt, so dass in der Tat ein Deutscher, der sich aus Deutschland an einem im Ausland ansässigen Internet-Glücksspiel beteiligt,[12] strafbar sein kann, auch wenn der Veranstalter des Glücksspiels an seinem Sitz nach dortigem Recht legal handelt, z.B. weil er eine (im Inland nicht wirksame) Konzession seines Heimatstaates erlangt hat.

[9] *Krehl* (Fn. 8), § 284 Rn. 5.
[10] BGBl. I 1998, S. 164, 180.
[11] Näher dazu *Krehl* (Fn. 8), § 284 Rn. 25.
[12] Vgl. *Krehl* (Fn. 8), § 284 Rn. 20a.

IV. Der Einfluss des Europarechts

Da das nach deutschem Strafrecht auch dann gelten soll, wenn dieser Staat ein Mitglied der Europäischen Union ist, stellt sich die Frage, ob eine so weit gehende nationale Strafnorm mit den Grundfreiheiten des Europarechts vereinbar ist.[13] Diese Frage stellt sich dabei nicht nur für das deutsche Recht, sondern auch für eine Anzahl anderer EU-Staaten, deren Glücksspiel-Regime ähnlich restriktiv wie das deutsche ausgestaltet ist. Die Frage hat den EuGH im letzten Jahrzehnt wiederholt beschäftigt. Der erste „leading case" – der Fall Gambelli aus dem Jahr 2003[14] – betraf dabei die Rechtslage in Italien[15]; weitere Verfahren betrafen die Niederlande[16] und Portugal[17], bevor im Herbst 2010 auch die Glücksspiel-Regelungen Deutschlands auf den Prüfstand des Europarechts gelangt sind;[18] zeitgleich wurde auch die Rechtslage in Österreich in Luxemburg hinterfragt.[19] Dem EuGH geht es dabei nicht im Detail um die Ausgestaltung des nationalen Glücksspielstrafrechts, etwa in Form der deutschen §§ 284-287 StGB; da eine Harmonisierung des Glücksspielrechts im EU-Binnenmarkt noch nicht erfolgt ist und deswegen die Mitgliedstaaten grundsätzlich Art und Umfang der auf ihrem Territorium zulässigen Glücksspiel-, Wett- und Lotterieangebote frei bestimmen können, kann es dem EuGH vielmehr nur darum gehen, unberechtigte Eingriffe in die im europäischen Primärrecht verankerten Grundfreiheiten auszuschließen.

In der Rechtsprechung des EuGH ist seit vielen Jahren anerkannt, dass sowohl das Veranstalten von Glückspielen als auch die Vermittlung von Wettangeboten im Grundsatz von der Dienstleistungsfreiheit im Sinne von Art. 56 AEUV erfasst sind;[20] daneben können sich die ausländischen Anbie-

[13] Vgl. dazu nur *Hecker*, Europäisches Strafrecht, 3. Aufl. 2010, § 9 Rn. 10 ff.; *Satzger*, Internationales und Europäisches Strafrecht, 5. Aufl. 2011, § 9 Rn. 77 ff.
[14] EuGH Slg. 2003, I-13031; ebenso EuGH NJW 2007, 1515.
[15] Hierzu auch jüngst EuGH EuZW 2012, 275.
[16] EuGH GewArch 2010, 423.
[17] EuGH Slg. 2009, I-7633 (m. Anm. *Mintas*, DVBl. 2009, 1373).
[18] EuGH NVwZ 2010, 1409 und 1422.
[19] EuGH EuZW 2010, 821 und EuGH EuZW 2011, 841.
[20] Vgl. EuGH Slg. 1999, I-7289 („Zanetti"); Slg. 2009, I-9735. Dazu EuGH EuZW 2011, 841 (3. Leitsatz): „3. Art. 49 EG ist dahin auszulegen,
a) dass ein Mitgliedstaat, der bestrebt ist, ein besonders hohes Schutzniveau für Verbraucher im Glücksspielsektor zu gewährleisten, Grund zu der Annahme haben kann, dass nur die Errichtung eines Monopols zugunsten einer einzigen Einrichtung, die von den Behörden genau überwacht wird, ihm erlaubt, die Kriminalität in diesem Sektor zu beherrschen und das Ziel, Anreize für übermäßige Spielausgaben zu vermeiden und die Spielsucht zu bekämpfen, hinreichend wirksam zu verfolgen;
b) dass, um mit den Zielen der Kriminalitätsbekämpfung und der Verringerung der Spielgelegenheiten im Einklang zu stehen, eine nationale Regelung, mit der ein Glücksspielmo-

ter im Einzelfall auch auf die in Art. 49 AEUV verbürgte Niederlassungsfreiheit berufen.[21] Mitgliedstaatliche Eingriffe in diese Grundfreiheiten sind freilich nicht per se verboten; sie bedürfen aber ihrerseits einer europarechtlich anerkannten Rechtfertigung. Eine solche Rechtfertigung für staatliche Regulierungen des Glücksspielmarktes kann einerseits aus der Zielsetzung der Bekämpfung von Straftaten wie Betrug und Geldwäsche, aber auch generell der organisierten Kriminalität hergeleitet werden, andererseits aber auch aus dem Gedanken, dass Glücksspiele wegen ihres Suchtpotenzials im Interesse der Spieler kontrolliert und begrenzt werden müssen. Beide Zielsetzungen werden von den EU-Mitgliedstaaten regelmäßig angeführt, wenn es um die Berechtigung von Eingriffen in den Glücksspiel- und Wettmarkt geht.

Völlig unkontrolliert zugelassen sind solche Dienstleistungen in keiner Rechtsordnung innerhalb der Europäischen Union. Allerdings unterscheiden sich die Regulierungskonzepte in den einzelnen Ländern erheblich. Grob gesagt lassen sich zwei Grundmodelle unterscheiden: Während in einigen Mitgliedstaaten – wie in Deutschland – die meisten Glücksspiel-, Wett- und Lotterieangebote einer staatlichen Konzessionierungspflicht unterliegen, die faktisch zu einem Gebietsmonopol staatlicher Toto-/Lotto-Gesellschaften führt, werden insbesondere in Großbritannien Konzessionen grundsätzlich erteilt, soweit die Veranstalter Gewähr dafür bieten, dass sie ihr Glücksspielangebot nicht zu verbotenen Zwecken missbrauchen. Hier werden Konzessionen relativ großzügig an private Veranstalter vergeben, die immer wieder versuchen, ihre Angebote auch auf die faktisch monopolisierten Glücksspiel- und Wettmärkte innerhalb der Europäischen Union auszudehnen. Schon hier ist allerdings darauf hinzuweisen, dass es auch in Deutschland bestimmte Glücksspiel- und Wettangebote gibt, die außerhalb des staatlichen Monopols von Privaten angeboten werden; das gilt einerseits für Automatenglücksspiele, deren Zahl in den letzten Jahren massiv zugenommen hat, und andererseits für Pferdewetten.

Neben den „klassischen" Vertriebswegen wie der Eröffnung von Vermittlungsbüros in den einzelnen Mitgliedstaaten und der Werbung für ihre im Ausland befindlichen Glücksspielangebote hat sich in den letzten 15 Jahren immer wieder die Frage gestellt, ob etwa Anbieter aus dem Vereinigten Königreich via Internet Glücksspielangebote so einrichten dürfen, dass sich z. B. auch Kunden aus Deutschland straflos daran beteiligen können. Die Diskussion um die Zulässigkeit von Glücksspielangeboten innerhalb der Europäischen Union dreht sich daher seit einem Jahrzehnt letztlich um zwei Punkte, wobei sich die Kreise freilich überschneiden. Einerseits geht es um die grundsätzliche Möglichkeit von grenzüberschreitenden Glücksspielangeboten, die durch rechtliche wie faktische Gebietsmonopole unmöglich gemacht werden. Andererseits geht es um die Nutzung moderner Technologie zu Zwecken des Glücksspiels, die eben ohne den Aufbau einer eigenen, durch die Monopolisierung zumeist unzulässigen Vertriebsstruktur auskommen. Staaten, die ihr Glücksspielmonopol abzusichern suchen, verbieten daher teilweise generell Glücksspielangebote via Internet oder aber sie pönalisieren deren Umfeld durch Straftatbestände einerseits gegen Werbemaßnahmen im Inland für solche Internetglücksspiele und andererseits gegen die Beteiligung an jedweder Form nicht staatlich konzessionierter Glücksspielangebote. Letzteres erfasst dann eben nicht nur – wie schon vor hundert Jahren – das Mitspielen im abgedunkelten Hinterzimmer, sondern auch das Zocken und Wetten am heimischen Computer. Deutschland kombiniert inzwischen alle drei Sanktionsmechanismen. Im Glücksspielstaatsvertrag der Bundesländer ist seit wenigen Jahren das Internetglücksspiel generell verboten – das heißt auch für die staatlich konzessionierten Monopolisten. Die Straftatbestände gegen Werbung für vom Inland zugängliche, ausländische Glücksspielangebote namentlich via Internet sind – wie erwähnt – 1998 in das StGB aufgenommen worden (§§ 284 Abs. 4, 287 Abs. 2 StGB). Die eigenständige Strafnorm gegen jede Form der Beteiligung an einem im Inland nicht staatlich genehmigten Glücksspiel (§ 285 StGB) geht auf das Gesetz gegen Glücksspiel v. 23.12.1919 zurück (damals § 284a RStGB)[22] und ist seither dem prinzipiellen Einwand ausgesetzt, dass – obwohl das Glücksspielstrafrecht gerade auch den Spieler vor kriminellen Akten wie auch einem Abgleiten in Spielsucht schützen soll – hier der Teilnehmer am Glücksspiel als solcher bestraft wird.

V. Erste deutsche Anpassungen

Antworten des deutschen Gesetzgebers auf die Neuerungen durch das Internet sind also einerseits das Verbot aller Glücksspielangebote via Internet und andererseits die Pönalisierung der Werbung hierfür. Während aber das Werbeverbot eine eigenständige Entscheidung des deutschen Gesetzgebers angesichts der zunehmenden Bedeutung des Internets darstellte und vor allem der Abschottung des deutschen Glücksspielmarktes diente, war er zu dem Totalverbot für das Internet-Glücksspiel durch die Judikatur des EuGH faktisch gezwungen worden. Bis zum Inkrafttreten des Glücksspielstaatsvertrages zum 1.1.2008 bot nämlich auch der deutsche Toto-/Lotto-Block Glücksspiele via Internet an.

nopol errichtet wird, das dem Inhaber des Monopols ermöglicht, eine Expansionspolitik zu verfolgen,
– auf der Feststellung beruhen muss, dass kriminelle und betrügerische Aktivitäten im Zusammenhang mit den Spielen und die Spielsucht im Hoheitsgebiet des betreffenden Mitgliedstaats ein Problem darstellen, dem eine Ausweitung der zugelassenen und geregelten Tätigkeiten abhelfen könnte, und
– nur den Einsatz maßvoller Werbung zulassen darf, die eng auf das begrenzt bleibt, was erforderlich ist, um die Verbraucher zu den kontrollierten Spielenetzwerken zu lenken;
c) dass der Umstand, dass ein Mitgliedstaat ein anderes Schutzsystem als ein anderer Mitgliedstaat gewählt hat, keinen Einfluss auf die Beurteilung der Erforderlichkeit und der Verhältnismäßigkeit der einschlägigen Bestimmungen haben kann, die allein im Hinblick auf die von den zuständigen Stellen des betroffenen Mitgliedstaats verfolgten Ziele und das von ihnen angestrebte Schutzniveau zu beurteilen sind."

[21] Vgl. nur EuGH EuZW 2012, 275.

[22] RGBl. 1919, S. 2145.

Der EuGH hat nämlich Eingriffe in die Dienstleistungsfreiheit aus Art. 56 AEUV auch in Form staatlicher Glücksspiel- und Wettmonopole nicht per se für unzulässig erklärt, sofern sie dem Schutz vor Kriminalität oder Spielsucht dienen. Dabei hat der EuGH von Anfang an deutlich gemacht, dass die von den Mitgliedstaaten mit ihren Glücksspielmonopolen daneben verfolgten fiskalischen Interessen zur Rechtfertigung der Abschottung der nationalen Märkte nicht herangezogen werden dürfen. Vielmehr müssten die Monopole als massive staatliche Eingriffe in die Grundfreiheiten ausländischer Anbieter im Lichte der europarechtlich zulässigen Eingriffsrechtfertigungen konsistent ausgestaltet sein. In diesem Sinne ist es vor allem problematisch, wenn die staatlichen Glücksspielanbieter ihre Angebote stark bewerben oder sonst auf die Erzielung maximaler Einnahmen setzen, denn vor allem der – jedenfalls vordergründig – angestrebte Schutz vor Spielsucht würde ja in sein Gegenteil verkehrt, würde man möglichst viele Personen zu möglichst hohen Einsätzen verleiten, um dadurch die Einnahmen des Staates zu erhöhen. Ebenso muss ein Verbot der Beteiligung an ausländischen Internetangeboten konsistent sein; gestattet ein Mitgliedstaat seinen Unternehmen, Glücksspiele und Sportwetten im Internet anzubieten, kann er nicht zugleich seinen Bürgern bei Strafe verbieten, sich an Internetglücksspielen ausländischer Anbieter zu beteiligen, die in einem anderen EU-Staat legal angeboten werden. Die Gefahr, dass durch den unkontrollierten Zugang zum eigenen PC Spielsüchtige zu immer neuen Einsätzen verleitet werden, ist keine andere, wenn das Angebot von einem inländischen Glücksspielunternehmen kommt. Deshalb zog Deutschland die „Notbremse“ und verbot – wie andere Mitgliedstaaten – generell Glücksspiele via Internet. Dieses Totalverbot ist immerhin diskriminierungsfrei, weil es sich nicht nur gegen ausländische Anbieter richtet.

Faktisch bewirkt ein nationales Glücksspielverbot via Internet allerdings eine Totalabschottung durch staatliche Konzessionen monopolisierter Glücksspielmärkte, denn wenn kein anderer als der nationale Monopolist eine Konzession erlangt und ohne eine solche sowohl das Veranstalten als auch das Vermitteln von Glücksspielangeboten verboten und strafbar sind, bliebe eben nur ein Angebot von außen mittels Internet. Deswegen haben sich in anderen EU-Staaten zugelassene private Glücksspielanbieter regelmäßig nicht nur gegen ihren Ausschluss bei der Konzessionierung, sondern auch gegen das Verbot von Internetglücksspielangeboten zur Wehr gesetzt.

Im Lichte seiner oben angedeuteten Überlegungen zur Rechtfertigung von Eingriffen in die Dienstleistungsfreiheit ist der EuGH vergleichsweise großzügig gegenüber nationalen Totalverboten des Internetglücksspiels, weil das Internet einerseits Betrügereien zum Nachteil der Verbraucher begünstigt und andererseits eine effektive Kontrolle gegen Spielsucht oder der Teilnahme von Minderjährigen am Glücksspiel – wie in Ansätzen bei einer Spielbank denkbar – faktisch unmöglich ist. Die Leitentscheidung hierfür erging vor zwei Jahren im Fall „Liga Portuguese“.[23]

[23] EuGH Slg. 2009, I-7633.

Im Interesse des Schutzes vor Spielsucht und vor Kriminalität akzeptiert der EuGH auch die Etablierung staatlicher Glücksspielmonopole, behält sich aber eine detaillierte Prüfung der konkreten Umstände vor, wohl weil ihm bewusst ist, dass die EU-Mitgliedstaaten mit ihren Monopolen auch erhebliche fiskalische Interessen verfolgen, die aber nicht so leitend sein dürfen, dass ein Markt innerhalb der Europäischen Union allein aus finanziellen Interessen abgeschottet wird. Ein Monopol wird daher nur akzeptiert, soweit es zur Kanalisierung des Spieltriebs der Bevölkerung sinnvoll ist. Verhindert werden soll damit einerseits, dass potenzielle Spieler auf illegale Glücksspielangebote ausweichen, andererseits aber auch, dass ihre Spielsucht ausgebeutet wird. Daher ist es zulässig, wenn angesichts der Entwicklung neuer Glücksspiel- und Sportwettangebote solche auch durch die deutschen Monopolisten vorgehalten werden. Zulässig ist auch eine gewisse Werbung, damit potenzielle Kunden überhaupt von den legalen Alternativen Kenntnis erlangen. Nicht zulässig ist es aber, wenn die Vielfalt der Angebote und insbesondere deren Bewerbung vor allem zu einer Ausweitung der Einnahmen der Monopolisten und damit des Staates führen, denn alle Mehreinnahmen führen letztlich zu einer Ausweitung, nicht zu der vorgeblich gewollten Eindämmung der Spielleidenschaft und begünstigen damit ein Abgleiten in Spielsucht bis hin zum wirtschaftlichen Ruin.

Deswegen wurde in Deutschland neben dem Verbot von Internetwetten auch die Werbung für die normalen Wettangebote deutlich eingeschränkt, die Zahl der Lotto-Annahmestellen sollte etwas reduziert und der mögliche Gewinn nicht allzu sehr betont werden. Auch wenn im Vorfeld der Fußball-WM 2006 daraufhin die von staatlichen Wettunternehmen geplanten Werbemaßnahmen reduziert wurden, hat sich allerdings in der Praxis wenig verändert. So gibt es in Berlin immer noch an den meisten Straßenecken Lotto-Annahmestellen. Dies ist allerdings von Europarechtswegen nicht zu beanstanden, solange eine Kanalisierung des Spieltriebs in legalen Bahnen stattfindet; nach dem Verbot von Internetglücksspielen kann man schlecht auch die Zahl der Wettbüros massiv zurückfahren. Problematischer ist dagegen, dass die Zahl der konzessionierten Spielbanken in den Jahren 2000 bis 2006 von 66 auf 81, d.h. um ein Viertel gestiegen ist.

VI. Die Absage des EuGH an das deutsche Glücksspielmonopol

Der Druck des EuGH auf das Glücksspiel- und Sportwettmonopol in Deutschland setzt denn auch an einer anderen Stelle an. Wie gesagt, gibt es in Deutschland längst einen liberalisierten Glücksspielmarkt, nämlich in Form der Automatenspiele, die in zahlreichen privat betriebenen Einrichtungen angeboten werden. Das Suchtpotenzial von Kasino- und Automatenspielen soll aber weit höher sein als dasjenige anderer Glücksspiele. Daraus folgert der EuGH nicht ohne Grund, dass das deutsche Glücksspielmonopol in seiner konkreten Ausgestaltung und mit seinen genannten Ausnahmen nicht geeignet ist, „die Erreichung des mit seiner Errichtung verfolgten Ziels (der Kanalisierung und Eindämmung der Spielsucht) dadurch zu gewährleisten, dass es dazu beiträgt, die Gelegenheit zum Spiel zu verringern und die Tätigkeiten

in diesem Bereich in kohärenter und systematischer Weise zu begrenzen“.[24]

Dagegen ist der legale Markt für Sportwetten in Deutschland – mit Ausnahme der Pferdewetten – komplett monopolisiert, doch hat sich daneben längst ein riesiger Markt privater, regelmäßig verbotener und strafbarer Sportwettangebote etabliert. An diesem Graumarkt werden nach Schätzungen ca. 97 % aller Sportwetten in Deutschland platziert. Bedenkt man, dass der Staat bei einer Konzessionierung privater Anbieter eine Abgabe erhalten könnte, entgehen Deutschland damit wohl erhebliche Summen. Deswegen, aber auch wegen der Rechtsprechung des EuGH, kam es zu einem Umdenken; im neuen Glücksspieländerungsstaatsvertrag (GlüÄndStV) von 15 Bundesländern sind mit Wirkung bereits zum 1.7.2012 sowohl private Sportwettangebote (begrenzt allerdings auf insgesamt 20 Konzessionen, was europarechtlich nicht unumstritten ist) als auch bestimmte Internetangebote zugelassen werden (verboten sind aber weiterhin Internetcasinospiele wie z. B. Online-Poker). Schleswig-Holstein ging sogar einen Schritt weiter, denn dort wurde Ende 2011 in einem eigenen Glücksspielgesetz der Sportwettmarkt noch weiter geöffnet und unter anderem auch Online-Poker erlaubt. Seit dem Regierungswechsel im Mai 2012 versucht die neue Landesregierung allerdings, dieses Gesetz wieder aufzuheben und dem Glücksspieländerungsstaatsvertrag beizutreten. Derzeit werden aber noch Lizenzen an private Anbieter auf Grundlage des Landesgesetzes vergeben; deren Rücknahme soll nach dem Willen der neuen Landesregierung geprüft werden. Welche strafrechtlichen Konsequenzen aus diesem zumindest zeitweiligen Nebeneinander verschiedener landesrechtlicher Glücksspielregelungen zu ziehen sein werden, bleibt derzeit noch abzuwarten.[25]

VII. Hausverlosungen

Nur kurz möchte ich auf das neue Phänomen der Hausverlosungen im Internet eingehen.[26] Vor allem in Zeiten der Finanzkrise, als sich niemand mehr bereitgefunden hat, für Luxusimmobilien die geforderten Preise zu bezahlen, kamen Verkaufswillige auf den Gedanken, bei einem Preisziel von 1 Mio. Euro z.B. 10.000 Lose zu je 99 Euro via Internet zu verkaufen; danach wurde der glückliche Erwerber aus der Lostrommel gefischt. Neben rechtstechnischen Fragen wie der notariellen Beurkundung, die aber sicherlich lösbar gewesen wären, stand dieses Vertriebsmodell in Deutschland vor strafrechtlichen Grenzen, denn dabei handelt es sich um eine staatlich nicht konzessionierte und damit nach § 287 StGB[27] bei Strafe verbotene Ausspielung.[28] Im Inland ist eine solche Verlosung per Internet schon deshalb nicht konzessionierbar gewesen, weil der Glücksspielstaatsvertrag seit 2008 Glücksspiele im Internet per se verbietet (dies ändert sich partiell mit dem Glücksspieländerungsstaatsvertrag, doch müssten weiterhin bestimmte Voraussetzungen erfüllt sein); dabei wird der Begriff „im Internet“ weit ausgelegt, so dass eine Hausverlosung diesen Charakter – und damit ihr generelles Verbotensein – nicht etwa dadurch verlieren kann, dass nach einem Angebot via Internet alle weiteren Schritte per Post oder E-mail-Verkehr erfolgen sollen.[29]

Diese Strafbarkeit besteht auch dann, wenn die Immobilie z.B. in Spanien via Internet angeboten wird, aber diese Internetlotterie in Deutschland beworben oder vermittelt wird. Faktisch müssen mithin wegen § 287 StGB solche Angebote vom deutschen Markt fernbleiben. Das beschränkt die Verkäufer, denen in Europa der größte Markt verschlossen ist, wie die deutschen Erwerbsinteressenten, die die Finca auf Mallorca nicht allein mit einem „Hunderter“ und ziemlich viel Glück ihr Eigen nennen können. Lediglich die Strafbarkeit für Mitspieler (§ 285 StGB) findet auf Lotterien und Ausspielungen und damit auf Hausverlosungen keine Anwendung, so dass der „Häuslekäufer“ straffrei bleibt. Allerdings dürfte er trotzdem von einer Spielteilnahme ausgeschlossen sein, weil der ausländische Anbieter unter dem Damok-

[24] EuGH NVwZ 2010, 1422; in EuGH NVwZ 2010, 1409 heißt es im 2. Leitsatz u.a.: „d) Stellt ein nationales Gericht sowohl fest,
– dass die Werbemaßnahmen des Inhabers eines solchen Monopols für andere, ebenfalls von ihm angebotene Arten von Glücksspielen nicht auf das begrenzt bleiben, was erforderlich ist, um die Verbraucher zum Angebot des Monopolinhabers hinzulenken und sie damit von anderen, nicht genehmigten Zugangskanälen zu Spielen wegzuführen, sondern darauf abzielen, den Spieltrieb der Verbraucher zu fördern und sie zwecks Maximierung der aus den entsprechenden Tätigkeiten erwarteten Einnahmen zu aktiver Teilnahme am Spiel zu stimulieren, als auch,
– dass andere Arten von Glücksspielen von privaten Veranstaltern, die über eine Erlaubnis verfügen, betrieben werden dürfen, als auch,
– dass in Bezug auf andere Arten von Glücksspielen, die nicht unter das Monopol fallen und zudem ein höheres Suchtpotenzial als die dem Monopol unterliegenden Spiele aufweisen, die zuständigen Behörden eine zur Entwicklung und Stimulation der Spieltätigkeiten geeignete Politik der Angebotserweiterung betreiben oder dulden, um insbesondere die aus diesen Tätigkeiten fließenden Einnahmen zu maximieren,
so kann es berechtigten Anlass zu der Schlussfolgerung haben, dass ein solches Monopol nicht geeignet ist, die Erreichung des mit seiner Errichtung verfolgten Ziels, Anreize zu übermäßigen Ausgaben für das Spielen zu vermeiden und die Spielsucht zu bekämpfen, dadurch zu gewährleisten, dass es dazu beiträgt, die Gelegenheiten zum Spiel zu verringern und die Tätigkeiten in diesem Bereich in kohärenter und systematischer Weise zu begrenzen.“

[25] Vgl. Lübecker Nachrichten vom 24.8.2012 (http://www.ln-online.de/nachrichten/3534489).

[26] Dazu *Mailänder*, ZfWG 2009, 395; *Sterzinger*, NJW 2009, 3690.

[27] Dazu *Mintas*, ZfWG 2009, 82.

[28] OVG Berlin-Brandenburg ZfWG 2012, 137; VG Regensburg, Urt. v. 5.7.2012 – RO 5 K 12.568 (juris); VG München ZfWG 2009, 70; VG Münster ZfWG 2010, 364.

[29] OVG Berlin-Brandenburg ZfWG 2012, 137; VG Regensburg, Urt. v. 5.7.2012 – RO 5 K 12.568 (juris), hält dies für unionsrechtskonform.

lesschwert des § 287 StGB schwerlich ein solches Angebot für Kunden aus Deutschland öffnen wird.

VIII. Auswirkungen des Europarechts auf die Strafrechtsprechung

Zu guter Letzt möchte ich noch einen Blick auf die strafrechtlichen Reaktionen in Deutschland werfen, die nämlich – auch wegen der europarechtlichen Fragwürdigkeit der Abschottung des deutschen Glücksspielmarktes – höchst unterschiedlich ausfallen. Während einige Strafgerichte zumindest wegen der Zweifelhaftigkeit der Vereinbarkeit der deutschen Strafrechtsregelung mit Europarecht den Angeklagten einen (häufig unvermeidbaren) Verbotsirrtum i.S.v. § 17 S. 1 StGB zubilligen wollen[30] und deshalb freisprechen, bejahen andere die Tatbestandsmäßigkeit des Verhaltens schlicht deswegen, weil es eben an einer staatlichen Konzession fehlt, ohne Rücksicht darauf, dass im Lichte des Europarechts die Nichterteilung der Konzession möglicherweise rechtswidrig ist.[31] M.E. mag man zwar die Tatbestandsmäßigkeit des Verhaltens der privaten Wettanbieter in Deutschland bejahen, muss dann aber im Lichte der durch das in seiner konkreten Ausgestaltung europarechtswidrige Monopol verletzten Dienstleistungsfreiheit eine Rechtfertigung kraft Europarechts annehmen.[32]

[30] Vgl. KG, Urt. v. 2.2.2012 – (4) 1 Ss 552/11 (327/11) – juris; Leitsatz: „Die unklare Rechtslage, wie sie im Bereich der Sportwettenvermittlung durch Gesetzgebung, Verwaltung und Rechtsprechung geschaffen worden ist, darf nicht einseitig dem Normadressaten aufgebürdet werden. Bei der Frage der Vermeidbarkeit eines Verbotsirrtums ist dies zu beachten." Ähnlich schon OLG Hamm JR 2004, 478, und OLG München NJW 2008, 3151.

[31] In diesem Sinne noch ganz strikt KG NVwZ-RR 2011, 647; Leitsatz: „Die Regelungen des Glücksspielstaatsvertrages und des für das Land Berlin dazu ergangenen Ausführungsgesetzes sind verfassungs- und gemeinschaftsrechtskonform und begründen in zulässiger Weise eine Erlaubnispflicht für die Veranstaltung und Vermittlung von Sportwetten. Die Erlaubnispflichtigkeit verstößt auch dann nicht gegen die Grundsätze der Niederlassungs- und Dienstleistungsfreiheit, wenn die Sportwetten für einen in einem anderen EU-Mitgliedstaat ansässigen Veranstalter von Sportwetten vermittelt werden, der dort über eine Erlaubnis verfügt."

[32] Für eine Rechtfertigungslösung auch *Walter*, in: Laufhütte/Rissing-van Saan/Tiedemann (Hrsg.), Strafgesetzbuch, Leipziger Kommentar, Bd. 1 (§§ 1-31), 12. Aufl. 2007, Vor § 13 Rn. 201; ausführlich *Kreis*, Die verbrechenssystematische Einordnung der EG-Grundfreiheiten, 2008, passim. – Die h.M. im deutschen Schrifttum präferiert demgegenüber eine Neutralisierung nationaler Strafnormen bereits auf der Ebene des Tatbestandes (vgl. nur *Hecker*, Europäisches Strafrecht, 3. Aufl., 2010, § 9 Rn. 10 ff.).

Arbeitnehmerüberwachung und Compliance unter Berücksichtigung der Cybercrime-Konvention*

Von Prof. Dr. **Jörg Eisele**, Konstanz

I. Einführung

Die Arbeitnehmerüberwachung und ihre strafrechtlichen Grenzen sind erst in jüngerer Zeit in das Blickfeld der Strafrechtswissenschaft getreten. Anlass hierfür waren einige spektakuläre Fälle unzulässiger Überwachung von Beschäftigten durch große deutsche Unternehmen, die eine breite gesellschaftliche und rechtspolitische Diskussion ausgelöst haben. So wurde etwa bei der Deutschen Bahn AG in den Jahren 2006 und 2007 der gesamte E-Mail-Verkehr massiv überwacht und nach bestimmten Schlagworten gefiltert (Logfile-Filterung); der Inhalt der E-Mails soll jedoch nicht überprüft worden sein. In einem weiteren Fall wurde eine Massen-Mail der Gewerkschaft Deutscher Lokomotivführer (GDL), die einen Streikaufruf enthielt, den Beschäftigten nicht zugestellt. Die Deutsche Bahn führte zu ihrer Verteidigung an, dass diese E-Mail mit einer weiteren internen Massen-Mail zur Überlastung und zum Zusammenbruch des Mailservers geführt habe. Im Zuge des Wiederhochfahrens des Servers sei dann entschieden worden, die E-Mail zu löschen, weil das Verschicken über das E-Mail-System der Bahn rechtswidrig gewesen sei. Schließlich wurden auch im Zuge eines sog. Screenings ohne konkreten Verdacht verschiedene Daten – wie Anschriften, Telefonnummern und Bankverbindungen – einer großen Zahl von Mitarbeitern mit Daten Angehöriger von Lieferanten abgeglichen, um so Korruptionsfällen auf die Spur zu kommen. Die Deutsche Bahn hat für die in diesem Zusammenhang begangenen Ordnungswidrigkeiten einen Bußgeldbescheid des Berliner Beauftragten für Datenschutz und Informationsfreiheit v. 16.10.2009 mit einem Bußgeld in Höhe von mehr als 1,1 Millionen Euro akzeptiert.[1] Im Folgenden möchte ich exemplarisch untersuchen, ob in Fällen der Arbeitnehmerüberwachung neben Ordnungswidrigkeiten wegen Verstößen gegen das Bundesdatenschutzgesetz auch „klassische Straftatbestände" zur Anwendung gelangen können.

II. Ausgangspunkt: Datenschutz und Compliance

Die Arbeitnehmerüberwachung betrifft den in jüngerer Zeit vieldiskutieren Bereich der sog. Compliance.[2] Von diesem Blickwinkel aus greifen Überwachungsmaßnahmen nicht nur in die Rechte des Arbeitnehmers ein, sondern können zugleich schutzwürdigen Interessen des Arbeitgebers dienen. So werden in der Praxis Überwachungsmaßnahmen zur Verhinderung oder Aufdeckung von Straftaten der Arbeitnehmer – wie z.B. Diebstahl, Bestechung, Untreue oder Verrat von Betriebsgeheimnissen u.s.w. – durchgeführt. Soweit die mit datenschutzrechtlichen Fragen im Unternehmen befassten Personen – insbesondere ein Datenschutzbeauftragter oder Compliance Officer, aber auch Rechtsabteilungen, Innenrevisionen, Vorstände, Geschäftsführer und Aufsichtsräte[3] – untätig bleiben, steht aufgrund neuerer Rechtsprechung des Bundesgerichtshofs zumindest eine Strafbarkeit wegen Beihilfe durch Unterlassen zu der von dem Beschäftigten begangenen Tat im Raum.[4] Diesbezüglich muss man also sehen, dass die Arbeitnehmerüberwachung dazu dienen kann, Compliance-Anforderungen im Unternehmen umzusetzen. Andererseits ist zu beachten, dass Compliance-Maßnahmen ihrerseits überhaupt nur zulässig sind, soweit sie nicht gegen Regelungen verstoßen, die den Arbeitnehmer schützen.[5]

III. Überwachung des E-Mail-Verkehrs

Im Folgenden möchte ich im Wesentlichen auf Fragen der Überwachung des E-Mail-Verkehrs eingehen. Die Überwachung des E-Mail-Verkehrs, die technisch problemlos möglich ist, erlangt schon deshalb zentrale Bedeutung, weil heute große Teile der Kommunikation eines Unternehmens per E-Mail erfolgen. Ausgeklammert bleiben daher im Wesentlichen – im Einklang mit dem Thema unseres Rechtsdialogs – insbesondere die Überwachung des Briefverkehrs, das Abhören des gesprochenen Wortes sowie unbefugte Bildaufnahmen mithilfe von installierten Kameras.

1. Verletzung des Fernmeldegeheimnisses nach § 206 StGB

Im Fokus meiner Ausführungen steht zunächst § 206 StGB, der dem Schutz des Post- und Fernmeldegeheimnisses dient. In den Schutzbereich einbezogen sind nach § 206 Abs. 5 S. 2 StGB der Inhalt der Telekommunikation sowie ihre näheren Umstände, insbesondere die Tatsache, ob jemand an einem Telekommunikationsvorgang beteiligt ist oder war. Erfasst ist damit der Inhalt jeder Art individueller Nachrichtenübermittlung, also auch per E-Mail oder Internettelefonie; dies gilt insbesondere auch für Verbindungsdaten – wie Rufnummern,

---

* Der folgende Vortrag beruht auf dem Manuskript meiner inzwischen erschienenen Monografie Compliance und Datenschutzstrafrecht, Strafrechtliche Grenzen der Arbeitnehmerüberwachung, 2012.

[1] Vgl. dazu näher Pressemitteilung v. 23.9.2009 des Berliner Beauftragten für Datenschutz und Informationsfreiheit unter http://www.datenschutz-berlin.de/attachments/627/PE_DB_AG.pdf?1256283223 sowie https://www.datenschutzzentrum.de/presse/20080911-bw-lidl-bussgeldverfahren.pdf (Stand: 20.8.2011).

[2] BT-Drs. 17/4230, S. 1 und S. 12; *Forst*, DuD 2010, 160 (161); *Salvenmoser/Hauschka*, NJW 2010, 331.

[3] *Wybitul*, BB 2009, 2590 (2591).

[4] BGHSt 54, 44 (Leiter der Innenrevision einer Anstalt des öffentlichen Rechts). Dazu *Rotsch*, ZJS 2009, 712, und jüngst *ders.*, in: Schulz/Reinhart/Sahan (Hrsg.)., Festschrift für Imme Roxin, 2012, S. 485 m.w.N.

[5] *Forst*, DuD 2010, 160 (161); *Kamp/Körffer*, RDV 2010, 72 (75); *Rübenstahl*, NZG 2009, 1341 (1342); unklar *Behling*, BB 2010, 892 (893 f.). Zu diesem Spannungsverhältnis auch ArbG Berlin ZIP 2010, 1191, wonach eine verhaltensbedingte Kündigung wegen eines leitenden Mitarbeiters im Bereich „Compliance" wegen Überwachungsmaßnahmen zur Korruptionsbekämpfung nur in engen Grenzen zulässig ist.

IP-Adresse, Zeit, Ort oder Gesprächsdauer eines Telekommunikationsvorgangs.

a) Was die Tathandlungen anbelangt, so ist für den hier vorliegenden Zusammenhang die Weitergabe von Informationen nach Abs. 1 und das Unterdrücken von E-Mails nach Abs. 2 Nr. 1 von Belang. Solange der E-Mail-Verkehr nur überwacht, protokolliert, nach bestimmten Begriffen gefiltert oder auch eingesehen wird, ohne dass Informationen an Dritte weitergeleitet werden, ist der Tatbestand von vornherein zu verneinen.[6] Hier kommen regelmäßig nur Ordnungswidrigkeiten nach § 43 BDSG, im Falle des Handelns gegen Entgelt oder in der Absicht, sich oder einen anderen zu bereichern oder einen anderen zu schädigen, auch eine Straftat nach § 44 BDSG in Betracht. Die Frage der Anwendbarkeit des Tatbestands erlangt neben Fällen des Nichtzustellens von E-Mails vor allem hinsichtlich der Weitergabe von Informationen an Externe – wie etwa Detektive oder Sicherheitsunternehmen –, die in die Überwachung eingeschaltet sind, sowie an Strafverfolgungsbehörden oder Gerichte in Kündigungsschutzprozessen Bedeutung.[7]

b) Als Täter des Delikts kommen aber nur Inhaber oder Beschäftigte eines Unternehmens in Betracht, das geschäftsmäßig Telekommunikationsdienste erbringt. Damit scheint der Anwendungsbereich auf den ersten Blick auf typische Telekommunikationsunternehmen und Internetprovider begrenzt zu sein. Die h.M. versteht diese Voraussetzung jedoch weiter und orientiert sich bei ihrer Auslegung an den einschlägigen Regelungen des Telekommunikationsgesetzes.[8] Unter dem geschäftsmäßigen Erbringen von Telekommunikationsdiensten wird nach § 3 Nr. 10 TKG das nachhaltige Angebot von Telekommunikation für Dritte mit oder ohne Gewinnerzielungsabsicht verstanden. Damit wird das *Angebot für Dritte* zum entscheidenden Kriterium erhoben. In Folge dessen soll dann jeder Unternehmer, der Telekommunikationseinrichtungen für seine Mitarbeiter zur privaten Nutzung zur Verfügung stellt, vom Tatbestand erfasst sein.[9] Zur Begründung wird u.a. angeführt, dass es auf eine Gewinnerzielungsabsicht nicht ankomme und so das unentgeltliche Bereitstellen erfasst werde.[10] Zudem wird auf die Gesetzesbegründung zu § 88 Abs. 2 TKG verwiesen, wonach auch Nebenstellenanlagen in Betrieben und Behörden einbezogen sein sollten.[11] Letztlich kann man auch noch anführen, dass es für die Schutzwürdigkeit des Arbeitnehmers unerheblich ist, ob er seine privaten E-Mails über das Webmail-Programm des Arbeitgebers oder einen allgemeinen Internetprovider versendet. Diese Ansicht hat zur Folge, dass das TKG nur dann nicht anwendbar ist, wenn eine rein betriebliche Nutzung der Telekommunikation erfolgt, d.h. die Privatnutzung verboten ist, weil dann kein Angebot an Dritte vorliegt; dabei bleibt es auch, wenn der Arbeitnehmer ein solches Verbot des Arbeitgebers missachtet.[12] Dabei ist zu beachten, dass der Arbeitnehmer grundsätzlich kein Recht auf die Inanspruchnahme der Kommunikationsmittel zur privaten Nutzung hat, so dass der Arbeitgeber prinzipiell frei entscheiden kann.

c) Die Gegenansicht wendet ein, dass Zweck des Telekommunikationsgesetzes nach dessen § 1 sei, den Wettbewerb und leistungsfähige Telekommunikationsinfrastrukturen zu fördern und flächendeckend angemessene und ausreichende Dienstleistungen zu gewährleisten, was jedoch auf den Arbeitgeber, der nur die Privatnutzung gestatte, nicht zutreffe.[13] Freilich überzeugt dieses Argument jedenfalls im Rahmen des § 206 StGB nicht, weil dieser Vorschrift ein anderer Schutzzweck zu Grunde liegt und Wettbewerbsaspekte von vornherein keine Rolle spielen.

Entscheidender ist aber, dass die Kontrollmöglichkeiten des Arbeitgebers stark eingeschränkt werden, wenn er als Telekommunikationsanbieter qualifiziert wird. Dann gelten für ihn nämlich auch bei der Kontrolle dienstlicher Tätigkeiten die strengen Vorgaben des TKG, wobei jedoch aufgrund seines Direktionsrechts im Ergebnis weitergehende Kontrollmaßnahmen als bei einer Privatnutzung möglich sind.[14] Würde der Arbeitgeber hingegen von vornherein die Privatnutzung von E-Mails verbieten, unterläge er insgesamt nur den weniger strengen Vorschriften des Bundesdatenschutzgesetzes. Auf weitere komplizierte Abgrenzungsfragen im Hinblick auf Telemedien soll hier nicht eingegangen werden. Entscheidende Strafbarkeitslücken wären mit einer Verneinung der Eigenschaft als Telekommunikationsanbieter und damit zugleich des Tatbestandes des § 206 StGB jedoch nicht verbunden. Da die Tathandlung des Unterdrückens auch von § 303a StGB erfasst wird, ginge es im Wesentlichen nur noch um die Mitteilung von Tatsachen durch den Arbeitgeber gegenüber Dritten. Dabei würde es sich freilich nicht um eine gravierende Strafbarkeitslücke handeln, da z.B. auch bei Schriftstü-

[6] Siehe *Altenburg/Reinersdorff/Leister*, MMR 2005, 135 (138); *Barton*, CR 2003, 839 (843); *Hoppe*, Private Nutzung betrieblicher Informations- und Kommunikationsmittel am Arbeitsplatz, 2010, S. 182; *Schuster*, ZIS 2010, 68 (72).

[7] Vgl. nur *Gola*, Datenschutz und Multimedia am Arbeitsplatz, 3. Auflage, 2010, Rn. 104; *Thüsing*, Arbeitnehmerdatenschutz und Compliance, Effektive Compliance im Spannungsfeld von reformiertem BDSG, Persönlichkeitsschutz und betrieblicher Mitbestimmung, 2010, Rn. 314.

[8] Vgl. § 88 Abs. 2 i.V.m. § 3 Nr. 6 TKG; dazu *Altvater*, in: Laufhütte/Rissing-van Saan/Tiedemann (Hrsg.), Strafgesetzbuch, Leipziger Kommentar, Bd. 5, 12. Aufl. 2005, § 206 Rn. 11; *Altenhain*, in: Joecks/Miebach (Hrsg.), Münchener Kommentar zum Strafgesetzbuch, Bd. 3, 2003, § 206 Rn. 15 ff.

[9] *Heidrich/Tschoepe*, MMR 2004, 75 (76); *Altvater* (Fn. 8), § 206 Rn. 12; *Altenhain* (Fn. 8), § 206 Rn. 18; *Kargl*, in: Kindhäuser/Neumann/Paeffgen (Hrsg.), Nomos Kommentar, Strafgesetzbuch, Bd. 2, 3. Aufl. 2010, § 206 Rn. 10; offen gelassen von VG Frankfurt a.M. CR 2009, 125 (126), und VGH Hessen NJW 2009, 2470 (2471 f.).

[10] *Elschner*, Handbuch Multimedia-Recht, Teil 22.1 Rn. 80; *Kalf/Papsthart*, in: Erbs/Kohlhaas, Strafrechtliche Nebengesetze, 188. Lfg., Stand: Januar 2012, § 85 Rn. 8.

[11] BT-Drs. 13/3609, S. 53.

[12] *Härting*, CR 2007, 311 (316); *Heidrich/Tschoepe*, MMR 2004, 75 (76); *Sassenberg/Lammer*, DuD 2008, 461 (463 f.); *Sauer*, K&R 2008, 399 (400); *Schuster*, ZIS 2010, 68 (71).

[13] So *Haussmann/Krets*, NZA 2005, 259 (260); *Thüsing* (Fn. 7), Rn. 240 f.

[14] *Thüsing* (Fn. 7), Rn. 237.

cken die Weitergabe des Inhalts nicht von der Strafvorschrift des § 202 StGB sanktioniert wird. Im Übrigen muss man sehen, dass auch die Weitergabe anderer (privater) Informationen durch den Arbeitgeber grundsätzlich nur als Ordnungswidrigkeit nach Datenschutzrecht sanktioniert werden kann.[15]

d) Angesichts der hier vertretenen Ansicht möchte ich nur noch zwei wichtige Aspekte aus der großen Anzahl der im Rahmen des Tatbestandes diskutierten Problemfelder hervorheben, die es aus dem Blickwinkel der h.M. zu beachten gilt.

aa) Zunächst muss man sehen, dass der Tatbestand beim Unterdrücken nach Abs. 2 Nr. 2 nur dem Unternehmen anvertraute Sendungen erfasst; der Schutz beginnt damit erst, wenn der versendende Rechner die Daten dem empfangenden Server des Unternehmens übermittelt hat.[16] Noch nicht anvertraut ist eine E-Mail daher, wenn das Unternehmen diese – z.B. bei Spam-Mails – von vornherein mittels sog. „Blacklists" aufgrund der IP- oder E-Mail-Adresse des Absenders ablehnt.[17] Andererseits fallen aber auch E-Mails, die vom Arbeitnehmer bereits vom Server des Unternehmens abgerufen und wie andere Dateien auf dem Rechner archiviert worden sind, nicht mehr in den tatbestandlichen Schutzbereich,[18] weil vom Fernmeldegeheimnis nur die Phase des Übertragungsvorgangs erfasst ist.[19] Hingegen werden nach h.M. E-Mails, die auf dem Server verbleiben und per Internetverbindung durch lokale Rechner, Notebooks, Mobiltelefone usw. abgerufen werden können, vom Schutzbereich umfasst.[20] Das Unternehmen erbringt demnach auch in dieser Phase weiterhin Telekommunikationsleistungen und wird nicht nur als Arbeitgeber tätig, der den Mitarbeitern IT-Einrichtungen zur Speicherung zur Verfügung stellt.[21] Auch die bloße Möglichkeit des Arbeitnehmers, darüber zu entscheiden, ob die E-Mail nach Kenntnisnahme im System verbleibt oder gelöscht wird, vermag daran nichts zu ändern, wenn diese weiterhin abrufbar bleibt.

bb) Hinsichtlich einer möglichen Rechtfertigung des Arbeitgebers ist die Regelung des § 88 Abs. 3 TKG zu beachten. Demnach ist es den Verpflichteten untersagt, sich oder anderen über das für die geschäftsmäßige Erbringung der Telekommunikationsdienste einschließlich des Schutzes ihrer technischen Systeme erforderliche Maß hinaus Kenntnis vom Inhalt oder den näheren Umständen der Telekommunikation zu verschaffen. Eine Verwendung dieser Kenntnisse für andere Zwecke, insbesondere die Weitergabe an Dritte wie Strafverfolgungsbehörden, ist nur zulässig, soweit das TKG oder eine andere gesetzliche Vorschrift dies vorsieht und sich dabei *ausdrücklich* auf Telekommunikationsvorgänge bezieht. Daraus wird überwiegend gefolgert, dass auch für die strafrechtliche Rechtfertigung nur solche Vorschriften in Betracht kommen, die sich nach ihrem Wortlaut ausdrücklich auf Telekommunikationsvorgänge beziehen,[22] was vor allem bei Notwehr (§ 32 StGB) und Notstand (§ 34 StGB) nicht der Fall ist. Andere möchten die Notstandsvorschrift des § 34 StGB zumindest im Falle des Unterdrückens anwenden, weil § 88 Abs. 3 S. 3 TKG nur an die Verwendung der Kenntnisse anknüpft, das Unterdrücken aber unerwähnt lässt; dem durch Art. 10 GG geschützten Fernmeldegeheimnis soll dann im Rahmen der bei § 34 StGB vorzunehmenden Abwägung freilich entsprechendes Gewicht einzuräumen sein.[23] Für die restriktive Ansicht der h.M. spricht jedoch, dass sich der Gesetzgeber die Entscheidung darüber vorbehalten wollte, wann ein Eingriff in das besonders schützenswerte Fernmeldegeheimnis als erlaubt anzusehen ist,[24] so dass sich dies grundsätzlich nach den speziellen Datenschutzvorschriften der §§ 91 ff. TKG richten soll. Unberührt von dieser Sperre bleibt lediglich die Einwilligung, weil hier der Betroffene selbst über das Rechtsgut disponieren kann.[25] Werden virenverseuchte E-Mails in einem Unternehmen durch Filter zurückgehalten und dem Adressaten deshalb nicht zugestellt, bieten übrigens § 88 Abs. 3 S. 2 TKG und § 109 TKG hierfür eine spezielle Befugnis.[26] Anders ist hingegen bei Spam-Mails zu entscheiden, weil diese nicht per se zur Schädigung oder Störung geeignet sind und automatisiert in einen gesonderten Spam-Ordner, der dem Arbeitnehmer zugänglich ist, verschoben werden können, so dass ein Unterdrücken nicht erforderlich

[15] Speziell zu § 44 BDSG *Wybitul/Reuling*, CR 2010, 829 (830 ff.).

[16] OLG Karlsruhe MMR 2005, 178 (180); *Heidrich/Tschoepe*, MMR 2004, 75 (78).

[17] Zur technischen Seite *Heidrich*, CR 2009, 168.

[18] Siehe VG Frankfurt a.M. CR 2009, 125 f.; *Behling*, BB 2010, 892 (893).

[19] BVerfGE 115, 166 (183 f.), 120, 274 (307 f.); 124, 43 (54); *Hauschild*, NStZ 2005, 337 (340); *Welp*, NStZ 1994, 294 (295). Zu den einzelnen Phasen der E-Mail-Kommunikation *Brodowski*, JR 2009, 402.

[20] Nach *Hoppe/Braun*, MMR 2010, 80 (82) gilt dies auch für Sicherungskopien des E-Mail-Verkehrs.

[21] So aber VGH Hessen NJW 2009, 2470 (2471); vgl. auch die Vorinstanz VG Frankfurt a.M. CR 2009, 125.

[22] *Bock*, in: Beck'scher Onlinekommentar, Telekommunikationsgesetz, Stand: 3. Aufl. 2006, § 88 Rn. 28; *Lackner/Kühl*, Strafgesetzbuch, Kommentar, 27. Aufl. 2011, § 206 Rn. 15; *Altenhain* (Fn. 8), § 206 Rn. 68; *Kargl* (Fn. 9), § 206 Rn. 47; *Lenckner/Eisele*, in: Schönke/Schröder, Strafgesetzbuch, Kommentar, 28. Aufl. 2010, § 206 Rn. 14; *Schuster*, ZIS 2010, 68 (75); *Hoyer*, in: Rudolphi u.a. (Hrsg.), Systematischer Kommentar zum Strafgesetzbuch, 56. Lfg., Stand: Mai 2003, § 206 Rn. 35; *Bosch*, in: Satzger/Schmitt/Widmaier (Hrsg.), Strafgesetzbuch, Kommentar, 2009, § 206 Rn.14; *Thüsing* (Fn. 7), Rn. 316; and. *Altvater* (Fn. 8), § 206 Rn. 80; krit. auch *Barton*, CR 2003, 839 (844).

[23] *Altvater* (Fn. 8), § 206 Rn. 80.

[24] BR-Drs. 147/97, S. 46; ferner BT-Drs. 13/ 3609, S. 53.

[25] *Bock* (Fn. 22), § 88 Rn. 56; *Eckhardt*, in: Spindler/Schuster, Recht der elektronischen Medien, 2008, § 88 Rn. 15; *Hanau/Hoeren*, Fundstelle, S. 56; *Lenckner/Eisele* (Fn. 22), § 206 Rn. 14; *Hoyer* (Fn. 22), § 206 Rn. 39; and. aber *Altenhain* (Fn. 8), § 206 Rn. 68.

[26] Vgl. auch *Gola* (Fn. 7), Rn. 110; *Heidrich/Tschoepe*, MMR 2004, 75 (78); *Altvater* (Fn. 8), § 206 Rn. 73; *Schmidl*, MMR 2005, 343 (344). Zum Erkennen, Eingrenzen und Beseitigen aktueller Störungen können auch nach § 100 Abs. 1 TKG Bestands- und Verkehrsdaten erhoben und verwendet werden.

ist.[27] Hier muss man sich ggf. mit Einwilligungslösungen behelfen.

2. Ausspähen von Daten nach § 202a StGB

a) Bedeutung erlangt in diesem Zusammenhang auch die Vorschrift des § 202a StGB. Diese wurde durch das StrafrechtsänderungsG zur Bekämpfung der Computerkriminalität modifiziert und dadurch den Vorgaben der jeweiligen Art. 2 des Rahmenbeschlusses der EU über Angriffe auf Informationssysteme und des Übereinkommens des Europarates über Computerkriminalität (Cybercrime-Konvention, Nr. 185) angepasst.[28] § 202a StGB betrifft dabei nicht nur den Telekommunikationsverkehr, sondern prinzipiell alle Daten, die auf dem Rechner des Arbeitnehmers gespeichert werden. Der Tatbestand setzt nunmehr voraus, dass der Täter sich oder einem anderen den Zugang zu Daten verschafft, die nicht für ihn bestimmt und die gegen unberechtigten Zugang besonders gesichert sind.

b) Entscheidende Bedeutung erlangt damit die Frage, für wen die Daten bestimmt sind. Da geschütztes Rechtsgut die Verfügungsbefugnis des Berechtigten an dem gedanklichen Inhalt der Daten ist,[29] ist insoweit anerkannt, dass es auf die Eigentümerposition am Datenträger nicht ankommen kann.[30] Speichert der Arbeitnehmer private Daten, so erlangt er hierüber die alleinige Verfügungsbefugnis.[31] Dies gilt auch, wenn die Privatnutzung des Computers nicht gestattet war, weil das bloß weisungswidrige Verhalten im Innenverhältnis keinen Einfluss auf die Verfügungsbefugnis hat.[32] Das insoweit gegenüber § 206 StGB abweichende Ergebnis lässt sich mit dem unterschiedlichen Rechtsgut erklären. Dienstlich veranlasste Datenspeicherungen sind hingegen dem Arbeitgeber zuzurechnen, da solche aufgrund des Weisungsrechts und mit Veranlassung des Arbeitgebers vorgenommen werden.[33] Soweit es speziell um den E-Mail-Verkehr geht, sind Daten, die für den Empfänger auf einem E-Mail-Server zum Abruf bereitgehalten werden, für diesen bestimmt.[34] Daraus folgt wiederum, dass dienstliche E-Mails regelmäßig für den Arbeitgeber,[35] private E-Mails hingegen für den Arbeitnehmer bestimmt sind. Was die Abgrenzung anbelangt, kann es sich insbesondere um private Nachrichten handeln, wenn dem Arbeitnehmer für diesen Zweck eine gesonderte E-Mail-Adresse mit eigenem Passwort zur Verfügung steht. Umgekehrt wird zumeist Geschäftspost vorliegen, wenn die E-Mail an eine allgemeine dienstliche E-Mail-Adresse gerichtet ist. Wie beim Brief kann im Einzelfall etwa anderes gelten, wenn ein Vermerk persönlich, vertraulich oder privat angebracht ist. Soweit der Arbeitgeber private Nachrichten des Arbeitnehmers kontrolliert, kann er sich also unter den weiteren Voraussetzungen strafbar machen.

c) § 202a StGB erfordert weiterhin, dass der Täter sich den Zugang zu den Daten durch Überwindung einer Zugangssicherung verschafft. Zugangssicherungen können insbesondere Passworte oder Verschlüsselungen sein.[36] Eine besondere Sicherung und damit eine Strafbarkeit nach § 202a StGB ist daher etwa zu verneinen, wenn unverschlüsselte E-Mails im Unternehmen anhand bestimmter Schlagworte gefiltert werden.[37] Die Zugangsverschaffung muss zudem gerade unter Überwindung der Zugangssicherung erfolgen. Bei einem Passwort kommt es daher darauf an, ob dieses auch zugunsten des Arbeitnehmers gegenüber dem Arbeitgeber Zugangssicherung bildet oder lediglich den Zugriff von anderen Arbeitnehmern und außenstehenden Dritten verhindern soll.[38] Entscheidend ist damit die Zweckbestimmung, die mit dem Passwort verfolgt wird.[39] Teilt der Arbeitgeber den einzelnen Arbeitnehmern verschiedene Passwörter zu, behält sich aber selbst eine Zugriffsmöglichkeit auf die Verzeichnisse der Mitarbeiter vor, so ist der Tatbestand nicht verwirklicht.[40] Auch kann er im Bereich der dienstlichen E-Mails aufgrund seines Direktionsrechts grundsätzlich die Mitteilung des

[27] *Gola* (Fn. 7), Rn. 118; *Heidrich/Tschoepe*, MMR 2004, 75 (78); *Schmidl*, MMR 2005, 343 (344). Vgl. aber auch *Bock* (Fn. 22), § 88 Rn. 26, wonach eine Rechtfertigung bei Viren- und Spam-Mails in Betracht kommen soll.

[28] ABl. EU 2005 Nr. L 69, S. 67; zur Umsetzung BT-Drs. 16/3656, S. 1; BT-Drs. 16/5449, S. 1; BT-Drs. 16/5486, S. 1. Dazu *Borges/Stuckenberg/Wegener*, DuD 2007, 275.

[29] OLG Köln JMBl NW 2008, 238 (239); *Lackner/Kühl* (Fn. 22), § 202a Rn. 1; *Rengier*, Strafrecht, Besonderer Teil, Bd. 2, 13. Aufl. 2012, § 31 Rn. 24; *Lenckner*, in: Schönke/Schröder (Fn. 22), § 202a Rn. 1.

[30] *Lackner/Kühl* (Fn. 22), § 202a Rn. 3; *Hilgendorf*, in: Laufhütte/Rissing-van Saan/Tiedemann (Fn. 8), § 202a Rn. 26; *Graf*, in: Joecks/Miebach (Fn. 8), § 202a Rn. 17; *Möhrenschlager*, wistra 1986, 128 (140); *Weidemann*, in: Beck'scher Onlinekommentar, Strafgesetzbuch, Stand: 15.6.2012, § 202a Rn. 4.

[31] *Mattl*, Die Kontrolle der Internet- und E-Mail-Nutzung am Arbeitsplatz unter besonderer Berücksichtigung der Vorgaben des Telekommunikationsgesetzes, 2008, S. 161; *Weißgerber*, NZA 2003, 1005 (1008).

[32] *Schuster*, ZIS 2010, 68 (70); *Weißgerber*, NZA 2003, 1005 (1008). Vgl. aber *Gola* (Fn. 7), Rn. 54.

[33] *Graf* (Fn. 30), § 202a Rn. 17; *Schuster*, ZIS 2010, 68 (69); ferner *Hilgendorf*, JuS 1996, 890 (893) zu § 303a StGB.

[34] *Lenckner/Eisele* (Fn. 22), § 202a Rn. 6.

[35] Vgl. auch *Jofer/Wegerich*, K&R 2002, 235 (238).

[36] BT-Drs. 16/3656, S. 11; *Hilgendorf/Frank/Valerius*, Computer- und Internetstrafrecht, 2005, Rn. 176; *Graf* (Fn. 30), § 202a Rn. 38; *Kargl* (Fn. 9), § 202a Rn. 10; *Hoyer* (Fn. 22) § 202a Rn. 5; and. aber *Dornseif/Schumann/Klein*, DuD 2002, 226 (229 f.).

[37] Siehe auch *Spindler/Ernst*, CR 2004, 437 (439).

[38] LAG Köln NZA-RR 2004, 527 (528); *Barton*, CR 2003, 839 (842).

[39] *Barton*, CR 2003, 839 (842); *Hoppe* (Fn. 6), S. 178.

[40] LAG Köln NZA-RR 2004, 527 (528); in dem zugrunde liegenden Sachverhalt mussten alle Arbeitnehmer bei Einrichtung der Computeranlage ihr persönliches Passwort dem Netzwerkadministrator bekannt geben; *Schuster*, ZIS 2010, 68 (70).

Passworts an andere Mitarbeiter zur Urlaubs- oder Krankheitsvertretung verlangen.[41]

d) Was Rechtfertigungsfragen anbelangt, ist bei Telekommunikationsvorgängen wiederum die Sperre des § 88 Abs. 3 TKG zu berücksichtigen. Ansonsten kann § 32 StGB im Einzelfall zu einer Rechtfertigung führen, wenn private Dateien auf Servern oder Rechnern des Arbeitgebers abgelegt werden, so dass das System aufgrund der Menge der Daten oder aufgrund von Viren, Trojanern usw. beeinträchtigt wird.[42] Soweit mit dem Zugang Beweise für zivilrechtliche, arbeitsrechtliche oder strafrechtliche Verfahren gesammelt werden sollen, ist zu beachten, dass für eine Rechtfertigung kraft Notstand (§ 34 StGB) die bloße Beweisnot nicht genügt.[43]

3. Abfangen von Daten nach § 202b StGB

Die aufgrund der Vorgaben des Art. 3 der Cybercrime-Konvention eingefügte Vorschrift des § 202b StGB ist hingegen verwirklicht, wenn der Täter sich oder einem anderen unter Anwendung von technischen Mitteln nicht für ihn bestimmte Daten aus einer nichtöffentlichen Datenübermittlung oder aus der elektromagnetischen Abstrahlung einer Datenverarbeitungsanlage verschafft. Für wen die Daten bestimmt sind und wer daher Verfügungsberechtigter im Verhältnis von Arbeitgeber und Arbeitnehmer ist, ist wie bei § 202a StGB zu bestimmen.

a) Anders als bei § 202a StGB müssen die Daten nicht besonders gesichert sein, so dass alle Formen der elektronischen Datenübermittlung durch den Arbeitnehmer erfasst werden. Zu erwähnen sind etwa E-Mail-Verkehr, Internettelefonie und auch Übertragungen innerhalb kleiner Netzwerke. Bei Var. 1 muss es sich um Daten in einem Übermittlungsvorgang handeln; nicht erfasst wird daher der Fall, dass der Arbeitgeber auf E-Mails zugreift, die bereits auf dem Rechner des Arbeitnehmers abgelegt sind. Anderes gilt nach h.M. jedoch auch hier, wenn diese noch auf dem Server zum Abruf durch den Adressaten bereitgehalten werden.[44]

b) Die Datenübermittlung muss ferner nichtöffentlich sein. Entscheidend ist, dass sich die Datenübermittlung nach Zielsetzung des Übermittelnden nicht an die Allgemeinheit, sondern an einen nur beschränkten Adressatenkreis richtet. Die Übermittlung ist daher nicht schon deshalb für die Öffentlichkeit bestimmt, weil keine Verschlüsselung benutzt wird.[45] Soweit sich die Kommunikation nur an Angehörige des Unternehmens richtet,[46] ist sie ebenfalls nichtöffentlich. Var. 2 schützt hingegen elektromagnetische Abstrahlungen einer Datenverarbeitungsanlage (insb. eines WLAN-Routers).[47] Da es hier nicht um einen Übermittlungsvorgang geht, ist auch die Abstrahlung bereits gespeicherter Daten geschützt.[48]

c) Schließlich muss sich der Täter anders als bei § 202a StGB nicht nur den Zugang zu den Daten, sondern die Daten selbst verschaffen. Ungeachtet dieser im Einzelnen umstrittenen Feinheiten soll bei E-Mails die bloße Kenntnisnahme und im Übrigen auch das Speichern und Kopieren von Daten genügen.[49]

4. Vorbereiten des Ausspähens und Abfangens von Daten nach § 202c StGB

§ 202c StGB, der auf Art. 6 Abs. 1 lit. a der Cybercrime-Konvention zurückgeht, stellt auch Vorbereitungshandlungen zu § 202a StGB und § 202b StGB unter Strafe. Tatgegenstände sind Passwörter und sonstige Sicherungscodes, die den Zugang zu Daten, d.h. ein Ausspähen nach § 202a oder ein Abfangen nach § 202b StGB ermöglichen (Nr. 1). Ferner sind Computerprogramme erfasst, deren Zweck die Begehung einer Tat nach §§ 202a, 202b StGB ist (Nr. 2). Strafbar nach dieser Vorschrift ist der Arbeitgeber etwa, wenn er Passwörter des Arbeitnehmers ausspäht, um so später Zugang zu den E-Mails zu erlangen.

5. Datenveränderung und Computersabotage nach §§ 303a, 303b StGB

a) Beim Abfangen von E-Mails und Eingreifen in Datenbestände ist ferner an eine Strafbarkeit nach § 303a StGB und auch § 303b StGB zu denken. Die Vorschriften wurden aufgrund von Art. 4 und Art. 5 der Cybercrime-Konvention sowie Art. 3 und 4 des Rahmenbeschlusses über Angriffe auf Informationssysteme modifiziert.[50] Für die Vorbereitung der §§ 303a, 303b StGB wird jeweils auf den eben angesprochenen § 202c StGB verwiesen. In unserem Zusammenhang erlangt insbesondere § 303a StGB Bedeutung, der das rechtswidrige Löschen, Unterdrücken, Unbrauchbarmachen sowie Verändern von Daten sanktioniert.

b) Rechtswidrig ist eine solche Handlung aber nur, wenn sie sich auf Daten bezieht, über die der Täter nicht die alleinige Verfügungsbefugnis besitzt. Wie bei § 202a StGB kommt es nicht auf das Eigentum am Datenträger an, sondern darauf, dass das Verfügungsrecht eines anderen,[51] der ein unmittelba-

[41] *Barton*, CR 2003, 839 (842).
[42] Vgl. auch *Weißgerber*, NZA 2003, 1005 (1008).
[43] *Weißgerber*, NZA 2003, 1005 (1008).
[44] *Schumann*, NStZ 2007, 675 (677); *Hoyer* (Fn. 22), § 202b Rn. 7; *Weidemann* (Fn. 30), § 202b Rn. 5.
[45] *Fischer*, Strafgesetzbuch und Nebengesetze, Kommentar, 59. Aufl. 2012, § 202b Rn. 4; *Hilgendorf* (Fn. 30), § 202b Rn. 9; *Weidemann* (Fn. 30), § 202b Rn. 6. Siehe aber auch *Schumann*, NStZ 2007, 675 (677).
[46] Vgl. auch *Kargl* (Fn. 9), § 202b Rn. 5.
[47] Einbezogen sind also Fälle, in denen aus Abstrahlungen (keine Daten i.S.d. § 202a Abs. 2 StGB) Daten wiederhergestellt werden; vgl. BT-Drs. 16/3656, S. 11.
[48] *Hilgendorf* (Fn. 30), § 202b Rn. 12.
[49] Siehe BT-Drs. 16/3656, S. 11; *Kargl* (Fn. 9), § 202b Rn. 6; nach AG Kamen SchAZtg 2008, 229, wird auch das Umleiten und Aufnehmen des Chat-Verkehrs erfasst. Enger hingegen *Hoyer* (Fn. 22), § 202b Rn. 6, der ein Verschaffen in der Absicht, die mit Hilfe der Daten ausgedrückten Informationen in Erfahrung zu bringen, verlangt.
[50] ABl. Nr. L 69 v. 16.3.2005, S. 67.
[51] Siehe *Lackner/Kühl* (Fn. 22), § 303a Rn. 4; *Wieck-Noodt*, in: Joecks/Miebach (Fn. 8), § 303a Rn. 9; *Zaczyk*, in: Kindhäuser/Neumann/Paeffgen (Fn. 9), § 303a Rn. 4; *Stree/*

res Interesse an dem Bestand bzw. der Unversehrtheit der Daten hat, verletzt wird. Insoweit ist auch hier zu klären, wem die Verfügungsberechtigung im Verhältnis zwischen Arbeitgeber und Arbeitnehmer zukommt. Entscheidende Bedeutung erlangt wiederum die Unterscheidung zwischen dienstlicher und privater Nutzung.

IV. Gesetzentwurf zur Regelung des Beschäftigtendatenschutzes

1. Bezug zum Strafrecht

Ein Gesetzentwurf zur Regelung des Beschäftigtendatenschutzes sieht spezifische Regelungen zur Arbeitnehmerüberwachung vor, die in das Bundesdatenschutzgesetz eingestellt werden sollen.[52] Solche Vorschriften hätten auch für den Bereich des Strafrechts Bedeutung. Zum ersten, weil Verstöße gegen diese Vorschriften Ordnungswidrigkeiten i.S.d. § 43 BDSG und ggf. auch Straftaten nach § 44 BDSG begründen würden. Zum zweiten, weil diese Vorschriften als Compliance-Maßnahmen Bedeutung erlangen sollen; so sieht etwa § 32d Abs. 3 des Vorschlags vor, dass zur Aufdeckung von Straftaten oder anderen schwerwiegenden Pflichtverletzungen, insbesondere Straftaten nach §§ 266, 299, 331 bis 334 StGB, ein automatisierter Datenabgleich vorgenommen werden darf.[53] Zum dritten würden solche Regelungen aber auch auf Rechtswidrigkeitsebene zu beachten sein, da es wenig einleuchtend wäre, wenn ein datenschutzrechtlich zulässiges Verhalten strafbares Unrecht wäre.

2. Verhältnis zum TKG

Der Entwurf möchte am Verhältnis zwischen TKG und BDSG nichts ändern, so dass die Regelungen des BDSG mit der h.M. nur gelten sollen, wenn eine Privatnutzung nicht gestattet ist.[54] Bei gestatteter Privatnutzung richten sich die Maßnahmen dann weiter nach dem TKG. Entscheidend soll dabei die abstrakte Erlaubnis zur Privatnutzung und nicht die tatsächliche Nutzung sein.[55] Dies begegnet erneut Bedenken: Denn damit würden die geplanten Vorschriften, die detailliert die Arbeitnehmerüberwachung bei Telefon-, E-Mail- und Internetnutzung regeln, häufig nicht zur Anwendung gelangen, so dass nur die engen Überwachungsmöglichkeiten nach TKG in Betracht kommen, die jedoch nicht auf die Arbeitnehmerüberwachung zugeschnitten sind. Der Gesetzgeber würde daher dieses wichtige Problemfeld nur teilweise regeln. Im Ergebnis ist damit der Arbeitgeber, der seinen Mitarbeitern auch in deren Interesse die Privatnutzung gestattet, hinsichtlich der Wahrung seiner schutzwürdigen Interessen selbst bei der Kontrolle dienstlicher E-Mails stark eingeschränkt.

3. Exemplarisch: E-Mail-Kontrolle

a) Nach § 32i Abs. 3 des Vorschlags darf der Arbeitgeber Inhalte bei E-Mails erheben, verarbeiten und nutzen, soweit dies zur Gewährleistung des ordnungsgemäßen Betriebs von Telekommunikationsnetzen oder Telekommunikationsdiensten, einschließlich der Datensicherheit oder zu einer stichprobenartigen oder anlassbezogenen Leistungs- oder Verhaltenskontrolle erforderlich ist und keine Anhaltspunkte dafür bestehen, dass das schutzwürdige Interesse des Beschäftigten an dem Ausschluss der Erhebung, Verarbeitung oder Nutzung überwiegt. Dies gilt auch, soweit es für den ordnungsgemäßen Dienst- oder Geschäftsbetrieb des Arbeitgebers in den Fällen einer Versetzung, Abordnung oder Abwesenheit (z.B. Urlaub) erforderlich ist.

b) Die Telekommunikation soll im Übrigen mit dem Empfang der übermittelten Signale – bei E-Mails mit Eingang auf dem „Arbeitsplatzcomputer" – abgeschlossen sein.[56] Dies überzeugt so allerdings nicht ohne weiteres, da E-Mails häufig auf dem Server des Arbeitgebers verbleiben.[57] Der Gesetzgeber jedenfalls hat dieses Problem in seiner Dimension vollständig verkannt. Der Arbeitgeber darf nach diesem Vorschlag erkennbar[58] private Daten und Inhalte nur erheben, verarbeiten und nutzen, wenn dies zur Durchführung des ordnungsgemäßen Dienst- oder Geschäftsbetriebes unerlässlich ist und er den Beschäftigten hierauf schriftlich hingewiesen hat. Die Begründung nennt den Fall, dass der Beschäftigte erkrankt ist und zur Bearbeitung dienstlicher E-Mails die gesamte elektronische Post samt privater Nachrichten gesichtet werden muss. Freilich muss man sehen, dass bei erlaubter privater Nutzung das BDSG ja auch nach Ansicht des Gesetzgebers gar nicht anwendbar sein soll,[59] so dass der Anwendungsbereich auch dieser Vorschrift beschränkt wäre.

V. Europäischer Kontext

Ein aktueller Vorschlag der EU für eine Verordnung zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (Datenschutz-Grundverordnung), die die bisher geltende Datenschutzrichtlinie 95/46/EG ersetzen soll, sieht vor allem die Einwilligung des Arbeitnehmers kritisch: „Die Einwilligung liefert keine rechtliche Handhabe für die Verarbeitung personenbezogener

Hecker, in: Schönke/Schröder (Fn. 22), § 303a Rn. 3; *Hoyer* (Fn. 22), § 303a Rn. 5; *Hilgendorf*, in: Satzger/Schmitt/Widmaier (Fn. 22), § 303a Rn. 5.

[52] BT-Drs. 17/4230. Vgl. den Diskussionsentwurf eines Gesetzes zum Datenschutz im Beschäftigungsverhältnis des Bundesministeriums für Arbeit und Soziales v. August 2009; siehe ferner den Referentenentwurf eines Gesetzes zur Regelung des Beschäftigtendatenschutzes des Bundesministerium des Innern v. 28.5.2010; Hintergrundpapier zum Entwurf eines Gesetzes zur Regelung des Beschäftigtendatenschutzes, Kabinettsbeschluss v. 25.8.2010.

[53] BT-Drs. 17/4230, S. 18.

[54] BT-Drs. 17/4230, S. 21 und S. 42; Hintergrundpapier zum Gesetzentwurf Beschäftigtendatenschutz v. 25.8.2010, S. 6; *Beckschulze/Natzel*, BB 2010, 2368 (2374); *Vietmeyers/Bryers*, MMR 2010, 807.

[55] Zum Entwurf eines Gesetzes zur Regelung des Beschäftigtendatenschutzes BT-Drs. 17/4230, S. 42.

[56] BT-Drs. 17/4230, S. 22.

[57] Siehe auch *Vietmeyer/Byers*, MMR 2010, 807 (809 f.).

[58] BT-Drs. 17/4230, S. 22.

[59] BT-Drs. 17/4230, S. 42.

Daten, wenn zwischen der Position der betroffenen Person und des für die Verarbeitung Verantwortlichen ein klares Ungleichgewicht besteht. Dies ist vor allem dann der Fall, wenn sich die betroffene Person in einem Abhängigkeitsverhältnis von dem für die Verarbeitung Verantwortlichen befindet, zum Beispiel dann, wenn personenbezogene Daten von Arbeitnehmern durch den Arbeitgeber im Rahmen von Beschäftigungsverhältnissen verarbeitet werden."[60] Eine solche Regelung würde Compliance- Maßnahmen gegenüber der geltenden Rechtslage eine weitere empfindliche Grenze setzen. Im Übrigen möchte der Vorschlag den Mitgliedstaaten die Regelung der Verarbeitung personenbezogener Arbeitnehmerdaten im Beschäftigungskontext jedoch in den von der geplanten Verordnung gezogenen Grenzen weiterhin überlassen.

[60] Erwägungsgrund 34 des Vorschlags; vgl. KOM(2012) 11 endg.

Die „Lufthansa-Blockade“ 2001 – eine (strafbare) Online-Demonstration?*

Von Wiss. Mitarbeiter **Sebastian Hoffmanns**, Gießen

Repeatedly there are reports of attacks on Websites of companies. These attacks are often made by individuals or groups wishing to express their displeasure with actions of the operators of the website. Ever since the attack on the website of Lufthansa in 2001, German jurisprudence and literature discuss the concept of „online“ demonstration. The aim of the Lufthansa attack was to hamper access to the website by simultaneous access from a large number of Internet users to the website. The actors planned to demonstrate against the participation of Lufthansa in the so-called „deportation-business“. It appears questionable, whether such an action is comparable to a „common“ demonstration. Here it is important to know that the German Constitution protects a demonstration only if it takes place „peacefully and without arms“. A similarity to so called DDoS-Attacks, which are punishable in Germany, cannot be rejected. This paper deals with the question, if such an online demonstration is a crime under German criminal law, or if there is a constitutional right to demonstrate online.

I. Einführung: „Demonstrieren“ im Internet

Mit der fortschreitenden Technik verändert sich auch die Kommunikation. Gerade das Internet hat sich mit seinen unzähligen Möglichkeiten zu kommunizieren zu einem der Zentren der modernen Kommunikation entwickelt.[1] Kommunikationsmöglichkeiten eröffnen auch die Möglichkeit zum Meinungsaustausch. Es war daher zu erwarten, dass sich aus einer solchen Möglichkeit auch neue Formen des (Online-) Protestes entwickeln. Im realen Leben gibt es die Möglichkeit, sich zu einer Versammlung zu verabreden und dort seinen Standpunkt zu einem politisch relevanten Thema vor einer Vielzahl von Menschen zum Ausdruck zu bringen. Im Internet gibt es zumindest die Möglichkeit des physischen Aufeinandertreffens von Personen nicht. Nichtsdestotrotz ist es möglich, seine Meinung auf unterschiedlichste Art und Weise zu verbreiten.

1. Meinungsaustausch im Internet

Es ist etwa möglich, Meinungen für alle Besucher sichtbar auf einer Internetseite, z.B. Facebook oder Twitter, zu veröffentlichen. Allerdings hat der nicht an dem Anliegen interessierte Nutzer keine Probleme, entsprechende Einträge mit wenigen Mausklicks aus seinem Sichtfeld zu schaffen. Ebenfalls denkbar wäre, sich mit kleinen bunten Avataren in einer virtuellen Umgebung, z.B. einem Online-Spiel, zu „versammeln“, um dort zu demonstrieren. Anwesende Spieler könnten sich dem „Protest“ je nach Gestaltung des Programms nur schwer entziehen, wenn sie das Programm nicht verlassen wollen. Es würde jedoch eine im Verhältnis eher kleine Zielgruppe erreicht. Der Protest vieler Personen per E-Mail erscheint auch nicht besonders effektiv. Heutzutage bereitet es keine große Mühe, einen Spamfilter so einzurichten, dass E-Mails mit bestimmten Begriffen im Betreff oder im Text den E-Mail Posteingang des Adressaten gar nicht erreichen, sondern bereits vorher aussortiert werden. Der demonstrationswillige Netzbürger[2] hat also das Problem, dass er seinen Protest nach außen hin bemerkbar machen muss, um überhaupt mit seinem Anliegen wahrgenommen zu werden.

So machen es sich die Demonstranten bei einer Online-Demonstration zu Nutze, dass inzwischen fast jede Person des öffentlichen Lebens, nahezu jede Behörde sowie der größte Teil der privaten Unternehmen über eine eigene Internetpräsenz verfügen. Über eine Webseite können zum Beispiel im Falle von Behörden für Bürger wichtige Informationen bereit gestellt werden oder sogar Anfragen direkt übermittelt werden, die den Behördengang ersparen und der Behörde ein schnelleres, effektiveres Arbeiten ermöglichen.[3] Viele Unternehmen wickeln teilweise (Lufthansa) bis vollständig (Amazon[4]) ihre Geschäfte online ab. Wie eine sogenannte Online-Demonstration abläuft, zeigt die „Lufthansa-Blockade“ aus dem Jahr 2001.

---

* Vortrag im Rahmen der AIDP-Tagung „Cybercrime: Ein deutsch-türkischer Rechtsdialog“ an der Bilgi Üniversitesi in Istanbul (Türkei) vom 13.-15.10.2011. Der Vortragsstil wurde weitgehend beibehalten.

[1] Laut der ARD/ZDF-Onlinestudie (abrufbar unter http://www.ard-zdf-onlinestudie.de/ [zuletzt aufgerufen am 30.3.2012]) waren im Jahr 2011 73,3 % der deutschen Bevölkerung ab einem Alter von 14 Jahren online. Hauptsächlich genutzt wurden Anwendungen zum Versand von E-Mails (80 % aller Internetnutzer) und Suchmaschinen (83% aller Internetnutzer). 43% der Internetnutzer verfügen über ein Profil bei einem sozialen Netzwerk wie etwa Facebook.

[2] Dieser Begriff ist von dem englischen Begriff „Netizen“ in die deutsche Sprache übernommen worden. Geprägt haben dieses Wort *Ronda* und *Michael Hauben*, die die „Netizens“ als Personen beschreiben, die mehr tun, als das Internet bloß zum Abrufen von Informationen zu benutzen, sondern vielmehr aktiv insbesondere am sozialen Ausbau dieses Mediums beteiligt sind oder Informationen für andere Nutzer, etwa in Blogs, zur Verfügung stellen. Vgl. *Hauben*, Netizens: On the History and Impact of Usenet and the Internet, 1997, passim.

[3] So ist z.B. inzwischen in vielen Städten die Online-Anforderung von Urkunden über die Webseite des Standesamtes möglich, z.B. in Berlin Charlottenburg-Wilmersdorf http://www.berlin.de/ba-charlottenburg-wilmersdorf/org/standesamt/onlinebestellung.html (zuletzt aufgerufen am 30.3.2012) oder Langenfeld (Rhld.) https://www.xsta.de/x/src/Start.php?urlConfId=langenfeld (zuletzt aufgerufen am 30.3.2012).

[4] Laut http://www.businesswire.com/news/home/20101227005123/en/Third-Generation-Kindle-Bestselling-Product-Time-Amazon-Worldwide (zuletzt aufgerufen am 30.3.2012) wurden 2010 am Spitzentag (29.11.2010) im Schnitt 158 Bestellungen pro Sekunde über die Amazon Webseite getätigt.

2. „Die Lufthansa-Blockade" (2001)

Im Juni 2001 rief ein politischer Aktivist dazu auf, die Internetpräsenz der Lufthansa, über die unter anderem das Buchen von Reisen möglich ist, zeitweise zu blockieren. Damit sollte dagegen protestiert werden, dass die Lufthansa AG im staatlichen Auftrag abzuschiebende Personen in ihren Flugzeugen befördert. Die Blockade der Webseite sollte nach dem Willen des Initiators Ähnlichkeit mit einer Sitzblockade haben und dazu führen, dass das Vertrauen der Kunden in das Online-Buchungssystem gestört wird. Um dieses Ziel zu erreichen, sollte eine Vielzahl von Internetnutzern zur gleichen Zeit auf die Internetseite zugreifen, um diese vorübergehend zu blockieren.[5] Es erfolgten insgesamt 1.262.000 Zugriffe von 13.614 unterschiedlichen IP-Adressen auf die Webseite der Lufthansa AG. Dies reichte aus, um die Webserver der Lufthansa AG für ca. zwei Stunden erheblich zu verlangsamen und zeitweise zum Erliegen zu bringen. Der Lufthansa AG entstand durch die ganze Aktion ein Schaden in Höhe von insgesamt 47.867,19 €.[6]

3. Funktionsweise der Online-Demonstration

Jede Webseite ist auf einem Webserver gespeichert. Hierbei handelt es sich um einen in der Regel unter Dauerbetrieb laufenden Rechner, der Speicherplatz für über das Internet abrufbare Inhalte zur Verfügung stellt und diese mittels einer Serversoftware verwaltet. Der Webserver ist auch dafür zuständig, die Zugriffe, also die Übertragung von Daten an einen Client,[7] z.B. einen Webbrowser, auf eine Internetseite zu verwalten, indem dieser für jeden Zugriff eine bestimmte Menge an Speicher reserviert.[8] Bei zu vielen gleichzeitigen Anfragen ist der Server nicht mehr in der Lage, genügend Speicherplatz für neue Anfragen zur Verfügung zu stellen. Es kommt entweder zu einem stark verzögerten Aufbau der angeforderten Internetseite oder sogar dazu, dass der Server gar nicht mehr in der Lage ist, neue Anfragen zu verarbeiten. Dann verweigert er den Zugriff auf die Webseite.[9] Ein Vorgehen wie bei der „Lufthansa-Blockade" führt also zu dem gewünschten Ziel, eine Webseite lahmzulegen, wenn sich genug Personen daran beteiligen.

Ziel einer Online-Demonstration ist es also, durch das Blockieren einer Webseite auf ein Anliegen aufmerksam zu machen.[10] Bedenkt man, wie schnell sich Nachrichten dank Diensten wie Twitter, Facebook & Co. heutzutage über das Internet verbreiten lassen und über Suchmaschinen für jedermann in kürzester Zeit abrufbar sind, so ist es nicht unwahrscheinlich, dass man auf der Suche nach den vermeintlichen technischen Schwierigkeiten auf die Ankündigung einer Online-Demonstration stößt. Die Online-Demonstration betrifft somit jede Person, die versucht, auf eine solche Webseite zuzugreifen und zeigt damit, insbesondere bei populären Web-Angeboten, eine erhebliche Außenwirkung.

4. Online-Demonstration versus DDoS-Attacke

Bei der „Lufthansa-Blockade" erfolgte eine große Zahl der Zugriffe nicht durch einfaches Bedienen der „Seite neu laden"-Funktion des Browsers. Der Initiator der Online-Demonstration hatte für den Zeitraum der Aktion eine Software zur Verfügung gestellt, die die Zugriffsfrequenz des einzelnen Online-Demonstranten auf eine Geschwindigkeit erhöhte, die durch manuelles neues Laden der Internetseite nicht möglich gewesen wäre.[11] Dies erklärt auch die große Differenz zwischen den tatsächlich erfolgten Zugriffen und der Anzahl der IP-Adressen, von denen aus die Zugriffe erfolgten. In dieser Konstellation erinnert die Online-Demonstration gegen die Lufthansa AG stark an eine sog. DDoS-Attacke.[12] Auch bei der DDoS-Attacke wird ein Webserver durch mehr Anfragen, als er gleichzeitig zu bearbeiten in der Lage ist, zum Erliegen gebracht, damit dieser seinen Dienst wegen Überlastung einstellt. Die technische Auswirkung auf die betroffene Webseite ist bei beiden Vorgehensweisen exakt die gleiche: Die Webseite ist zeitweise nur verlangsamt oder gar nicht aufrufbar.

Im Unterschied zur Online-Demonstration werden bei der DDoS-Attacke häufig sog. Botnetzwerke verwendet. Diese bestehen aus einer Vielzahl von Rechnern, die gleichzeitig Anfragen an den Webserver senden. Der Besitzer des einzelnen Rechners bekommt davon oftmals nichts mit, da der PC durch einen vorher eingeschleusten Trojaner „ferngesteuert" wird.[13] Der Hauptunterschied in tatsächlicher Hinsicht zwischen Online-Demonstration und DDoS-Attacke ist, dass die DDoS-Attacke von einer einzigen Person gesteuert werden

[5] Für eine ausführliche Darstellung des Sachverhalts siehe AG Frankfurt a.M., Urt. v. 1.7.2005 – 991 Ds 6100 Js 226314/01 = MMR 2005, 863 sowie *Medosch*, in: Schulzki-Haddouti (Hrsg.), Bürgerrechte im Netz, 2003, S. 261 (S. 295 ff.).

[6] Dieser Betrag ergab sich aus einem materiellen Schaden von 5.496,39 € sowie 42.370,80 € Fremdkosten, vgl. AG Frankfurt a.M., Urt. v. 1.7.2005 – 991 Ds 6100 Js 226314/01 = MMR 2005, 863 (864).

[7] Vgl. *Böckenförde*, Die Ermittlung im Netz, 2003, S. 29 f.; ausführlich zur Funktionsweise der Kommunikation zwischen Server und Client *Valerius*, Ermittlungen der Strafverfolgungsbehörden in den Kommunikationsdiensten des Internet, 2004, S. 5 ff.

[8] Zur Funktionsweise von Webservern vgl. http://www.itwissen.info/definition/lexikon/Webserver-web-server.html (zuletzt aufgerufen am 30.3.2012).

[9] Siehe zur Funktionsweise auch *Medosch* (Fn. 5), S. 261 (S. 262).

[10] Siehe etwa *Pifan*, http://www.spiegel.de/netzwelt/web/0,1-518,82964,00.html (zuletzt aufgerufen am 30.3.2012).

[11] Siehe etwa http://no-racism.net/article/575/ (zuletzt aufgerufen am 30.3.2012).

[12] DDoS steht für „Distributed Denial of Service", zu Deutsch: „Verweigerung des Dienstes". „Distributed" (verteilt) bedeutet, dass der Angriff nicht von einem einzelnen, sondern von vielen verteilten Rechnern aus erfolgt, vgl. http://www.computerlexikon.com/definition-ddos (zuletzt aufgerufen am 30.3.2012).

[13] Siehe hierzu *Kamluk*, Botnetze – Geschäfte mit Zombies, http://www.viruslist.com/de/analysis?pubid=200883611 (zuletzt aufgerufen am 30.3.2012)

kann. Für diese Person ist der Erfolg der Attacke vorhersehbar, wenn ihr bekannt ist, über wie viele Rechner das Botnetzwerk verfügt. Der Initiator sowie auch der einzelne Teilnehmer einer Online-Demonstration können hingegen nicht sicher sein, ob sich genügend Personen an dieser beteiligen werden.

III. Strafrechtliche Würdigung

Unklarheit besteht darüber, ob ein solches Verhalten als strafbar anzusehen ist. Die inzwischen geläufige Bezeichnung als Online-Demonstration legt jedoch nahe, dass für diese andere Maßstäbe gelten müssen, als für bloßen Web-Vandalismus.

1. Verurteilung im Fall der „Lufthansa-Blockade“

In erster Instanz wurde der Initiator der „Lufthansa-Blockade“ 2005 durch das Amtsgericht Frankfurt a.M. wegen eines öffentlichen Aufrufs zu Straftaten (§ 111 StGB) verurteilt.[14] Das Amtsgericht sah in der Blockade der Internetseite der Lufthansa AG, zu der der Angeklagte aufgerufen hatte, eine strafbare Nötigung (§ 240 StGB). Bei dem Mausklick, der den Blockadeprozess in Gang setzte, handelte es sich nach der Auffassung des Gerichts um Gewalt i.S.d. Nötigung (§ 240 StGB). Die physische Wirkung würde zum einen gegenüber den Besuchern der Internetseite entfaltet, da diese nicht mehr auf die Webseite zugreifen können. Zum anderen liege Gewalt auch gegenüber den verantwortlichen Personen bei der Lufthansa AG vor, indem der Kontakt zu den Kunden über die Webseite unterbunden wurde.[15] Das OLG Frankfurt a.M. hob die Verurteilung auf und führte aus, dass es sich bei der Beeinträchtigung der Webseitenbesucher gerade nicht um eine physische Einwirkung und somit nicht um Gewalt im Sinne von § 240 StGB handelt.[16]

2. Datenunterdrückung, § 303a StGB

Wegen Datenunterdrückung macht sich gem. § 303a Abs. 1 StGB strafbar, „wer rechtswidrig Daten[17] löscht, unterdrückt, unbrauchbar macht oder verändert“. Die Subsumtion der Online-Demonstration unter diese Vorschrift erscheint jedoch schwierig, da bis auf wenige Ausnahmen auch die DDoS-Attacke nicht von dieser erfasst ist.[18]

3. Computersabotage, § 303b StGB

Der Streit um die Subsumtion unter § 303a StGB könnte seit 2007, also nach den Entscheidungen im Fall der „Lufthansa-Blockade“, jedoch bedeutungslos geworden sein, wenn die Online-Demonstration den Tatbestand der Computersabotage, § 303b StGB, erfüllt. § 303b StGB wurde durch das 41. Strafrechtsänderungsgesetz 2007 zur Umsetzung der Convention on Cybercrime des Europarates umfassend überarbeitet und zu einem eigenständigen Tatbestand ausgebaut.[19] Die Vorschrift entspricht jetzt den Vorgaben des Art. 5 der Convention on Cybercrime des Europarats.[20]

Schutzgut der Strafnorm ist die Funktionsfähigkeit von Datenverarbeitungsvorgängen.[21] Als Tathandlung genügt, entsprechend den Vorgaben in der Convention on Cybercrime, bereits jedes Eingeben oder Übermitteln von Daten in ein Computersystem. Als Taterfolg ist der tatsächliche Eintritt der Störung einer Datenverarbeitung erforderlich.[22] Obwohl die Norm somit geradezu auf Webseitenattacken ausgerichtet ist,[23] gibt es bis jetzt nur eine Entscheidung des Landgerichts Düsseldorf, welches den Verwender einer DDoS-Attacke

[14] AG Frankfurt a.M., Urt. v. 1.7.2005 – 991 Ds 6100 Js 226314/01 = MMR 2005, 863 (864).

[15] AG Frankfurt a.M., Urt. v. 1.7.2005 – 991 Ds 6100 Js 226314/01 = MMR 2005, 863 (865); so sahen dies auch bereits 2003 *Kraft/Meister*, MMR 2003, 366 (370).

[16] OLG Frankfurt a.M., Beschl. v. 22.5.2006 – 1 Ss 319/05 = MMR 2006, 547, kritisch hinsichtlich einer Strafbarkeit gem. § 240 Abs. 1 StGB bereits *Gercke*, Anmerkung zu AG Frankfurt a.M., Urt. v. 1.7.2005 – 1 Ss 319/05 = MMR 2005, 863 (868 f.); siehe zum Erfordernis der physischen Wirkung von Gewalt auch *Sinn*, Die Nötigung im System des heutigen Strafrechts, 2000, S. 202 ff., insb. S. 207: Eine Kraftentfaltung als solche kann nicht allein das Kriterium für die Annahme von Gewalt darstellen.

[17] Der Begriff der Daten ist legaldefiniert in § 202a Abs. 2 StGB: „Daten […] sind nur solche, die elektronisch, magnetisch oder sonst nicht unmittelbar wahrnehmbar gespeichert sind oder übermittelt werden.“

[18] So soll eine strafbare Datenveränderung jedenfalls nur dann vorliegen, wenn es durch einen Systemabsturz zum Datenverlust kommt, was in der Regel bei einer vorübergehenden Nichterreichbarkeit einer Webseite nicht der Fall ist. Hier käme allenfalls ein zeitweiliges Unterdrücken von Daten in Betracht, vgl. *Wolff*, in: Laufhütte/Rissing-van Saan/Tiedemann (Hrsg.), Strafgesetzbuch, Leipziger Kommentar, Bd. 10, 12. Aufl. 2008, § 303a Rn. 33, sowie *Faßbender*, Angriffe auf Datenangebote im Internet und deren strafrechtliche Relevanz: Distributed Denial of Service Angriffe, 2003, S. 30 ff.

[19] Zuvor handelte es sich nach dem Willen des Gesetzgebers bei der Computersabotage lediglich um einen Qualifikationstatbestand des § 303a StGB, BT-Drs. 10/5058, S. 35 f.

[20] Artikel 5 (Convention on Cybercrime) – Eingriff in ein System: „Jede Vertragspartei trifft die erforderlichen gesetzgeberischen und anderen Maßnahmen, um die unbefugte schwere Behinderung des Betriebs eines Computersystems durch Eingeben, Übermitteln, Beschädigen, Löschen, Beeinträchtigen, Verändern oder Unterdrücken von Computerdaten, wenn vorsätzlich begangen, nach ihrem innerstaatlichen Recht als Straftat zu umschreiben.“

[21] Vgl. BT-Drs. 16/3656, S. 13; *Stree/Hecker*, in: Schönke/Schröder, Strafgesetzbuch, Kommentar, 28. Aufl. 2010, § 303b Rn. 1; *Wolff* (Fn. 18), § 303b Rn. 2. Dies entspricht dem Schutzgut des § 303a StGB, siehe hierzu BT-Drs. 10/5058, S. 34; *Hilgendorf*, JuS 1996, 890; *Stree/Hecker* (a.a.O.), § 303a Rn. 1.

[22] Vgl. etwa *Hilgendorf/Frank/Valerius*, Computer- und Internetstrafrecht, 2005, S. 57 Rn. 207.

[23] Vgl. auch BT-Drs. 16/3656, S. 13 sowie *Schumann*, NStZ 2007, 675 (679) und *Cornelius*, in: Leupold/Glossner (Hrsg.), Münchener Anwaltshandbuch IT-Recht, 2. Aufl. 2011, Teil 10 Rn. 109.

wegen Computersabotage verurteilte, die es in die überregionalen Medien geschafft hat.[24] Mit diesem Urteil schließt sich das Landgericht Düsseldorf einer in der strafrechtlichen Literatur bereits seit einiger Zeit vertretenen Auffassung an.[25] Bis jetzt sucht man allerdings vergebens nach veröffentlichter Rechtsprechung, aus der hervorgeht, ob es sich auch bei einer Online-Demonstration um eine strafbare Computersabotage handelt.

Bei der Frage, ob die Online-Demonstration ein Fall von § 303b StGB ist, kann das subjektive Erfordernis der Eingabe oder Übermittlung in Nachteilszufügungsabsicht weiterhelfen. Durch diese Voraussetzung erfährt der sehr weite objektive Tatbestand eine Einschränkung. Der angestrebte Nachteil muss in der Beeinträchtigung des Betreibens von Computersystemen liegen.[26] In dem der Entscheidung des Landgerichts Düsseldorf zugrunde liegenden Sachverhalt lag eine solche Absicht vor, da es dem Angeklagten darum ging, verschiedene Unternehmen mit der Durchführung von DDoS-Attacken zu erpressen.[27] Die Nachteilszufügungsabsicht kann auch dann vorliegen, wenn die Dateneingabe oder Datenübermittlung aufgrund von nachvollziehbaren Gründen – wie etwa politischer oder gesellschaftlicher Anliegen – erfolgt[28], wie es gerade bei der Online-Demonstration der Fall ist. Auch im Fall der „Lufthansa-Blockade“ 2001 lag eine Nachteilszufügungsabsicht vor. Die Blockade der Webseite sollte auch dazu führen, dass das Vertrauen der Kunden in das Online-Buchungssystem durch die Beeinträchtigung seiner Funktionsfähigkeit gestört wird. Heute nach der Gesetzesänderung wäre damit ein Fall von strafbarer Computersabotage anzunehmen. Eine Online-Demonstration wird damit grundsätzlich vom Tatbestand des § 303b StGB erfasst.[29]

Allerdings sollte hier differenziert werden: Es muss unterschieden werden, ob die Online-Demonstration, wie bei der „Lufthansa-Blockade“, unter Zuhilfenahme einer den Erfolg wahrscheinlicher machenden Software verwendet wird, oder aber ob tatsächlich nur manuell auf eine Internetseite zugegriffen wird. Greift der Internetdemonstrant nur manuell auf die Webseite zu, stellt sich für die Strafverfolgung das Problem, dass der Zugriff eines Demonstranten nicht von dem Zugriff einer Person zu unterscheiden ist, die die Webseite besucht, um sie ihrem eigentlichen Zweck entsprechend zu verwenden. Bei der Verwendung von Hilfsmitteln wie entsprechenden Programmen hingegen lässt sich anhand der auf dem Webserver gespeicherten Zugriffsprotokolle feststellen, von welcher IP-Adresse eine so hohe Anzahl von Anfragen auf die Webseite einging, wie sie bei „ordnungsgemäßer“ Verwendung, also manuellem Nachladen der Internetseite, nicht möglich gewesen wäre.[30] Der Online-Demonstrant, der sich keiner Hilfsmittel bedient, verwendet die Webseite also, wie dies vom Betreiber vorgesehen ist. Dass so viele „normale“ Zugriffe gleichzeitig erfolgen können, dass der Zugriff auf die Internetseite zeitweise verlangsamt wird oder nicht möglich ist, fällt in den Risikobereich des Webseitenbetreibers, da er es in der Hand hat, Serverkapazitäten zur Verfügung zu stellen, die auch einer großen Anzahl an gleichzeitigen Zugriffen standhalten. Eine uneingeschränkte Anwendung des § 303b StGB auf Online-Demonstrationen, die ohne Hilfsmittel erfolgen, würde dazu führen, dass der Online-Demonstrant auch dann dem Risiko der Strafverfolgung ausgesetzt ist, wenn der Webseitenbetreiber nur sehr geringe Serverkapazitäten bereitstellt. In diesem Fall ist der Tatbestand der Computersabotage daher restriktiv anzuwenden.

Wird aber eine Software verwendet, die das Risiko für den Ausfall der Webseite über das allgemeine Risiko der Serverüberlastung auch bei dem Vorhandensein ausreichender Serverkapazitäten hinaus anhebt, dann kann diese Einschränkung nicht gelten. In diesem Fall ist der Ausfall nämlich dem Verwender dieser Software und nicht dem Webseitenbetreiber, der nicht für ausreichende Serverkapazitäten gesorgt hat, zurechenbar. Ein gutes Beispiel ist abermals die „Lufthansa-Blockade“, da hier 1.262.000 Zugriffe von lediglich 13.614 IP-Adressen erfolgten. Richtigerweise wäre ein solches Verhalten genau wie die DDoS-Attacke als eine strafbare Computersabotage zu behandeln. § 303b StGB schließt somit auch eine Strafbarkeitslücke, die insbesondere bei mit DDoS-Attacken vergleichbaren Verhaltensweisen bestand.

IV. Erfordernis eines (grundrechtlichen) Schutzes von Online-Demonstrationen

Eine uneingeschränkte Anwendung der Strafvorschriften auf die ohne technische Hilfsmittel durchgeführte Online-Demonstration könnte darüber hinaus gegen Grundrechte verstoßen. Dies wäre der Fall, wenn der Initiator und die Teilnehmer der Demonstration sich auf ein Grundrecht oder ein ähnliches Recht berufen können, das eine Online-Demonstration als legitimes Mittel der Meinungsäußerung zugesteht.[31] Dann wäre es erforderlich, § 303b StGB verfassungskonform auszulegen.

1. Versammlungsfreiheit, Art. 8 GG

Die Teilnehmer an der Online-Demonstration gegen die Lufthansa AG beriefen sich auf ihre Versammlungsfreiheit aus

[24] Vgl. http://www.spiegel.de/netzwelt/netzpolitik/0,1518,768245,00.html (zuletzt aufgerufen am 30.3.2012).

[25] So etwa *Lackner/Kühl*, Strafgesetzbuch, Kommentar, 27. Aufl. 2011, § 303b Rn. 5; *Wolff* (Fn. 18), § 303b Rn. 25; *Zaczyk*, in: Kindhäuser/Neumann/Paeffgen (Hrsg.), Nomos Kommentar, Strafgesetzbuch, Bd. 2, 3. Aufl. 2010, § 303b Rn. 6; *Hilgendorf/Frank/Valerius* (Fn. 22) S. 55 Rn. 197 hingegen sieht sowohl Online-Demonstration als auch DDoS-Attacke als Fall von § 303a StGB.

[26] Vgl. *Wolff* (Fn. 18), § 303b Rn. 28.

[27] Vgl. LG Düsseldorf, Urt. v. 22.3.2011 – 3 KLs 1/11 = MMR 2011, 624 (625); für eine ausführliche Darstellung des Sachverhalts vgl. a.a.O. 624 f.

[28] So auch *Wolff* (Fn. 18), § 303b Rn. 29.

[29] Von der Online Demonstration zu unterscheiden ist der sog. Massen-E-Mail-Protest, welcher nicht den Tatbestand des § 303b StGB erfüllt, da es an der erforderlichen Nachteilzufügungsabsicht fehlt. Vgl. BT-Drs. 16/5449, S. 5, sowie *Cornelius* (Fn. 23), Rn. 109.

[30] Vgl. *Medosch* (Fn. 5), S. 261 (S. 272).

[31] Siehe hierzu auch BT-Drs. 16/5449, S. 6.

Art. 8 GG.[32] Dieser Artikel verweist nicht ausdrücklich auf das Recht zu demonstrieren, sondern auf das Recht, sich zu versammeln. Vor dem Hintergrund dieser Überlegung sind durchaus Versammlungen denkbar, die keine Demonstrationen sind, aber auch Demonstrationen, die keine Versammlungen sind.[33] Eine Versammlung setzt jedoch voraus, dass sich eine Anzahl von Menschen physisch an einem gemeinsamen Ort aufhält.[34] Bei einer Online-Demonstration „treffen“ zwar die Serveranfragen der einzelnen Teilnehmer „aufeinander“, die Teilnehmer können sich jedoch an ganz verschiedenen Orten mit Internetzugang befinden. Sie müssen jedoch gerade keinen gemeinsamen physischen Aufenthaltsort haben. Die Versammlungsfreiheit schützt somit keine Online-Demonstrationen.

2. Meinungsfreiheit, Art. 5 Abs. 1 GG

Auch die Meinungsfreiheit[35] erscheint nicht geeignet, den gleichen Schutz zu gewährleisten. Geschützt würde hier lediglich die übermittelte Meinung der Demonstrierenden, nicht jedoch die Online-Demonstration als solche.[36]

3. EMRK

Des Weiteren finden sich auch in der EMRK (Europäische Menschenrechtskonvention) keine Menschenrechte, die ausdrücklich eine Online-Demonstration schützen. Art. 11 Abs. 1 EMRK[37] schützt Versammlungen, die ein Zusammentreffen von Menschen voraussetzen.[38] Art. 10 Abs. 1 EMRK[39] schützt Meinungen und Meinungsäußerungen in jeder Kommunikationsform,[40] also auch den Meinungsaustausch über das Internet. Auch ist die Möglichkeit geschützt, Meinungen durch eine Handlung zum Ausdruck zu bringen.[41] Denkbar wäre es also, einen Schutz der Online-Demonstration über Art. 10 Abs. 1 EMRK anzunehmen. Es existiert allerdings keine Entscheidung des Europäischen Gerichtshofes für Menschenrechte, die dies bestätigen würde. Überdies steht die EMRK in der deutschen Rechtsordnung im Rang eines einfachen Bundesgesetzes und gewährleistet somit nicht den gleichen Schutz wie ein Grundrecht.[42]

4. Eigener Schutzbereich über Art. 2 Abs. 1 GG

Bis jetzt gibt es kein ausdrücklich verankertes Grund- oder Menschenrecht, das die Online-Demonstration als legitimes Pendant der Versammlung im virtuellen Raum anerkennt. Die maßgeblich zu stellende Frage ist, ob für Online-Demonstrationen ein dem Versammlungsgrundrecht ähnlicher Schutz über Art. 2 Abs. 1 GG, die allgemeine Handlungsfreiheit,[43] zu gewährleisten ist. Dies ist naheliegend, da die Aussagekraft neuer Protestformen im Internet durchaus mit einer Versammlung vergleichbar sein kann. Der Schutzbereich von Art. 2 Abs. 1 GG erfasst zunächst jedes Tun und Lassen und damit sehr weit ausgestaltet.[44] Daher ist es auch möglich, über diese Norm Handlungen zu erfassen, die denen spezifischerer Grundrechte ähnlich sind, jedoch nicht in deren Schutzbereich fallen.[45]

Zur Formulierung eines Schutzbereichs für Online-Demonstrationen lassen sich die für eine Versammlung – man könnte auch sagen „herkömmliche Demonstration“ – geltenden Regeln ins Internet übertragen. Hier bietet sich ein Vergleich mit der Rechtsprechung des Bundesverfassungsgerichtes zu den sogenannten Sitzblockaden an. Auch bei einer Sitzblockade geht es, genau wie bei dem als Online-Demonstration bezeichneten Vorgehen, darum, auf eine Meinung hin-

[32] Vgl. AG Frankfurt a.M., Urt. v. 1.7.2005 – 991 Ds 6100 Js 226314/01 = MMR 2005, 863 (866).

[33] So auch m.w.N. *Kraft/Meister*, MMR 2003, 366 (367); vgl. auch *Pieroth/Schlink*, Grundrechte, Staatsrecht II, 27. Aufl. 2011, Rn. 689.

[34] Vgl. *Pieroth/Schlink* (Fn. 33), Rn. 695.

[35] Art. 5 Abs. 1 GG: „Jeder hat das Recht, seine Meinung in Wort, Schrift und Bild frei zu äußern und zu verbreiten und sich aus allgemein zugänglichen Quellen ungehindert zu unterrichten. […].“

[36] Art. 5 Abs. 1 GG schützt zwar auch die Kontaktaufnahme des einzelnen mit anderen Menschen im Sinne eines Kommunikationsgrundrechtes, allerdings wird dieser Schutz nicht auf die Gemeinschaftsbezogenheit des Menschen ausgeweitet, wie dies etwa bei der Versammlungsfreiheit aus Art. 8 GG der Fall ist. Insbesondere enthält Art. 5 Abs. 1 GG nicht das Recht von „jedermann“ oder von einer bestimmten Person gehört zu werden, vgl. *Herzog*, in: Maunz/Dürig, Grundgesetz, Kommentar, 30. Lfg., Stand: Dezember 1992, Art. 5 Rn. 57 bis 60. Fraglich ist außerdem, inwieweit das Blockieren einer Internetseite als „Meinungsäußerung“ angesehen werden kann. Vielmehr ist hier wohl von einem bloßen Hinweis auf eine Meinung auszugehen.

[37] Art. 11 Abs. 1 EMRK: „Jede Person hat das Recht, sich frei und friedlich mit anderen zu versammeln und sich frei mit anderen zusammenzuschließen; […].“

[38] Vgl. *Meyer-Ladewig*, Europäische Menschenrechtskonvention, Kommentar, 3. Aufl. 2011, Art. 11 Rn. 6.

[39] Art. 10 Abs. 1 EMRK: „Jede Person hat das Recht auf freie Meinungsäußerung. […].“

[40] Vgl. *Meyer-Ladewig* (Fn. 38), Art. 10 Rn. 5.

[41] Vgl. EGMR, Urt. v. 25.11.1999 – 25594/94 (Hashman u. Harrup v. Vereinigtes Königreich), RUDH 1999, 331, Rn. 28 = Slg. 99-VIII; der EGMR sah die Störung einer Fuchsjagd durch Hornblasen und Lärmen als legitimes Mittel des Ausdrucks von Protest gegen die Veranstaltung von Fuchsjagden an.

[42] Siehe statt vieler *Payandeh*, JuS 2009, 212 m.w.N. in Fn. 2.

[43] Art. 2 Abs. 1 GG: „Jeder hat das Recht auf die freie Entfaltung seiner Persönlichkeit, soweit er nicht die Rechte anderer verletzt und nicht gegen die verfassungsmäßige Ordnung oder das Sittengesetz verstößt.“

[44] Vgl. *Di Fabio*, in: Maunz/Dürig (Fn. 36), 39. Lfg, Stand: Juli 2001, Art. 2 Rn. 12.

[45] Vgl. *Di Fabio* (Fn. 44), Art. 2 Rn. 19, der ein solches Vorgehen als Schaffung von Rechtsklarheit im Hinblick auf den sehr weit gefassten Schutzbereich der Art. 2 Abs. 1 GG durch Fallgruppenbildung bewertet. Ferner ist auch die Ergänzung benannter Grundrechte durch Art. 2 Abs. 1 GG möglich, vgl. *Di Fabio* (Fn. 44), Art. 2 Rn. 36.

zuweisen und so die Kommunikationswirkung nach außen hin zu verstärken.[46] Eine Sitzblockade soll daher nur dann unter den Schutzbereich des Art. 8 GG fallen, wenn die bezweckte Beeinträchtigung der blockierten Einrichtung „nicht Selbstzweck [ist], sondern ein dem Kommunikationsanliegen untergeordnetes Mittel zur symbolischen Unterstützung ihres Protests und damit zur Verstärkung der kommunikativen Wirkung in der Öffentlichkeit“[47] darstellt. Für die Online-Demonstration bedeutet dies, dass die Blockade einer Webseite nicht einem bloßen Selbstzweck dienen darf. Nicht geschützt wäre dann z.B. ein Angriff durch die Hacker-Gruppierung Anonymus auf die Webseiten von Finanzdienstleistern wie PayPal oder Visa, um sich dafür zu „rächen“, dass diese Zahlungen an die Online-Enthüllungsplattform Wikileaks verweigerten, da es hier in erster Linie um eine Vergeltungsaktion und nicht um den Hinweis auf eine Meinung geht.

Eine „herkömmliche Demonstration“ und somit auch eine Sitzblockade genießt außerdem auch nur dann verfassungsrechtlichen Schutz, wenn diese friedlich und ohne Waffen stattfindet. Bei einer Sitzblockade ist dies jedenfalls dann der Fall, wenn die Teilnehmer sich passiv verhalten.[48] Eine Entsprechung hierfür ließe sich auf virtueller Ebene in dem Erfordernis „ohne Verwendung von anderer Software als dem Internetbrowser“ formulieren. Sowohl eine Online-Demonstration unter Verwendung von anderer Software als dem Internetbrowser als auch eine Demonstration mittels DDoS-Attacke wären daher bereits aus dem Schutzbereich ausgenommen. Dies würde auch gewährleisten, dass Online-Demonstrationen nur dann Erfolg haben, wenn sich tatsächlich eine sehr große Zahl an Menschen an ihnen beteiligt, was für die Relevanz des gemeinsamen Anliegens spricht. In diesem Fall ist die Online-Demonstration Ausdruck der in Art. 2 Abs. 1 geschützten allgemeinen Handlungsfreiheit.

V. Fazit

Auch wenn die vom deutschen Gesetzgeber getroffenen Regelungen der Umsetzung der Convention on Cybercrime dienen, ist nicht davon auszugehen, dass es den Unterzeichnern des Übereinkommens darum ging, das Lenken der Aufmerksamkeit auf legitime politische und gesellschaftliche Anliegen mittels moderner Kommunikationsmöglichkeiten mit Strafe zu bedrohen. Insoweit erscheint das Ergebnis zutreffend, dass eine Online-Demonstration, die ohne technische Hilfsmittel durchgeführt wird, straffrei bleibt. Die deutsche Umsetzung der europäischen Vorgaben schließt effektiv Strafbarkeitslücken, die im Hinblick auf Angriffe auf Webseiten mittels DDoS-Attacken bestanden. Das Beispiel der Online-Demonstration zeigt jedoch, dass es im Internet schwer ist, rechtmäßiges Verhalten von kriminellen Handlungen zu unterscheiden. Hierzu tragen nicht zuletzt die sehr weit gefassten Straftatbestände und fehlende verfassungsrechtliche Grundlagen über den Umgang mit dem nicht mehr ganz so neuen Medium „Internet“ bei.[49]

Umso wichtiger ist es, sich intensiv mit den vorhandenen Rechtsgrundlagen auseinanderzusetzen, um herauszufinden, wo tatsächlich Nachbesserungsbedarf besteht. Hierbei ist auf neue gesellschaftliche Entwicklungen einzugehen. Eine Demonstration im Internet kann ganz anders aussehen als eine Demonstration in der realen Welt. Es muss sich nicht immer um eine Versammlung handeln. Das Internet ist kein rechtsfreier Raum.[50] Dies darf jedoch nicht nur für den Bürger gelten, der sich an Vorschriften zu halten hat, sondern muss auch für den Gesetzgeber gelten, dem ebenfalls verfassungsrechtliche Grenzen gesetzt sein müssen.[51] Warum sollte also nicht auch das Recht zu demonstrieren dort geschützt sein, wo sich der „moderne“ Mensch am häufigsten „versammelt“: im Internet?

[46] Vgl. für die Einordnung der Sitzblockade in den Schutzbereich der Versammlungsfreiheit nur *Rusteberg*, NJW 2011, 2999 (3001); andere Auffassung: *Depenheuer*, in: Maunz/Dürig (Fn. 36), 48. Lfg, Stand: November 2006, Art. 8 Rn. 66, der die Sitzblockade von vornherein aus dem Schutzbereich ausschließen will, da es sich nach seiner Auffassung lediglich um „unmittelbaren Zwang durch Personenmehrheiten“ handele, nicht jedoch um eine Versammlung.

[47] So BVerfG NJW 2002, 1031 (1032).

[48] Vgl. etwa BVerfGE 73, 206 (249); 87, 399 (406).

[49] So auch *Medosch* (Fn. 5), S. 261 (S. 303); vgl. auch BT-Drs. 16/5449, S. 6, wo zumindest auf bestehende Probleme im Zusammenhang mit Grundrechten und Online-Demonstrationen und DDoS-Attacken hingewiesen wurde.

[50] Zur inhaltlichen Bedeutung dieses Satzes vgl. *Lischka*, http://www.spiegel.de/netzwelt/web/0,1518,632277,00.html (zuletzt aufgerufen am 30.3.2012).

[51] So auch *Bizer*, in: Schulzki-Haddouti (Fn. 5), S. 21. Dieser weist auch auf das Problem hin, dass die Grundrechte eines Staates auch nur dessen Staatsgewalt binden. Gemindert wird dieses Problem jedoch im Geltungsbereich der EMRK, vgl. hierzu *Bizer* (a.a.O.), S. 21 (S. 22).

Debit Card Fraud: Strafrechtliche Aspekte des sog. „Skimmings“

Von Wiss. Mitarbeiter und Mediator (CVM) **Alexander Seidl**, Passau*

Die Zahl der „Angriffe auf Geldautomaten“ bewegt sich seit Jahren auf hohem Niveau. 2009 wurden laut Bundeskriminalamt (BKA) in Deutschland über 100.000 Menschen Opfer sog. Skimming-Attacken,[1] wobei ein Schaden von etwa 40 Millionen Euro entstand. Ihre bisherige Spitze erreichte die Zahl der Skimming-Attacken mit 190.000 betroffenen Kunden und einem Schaden von schätzungsweise 60 Millionen Euro im Jahr 2010.[2] Für das Jahr 2011 war ein Rückgang im Vergleich zum Vorjahr von rund 50 Prozent festzustellen.[3] Dennoch dürfte der Kampf gegen das Skimming noch nicht endgültig gewonnen sein. Es ist zu befürchten, dass die rückläufigen Zahlen auf eine Phase der Umorganisation der kriminellen Banden zurückzuführen sind.

Im Folgenden soll die Strafbarkeit dieser Form der Geldautomatenkriminalität nach dem StGB näher beleuchtet werden.[4] Insbesondere werden die neueren Entscheidungen der verschiedenen Senate des BGH zum Versuchsbeginn bei der Fälschung von Zahlungskarten mit Garantiefunktion gem. §§ 152b, 22 StGB untersucht.

I. Einführung – Was ist Skimming?

Skimming meint das Abschöpfen von Daten aus einer Debit- (früher: ec-Karte) oder Kreditkarte (zusammengefasst als Zahlungskarten bezeichnet) durch Auslesen und Kopieren des Inhalts des auf der Karte befindlichen Magnetstreifens, um die Informationen anschließend auf einen Kartenrohling zu übertragen und diesen in der Folge gemeinsam mit der ebenfalls ausspionierten zugehörigen persönlichen Identifikationsnummer (PIN) für Geldabhebungen im Ausland zu missbrauchen. Namengebend für diese Form des „Zahlungskartenbetrugs“ sind die dabei zum Einsatz kommenden Kartenlesegeräte, die sog. Skimmer.[5]

Skimming-Angriffe treten in unterschiedlichen Erscheinungsformen auf. So wurden zuletzt nicht nur Geldautomaten mit zusätzlichen Kartenlesegeräten ausgestattet, auch an SB-Tankstellen und Bahnkartenautomaten wurden die Bank- bzw. Kreditkartenterminals auf diese Weise manipuliert.[6] Beim „klassischen“ Fall des Skimmings – auf den sich die folgenden Darstellungen beschränken –, also dem Ausspähen von Zahlungskartendaten an Geldautomaten, wird von den Tätern zunächst ein Miniatur-Kartenleser von außen vor dem Leseschlitz des Geldautomaten befestigt oder aber bereits am Türöffner im Eingangsbereich des betroffenen Kreditinstituts angebracht.[7] Die Zahlungskarte des Kunden wird bei der Benutzung von Automat oder Türöffner unbemerkt durch das zusätzliche Lesegerät gezogen, wobei es zum Auslesen des Inhalts des Magnetstreifens kommt. Für das ungeschulte Auge ist die Manipulation kaum zu erkennen, da der Aufsatz von den Tätern in Farbe und Form dem jeweiligen Geldautomaten bzw. Türöffner angepasst wird. Die abgegriffenen Daten werden gespeichert und nach dem Abbau der Skimming-Vorrichtung auf einen PC übertragen oder gleich per Funk an die Täter übermittelt.[8]

Das Ausspähen der PIN des Karteninhabers kann ebenfalls auf unterschiedliche Weise erfolgen. Meist kommt eine oberhalb des Tastaturfeldes angebrachte Videoleiste zum Einsatz, hinter der sich eine kleine Kamera verbirgt, mittels derer die PIN-Eingabe aufgezeichnet wird. Alternativ verwenden die Täter auch Nachbildungen der Geldautomatentastaturen, die auf die echte Tastatur geklebt werden. Bei Eingabe der PIN werden die Anschläge an die Originaltastatur durchgereicht und dabei protokolliert, während gleichzeitig der Geldautomat störungsfrei bedient wird. Das Ausspähen kann aber auch schlicht durch „Über-die-Schulter-Schauen“ eines Täters erfolgen.

Nach erfolgreicher Kartendaten- und PIN-Beschaffung stellen die Skimming-Täter unter Verwendung von leeren Kartenrohlingen (sog. „White-Plastics“) Dubletten her, mit denen sie nunmehr Abhebungen vornehmen können. Diese erfolgen dabei stets im – in den letzten Jahren vor allem europäischen – Ausland, da Zahlungskarten deutscher Ausgabestellen mit einem besonderen Schutzmechanismus, dem sog. moduliert maschinenfähigen Merkmal (MM-Merkmal) ausgestattet sind, das Abhebungen unter Zuhilfenahme billiger Datenträger unmöglich macht. Seit der zweiten Jahreshälfte 2010 erfolgen die missbräuchlichen Karteneinsätze zunehmend im außereuropäischen Bereich. Grund dafür ist, dass seit Anfang 2011 Transaktionen europäischer Debitkarten im SEPA-Raum EMV-Chip-basiert[9] abgerechnet werden.[10] Da

---

* *Alexander Seidl* ist Assessor und wissenschaftlicher Mitarbeiter am Lehrstuhl für Öffentliches Recht, Sicherheitsrecht und Internetrecht (Prof. *Dr. Dirk Heckmann*) an der Universität Passau. Der *Autor* dankt Herrn KHK *Stephan Ruf*, LKA Bayern, für technische Erläuterungen und Frau StAin *Ulrike Hackler*, Staatsanwaltschaft Traunstein, für die Unterstützung bei der Ausarbeitung des Beitrags.

[1] http://wirtschaft.t-online.de/bka-2009-ueber-100-000-opfer-von-skimming/id_41434792/index (16.8.2012).

[2] Vgl. BKA, Zahlungskartenkriminalität, Bundeslagebild 2010, S. 5.

[3] S. www.ftd.de/unternehmen/finanzdienstleister/:skimming-erfolgreicher-kampf-gegen-datenklau-am-geldautomaten/60146294.html (16.8.2012).

[4] Zur Strafbarkeit auch nach dem Nebenstrafrecht vgl. *Seidl/Fuchs*, HRRS 2011, 265.

[5] *Kochheim*, Skimming – Hintergründe und Strafrecht, Fassung 2.21, Stand: April 2011, S. 4, im Internet abrufbar unter: http://www.kochheim.de/cf/doc/Kochheim-Skimming-2010.pdf (16.8.2012).

[6] BKA (Fn. 2), S. 8 f.

[7] Letztere Variante war allerdings im Jahr 2010 stark rückläufig und machte nur noch 2 % der Fälle aus.

[8] *Bachfeld*, c't 25/2007, 76 (77).

[9] EMV steht für „Europay International (heute MasterCard Europe), MasterCard und Visa“ und ist ein internationaler technischer Standard zur Abwicklung von Chipkartenzahlungen. Vertiefend hierzu *Seidl/Fuchs*, HRRS 2011, 265 (274).

[10] Eine kriminologische Betrachtung des Skimmings findet sich bei *Bachmann/Goeck*, Neue Kriminalpolitik 2011, 153.

viele Banken im Hinblick auf diese Umstellung die Geräte bereits sukzessive umgerüstet haben, wichen die Täter zunehmend in die Nicht-Chip-Länder aus, insbesondere in die Staaten Südafrika, Kenia, USA, Kanada sowie die Dominikanische Republik.[11]

II. Strafrechtliche Würdigung

Um eine strafrechtliche Würdigung des Skimmings vornehmen zu können, ist der Gesamtvorgang „Skimming" zunächst in folgende Tatkomplexe aufzuteilen:

- Herstellung bzw. Verschaffen der Skimming-Ausrüstung,
- Ausspähen von Magnetstreifen und PIN,
- Herstellung der Dubletten,
- Einsatz der Dubletten,
- Verteilung der Beute.

Ihre strafrechtliche Bewertung soll zum besseren Verständnis hier jedoch nicht chronologisch vorgenommen werden.

Dass jedenfalls der Einsatz der Dubletten stets im Ausland erfolgt, ist für die Anwendbarkeit des deutschen Strafrechts unerheblich.[12] Da nämlich für sämtliche Tatbeteiligte Mittäterschaft anzunehmen sein wird,[13] ist aufgrund der hierbei erfolgenden gegenseitigen Anrechnung der Tatbeiträge an jedem Ort, an dem einer der Mittäter gehandelt hat, mithin auch in Deutschland, ein Tatort i.S.d. § 9 Abs. 1 StGB begründet.[14] Damit findet das deutsche Strafrecht gemäß § 3 StGB Anwendung.[15]

1. Strafbarkeit des Ausspähens von Magnetstreifen und PIN

a) Ausspähen der Magnetstreifeninformationen

aa) Strafbarkeit nach § 202a StGB

Das Auslesen des auf der EC-Karte befindlichen Magnetstreifens erfüllt den Tatbestand des § 202a StGB nicht. Zwar handelt es sich bei den auf dem Magnetstreifen einer EC-Karte gespeicherten Informationen, insbesondere Kontonummer und Bankleitzahl, um nicht unmittelbar wahrnehmbar gespeicherte Daten, da sie in einer für eine Datenverarbeitungsanlage erkennbaren Form codiert sind und erst nach einer Transformation mittels technischem Hilfsmittel wahrgenommen werden können, also mithin Daten i.S.d. § 202a StGB.

Die Daten sind auch „nicht für den Täter bestimmt". Für den Täter bestimmt sind sie nur dann, wenn sie nach dem Willen desjenigen, der zum Zeitpunkt der Tat die formelle Verfügungsberechtigung über die Daten innehat, dem Täter zur Verfügung stehen sollen.[16] Maßgeblich ist bei Bank- und Kreditkarten der Wille des kartenausgebenden Kreditinstituts.[17] Dieses wird mit dem Ausspähen der Magnetstreifeninformationen nicht einverstanden sein.

Eine Strafbarkeit nach § 202a Abs. 1 StGB scheitert jedoch am fehlenden Vorliegen einer besonderen Zugangssicherung, zumindest am mangelnden Überwinden einer solchen. Eine besondere Zugangssicherung liegt nur dann vor, wenn Vorkehrungen getroffen sind, um den Zugriff auf die Daten auszuschließen oder wenigstens nicht unerheblich zu erschweren. Die Zugangssicherung kann dabei sowohl durch mechanische (z.B. Schlösser, Versiegelungen) als auch durch technische, insbesondere systemimmanente Vorkehrungen (z.B. Passwort, biometrische Erkennungsverfahren) erfolgen.[18] Weder die auf dem Magnetstreifen gespeicherte Kontonummer noch die Bankleitzahl werden jedoch durch derartige Schutzmechanismen gesichert. Insoweit scheitert eine Strafbarkeit nach § 202a Abs. 1 StGB also bereits am fehlenden Vorhandensein einer Zugangssicherung.[19] Doch selbst wenn sich auch verschlüsselte Daten auf dem Magnetstreifen befinden sollten,[20] würde der Tatbestand des § 202a Abs. 1 StGB nicht verwirklicht. Zwar wäre in diesem Fall das Vor-

[11] bka.de/nn_227456/SharedDocs/Downloads/DE/Publikationen/JahresberichteUndLagebilder/Zahlungskartenkriminalitaet/zahlungskartenkriminalitaetPraesentationInternationaleKonferenz,templateId=raw,property=publicationFile.pdf/zahlungskartenkriminalitaetPraesentationInternationaleKonferenz.pdf (16.8.2012).

[12] Ausf. hierzu vgl. *Seidl/Fuchs*, HRRS 2011, 265 (266).

[13] *Braun/Heidberg*, StrafRechtsReport 2010, 89 (93); vgl. auch *Bachmann/Goeck*, JR 2011, 425.

[14] *Eser*, in: Schönke/Schröder, Strafgesetzbuch, Kommentar, 28. Aufl. 2010, § 9 Rn. 10; *Rotsch*, in: Graf/Jäger/Wittig (Hrsg.), Wirtschafts- und Steuerstrafrecht, Kommentar, 2011, § 9 Rn. 13.

[15] Sollte eine Anwendbarkeit deutschen Strafrechts nach diesen Vorschriften ausnahmsweise nicht in Betracht kommen, kann sie sich aus § 6 StGB ergeben. Diese Vorschrift nennt Taten (u.a. § 152b und § 149 StGB, s. § 6 Nr. 7 StGB), die nach dem Weltrechtsprinzip ohne Rücksicht auf Tatort, Recht des Tatorts und Staatsangehörigkeit des Täters dem deutschen Strafrecht unterliegen.

[16] *Lenckner/Eisele*, in: Schönke/Schröder (Fn. 14), § 202a Rn. 6.

[17] Vgl. *Seidl/Fuchs*, HRRS 2011, 265 (267).

[18] Vgl. *Weidemann*, in: von Heintschel-Heinegg (Hrsg.), Beck'scher Online-Kommentar, Strafgesetzbuch, Stand: Juni 2012, § 202a Rn. 13.

[19] Dass die Daten magnetisch und damit nicht unmittelbar wahrnehmbar gespeichert sind, stellt keine besondere Sicherung gegen unberechtigten Zugang dar, sondern ist gem. § 202a Abs. 2 StGB vielmehr Voraussetzung dafür, dass es sich überhaupt um Daten i.S.d. Abs. 1 handelt. Daran zeigt sich, dass nicht schon die Art der Speicherung eine besondere Sicherung i.S.d. § 202a Abs. 1 StGB darstellt, sondern dass darüber hinaus Vorkehrungen getroffen sein müssen, die den unbefugten Zugriff auf Daten ausschließen oder zumindest erheblich erschweren, vgl. BGH, Beschl. v. 14.1.2010 – 4 StR 93/09 und BGH, Beschl. v. 6.7.2010 – 4 StR 555/09. So auch *Eisele*, CR 2011, 131 (132).

[20] Vgl. *Richter*, CR 1989, 303 (305); im Beschl. des BGH v. 18.3.2010 – 4 StR 555/09 wird die Frage, ob sich auf dem Magnetstreifen auch verschlüsselte Daten befinden, ausdrücklich offen gelassen. Laut LKA Bayern befinden sich auf dem Magnetstreifen keine verschlüsselten Daten.

liegen einer Zugangssicherung zu bejahen.[21] Beim bloßen Auslesen und Abspeichern der auf dem Magnetstreifen einer Zahlungskarte gespeicherten Daten würde diese jedoch nicht überwunden.[22] Ein Überwinden erfordert eine Vorgehensweise, durch die die jeweilige Zugangssicherung außer Kraft gesetzt oder umgangen wird.[23] Gerade daran würde es jedoch fehlen: Die verschlüsselten Daten würden nicht etwa entschlüsselt, sondern in verschlüsseltem Zustand gespeichert.[24]

bb) Strafbarkeit nach § 263a StGB

Auch eine Strafbarkeit wegen Computerbetrugs durch unbefugte Verwendung von Daten gem. § 263a Abs. 1 Var. 3 StGB scheidet aus.[25] Zwar erfasst § 263a Abs. 1 Var. 3 StGB – im Gegensatz zu den ersten beiden Tatvarianten – gerade die Fälle, in denen der Täter – wie beim Skimming – richtige Daten verwendet.[26] Es fehlt jedoch an der für die Verwirklichung des Tatbestands erforderlichen Beeinflussung des Ergebnisses eines Datenverarbeitungsvorgangs: Hierfür reicht eine Einflussnahme, die zu keinem abweichenden Ergebnis des Datenverarbeitungsvorgangs führt, nicht aus. Vielmehr muss diese ein Ergebnis hervorgerufen haben, das ohne die Einwirkung entweder überhaupt nicht oder mit anderem Inhalt entstanden wäre.[27] Dies ist hier jedoch gerade nicht der Fall. Nachdem die Zahlungskarte das zusätzlich angebrachte Kartenlesegerät passiert hat und die auf dem Magnetstreifen enthaltenen Informationen mithilfe des Moduls ausgelesen wurden, läuft der im Geldautomaten stattfindende Datenverarbeitungsprozess ordnungsgemäß ab, es kommt also zu keiner Beeinflussung seines Ergebnisses.

cc)Strafbarkeit nach § 303b StGB

Nichts anderes gilt hinsichtlich einer Strafbarkeit gem. § 303b StGB mangels erheblicher Störung einer Datenverarbeitung. Die Datenverarbeitung ist dann erheblich gestört, wenn ihr reibungsloser Ablauf beeinträchtigt wird.[28] Beim Auslesen der Magnetkartendaten durch das zusätzlich angebrachte Kartenlesegerät wird der Ablauf der Datenverarbeitung im Geldautomaten aber gerade nicht beeinträchtigt. Die Datenverarbeitung läuft vielmehr ordnungsgemäß ab.

dd) Strafbarkeit nach § 303a StGB

Auch eine Strafbarkeit nach § 303a Abs. 1 StGB wegen Veränderns der auf dem Magnetstreifen enthaltenen Daten der Originalbankkarte scheidet aus. Dieses ist nämlich nur dann gegeben, wenn eine inhaltliche Umgestaltung der Daten erfolgt und sie deshalb einen anderen Informationsgehalt aufweisen. Das bloße unbefugte Kopieren von Daten wird dagegen nicht vom Tatbestand erfasst.[29]

ee) Strafbarkeit nach § 202b StGB

Eine Strafbarkeit nach § 202b StGB scheitert daran, dass der Skimming-Täter die auf dem Magnetstreifen enthaltenen Informationen – bei denen es sich um nicht für ihn bestimmte Daten i.S.d. § 202b StGB handelt – nicht aus einer nicht öffentlichen Datenübermittlung abfängt.[30] Eine nicht öffentliche Datenübermittlung findet beim Abhebungsvorgang zwar statt, die Magnetstreifendaten werden aber noch im Vorfeld des zwischen Bankkunde und Kreditinstitut erfolgenden Datenübertragungsvorgangs, der erst mit Einlesen der Zahlungskarte durch den Originalkartenleser beginnt, vom Täter abgeschöpft. Im Zeitpunkt des Abschöpfens der Informationen stammen die Daten also gerade nicht aus einer nicht öffentlichen Datenübertragung. Vielmehr wird eine eigene Datenübertragung durch den Täter initiiert, deren Adressat er selbst ist.[31]

ff) Strafbarkeit nach §§ 269 Abs. 1 Alt. 1, 25 Abs. 1 Alt. 2 StGB

Indem der unwissende Bankkunde seine EC-Karte in den am Bankautomaten angebrachten Skimming-Aufsatz einführt, macht sich der Täter jedoch wegen Fälschung beweiserheblicher Daten in mittelbarer Täterschaft strafbar. Der vorsatzlos handelnde Bankkunde erfüllt die Tatbestandsvoraussetzungen

[21] Nach h.M. stellen auch Datenverschlüsselungen Sicherungen i.S.v. § 202a StGB dar, vgl. *Fischer*, Strafgesetzbuch und Nebengesetze, Kommentar, 59. Aufl. 2012, § 202a Rn. 9a.

[22] BGH, Beschl. v. 14.1.2010 – 4 StR 93/09, BGH, Beschl. v. 18.3.2010 – 4 StR 555/09 und BGH, Beschl. v. 6.7.2010 – 4 StR 555/09; *Seidl/Fuchs*, jurisPR-ITR 9/2010 Anm. 6; i.E. auch *Tyszkiewicz*, HRRS 2010, 207 (209), die jedoch trotz Bejahung des Vorhandenseins verschlüsselter Daten weniger auf das Überwinden, als vielmehr auf das Fehlen einer ausreichenden Zugangssicherung abstellt; a.A. dagegen *Braun/Heidberg*, StrafRechtsReport 2010, 89 (91), die ohne nähere Erläuterung das Vorhandensein von Schutzvorkehrungen und deren Überwindung bejahen.

[23] *Weidemann* (Fn. 18), § 202a Rn. 17; Eine Datenverschlüsselung schützt nur vor der Erfassung des Bedeutungsgehalts (kryptierter) Daten, nicht aber vor dem bloßen Auslesen und Abspeichern der verschlüsselten Daten auf einem Datenträger des Täters, vgl. BGH, Beschl. v. 18.3.2010 – 4 StR 555/09.

[24] Vgl. auch BGH, Beschl. v. 14.1.2010 – 4 StR 93/09, und BGH, Beschl. v. 18.3.2010 – 4 StR 555/09; a.A. dagegen noch BGH, Urt. v. 10.5.2005 – 3 StR 425/04, die jedoch auf Anfragebeschluss aufgegeben wurde, vgl. BGH, Beschl. v. 6.7.2010 – 4 StR 555/09.

[25] Im Ergebnis ebenso, aber mit anderer Begründung *Eisele*, CR 2011, 131 (134).

[26] „Verwenden“ meint in diesem Zusammenhang die Einführung der Daten in den Datenverarbeitungsprozess, wobei über die Fälle der eigenhändigen Eingabe hinaus auch diejenigen erfasst sind, in denen der Täter sich – wie beim Skimming – für den unmittelbaren Akt der Eingabe einer anderen Person bedient, vgl. *Wohlers*, in: Joecks/Miebach (Hrsg.), Münchener Kommentar zum Strafgesetzbuch, Bd. 4, 2007, § 263a Rn. 29.

[27] *Wohlers* (Fn. 26), § 263a Rn. 17.

[28] *Hilgendorf*, JuS 1996, 1082 (1083).

[29] *Weidemann* (Fn. 18), § 303a Rn. 13.

[30] Ebenso *Eisele*, CR 2011, 131 (132).

[31] Vgl. zur ähnlichen Problematik beim Phishing *Seidl/Fuchs*, HRRS 2010, 85 (86).

des § 269 Abs. 1 Alt. 1 StGB, denn er speichert beweiserhebliche Daten so, dass bei ihrer Wahrnehmung eine unechte Urkunde vorliegen würde. Daten sind beweiserheblich, wenn sie dazu bestimmt sind, bei einer Verarbeitung im Rechtsverkehr als Beweisdaten für rechtlich erhebliche Tatsachen benutzt zu werden.[32] Bei Codekartendaten im Bankautomatenverkehr ist dies der Fall.[33] Ein Speichern der Daten ist gegeben, wenn sie auf einem Datenträger erfasst oder aufbewahrt oder auf ihn kopiert bzw. aufgenommen werden. Durch das Speichern muss ein Falsifikat entstehen, das – von der Wahrnehmbarkeit abgesehen – die Merkmale einer falschen Urkunde aufweist.[34] Die auf dem Magnetstreifen einer EC-Karte gespeicherten Daten beinhalten eine Garantieerklärung der Ausstellerbank zugunsten des berechtigten Karteninhabers. Wer den Magnetstreifen einer solchen Karte kopiert, erzeugt den falschen Anschein einer weiteren Gedankenerklärung der Ausstellerbank und verwirklicht dadurch § 269 StGB.[35] Dieser vom Bankkunden unvorsätzlich herbeigeführte, strafrechtlich verbotene Erfolg wird vom Skimming-Täter vorsätzlich bewirkt, sodass ein klassischer Fall der mittelbaren Täterschaft vorliegt.[36] Der Skimming-Täter handelt darüber hinaus auch mit dem Willen, die erlangten Daten zur fälschlichen Beeinflussung einer Datenverarbeitung zu verwenden, welche gem. § 270 StGB der Täuschung im Rechtsverkehr gleichsteht. Regelmäßig wird zudem der Qualifikationstatbestand des § 267 Abs. 4 StGB, auf den § 269 Abs. 3 StGB verweist und der eine verschärfte Sanktionierung für die gewerbsmäßige Begehung als Mitglied einer Bande, die sich zur fortgesetzten Begehung von Straftaten nach den §§ 263-264 oder 267-269 StGB verbunden hat, vorsieht, verwirklicht sein.[37]

gg) Strafbarkeit nach § 152b Abs. 5 i.V.m. § 149 Abs. 1 Nr. 1 StGB

Ferner ist auch der Tatbestand der Vorbereitung der Fälschung von Zahlungskarten mit Garantiefunktion gem. § 152b Abs. 5 i.V.m. § 149 Abs. 1 Nr. 1 StGB zu bejahen.[38] § 149 Abs. 1 Nr. 1 StGB beschreibt bestimmte Vorrichtungen zur Herstellung von Falsifikaten, die ihrer Art nach zur Begehung der Tat geeignet sein müssen. Neben den explizit erwähnten fallen darunter auch solche, denen schon ihrer Art nach eine spezifische Verwendbarkeit zur Ausführung von Fälschungen innewohnt.[39] Erforderlich ist auch, dass diese „ähnlichen Vorrichtungen" gebrauchsfertig und zum unmittelbaren Einsatz im eigentlichen Fälschungsvorgang geeignet sind.[40] Seit der Aufnahme des Begriffs „Computerprogramme" in den Tatbestand des § 149 Abs. 1 Nr. 1 StGB,[41] mit dem zum Ausdruck kommt, dass sich der Anwendungsbereich der Vorschrift nicht prinzipiell auf körperliche Tatobjekte beschränkt, steht darüber hinaus fest, dass auch nicht körperliche Vorlagen der Vervielfältigungstechnik als „ähnliche Vorrichtungen" von der Vorschrift erfasst werden.[42] Damit fallen auch die mithilfe des Skimmers ausgelesenen Datensätze, die im Anschluss auf die Magnetstreifen der Kartendubletten kopiert werden können und dabei unmittelbar zur Entstehung unechter Zahlungskarten mit Garantiefunktion führen, unter diesen Begriff.[43]

hh) Strafbarkeit nach §§ 152b, 22 StGB in Abgrenzung zu §§ 152b, 30 Abs. 2 Var. 3 StGB

Mehrfach Gegenstand höchstrichterlicher Entscheidungen war zuletzt die Frage, wann – in Fällen, in denen die Manipulationen am Geldautomaten vor Tatvollendung durch Sicherstellung der Skimming-Anbauten verhindert wurde – ein unmittelbares Ansetzen der Täter zum Fälschen von Zahlungskarten mit Garantiefunktion zu bejahen ist.[44]

Nach den allgemeinen Grundsätzen zur Abgrenzung von Vorbereitungshandlungen zum strafbaren Versuch liegt ein unmittelbares Ansetzen nur bei solchen Handlungen vor, die nach Tätervorstellung in ungestörtem Fortgang unmittelbar zur Tatbestandserfüllung führen oder mit ihr in einem unmittelbaren räumlichen und zeitlichen Zusammenhang stehen. Dies ist insbesondere der Fall, wenn der Täter subjektiv die

[32] *Fischer* (Fn. 21), § 269 Rn. 4.
[33] Vgl. *Lackner/Kühl*, Strafgesetzbuch, Kommentar, 27. Aufl. 2011, § 269 Rn. 2.
[34] *Fischer* (Fn. 21), § 269 Rn. 7.
[35] *Hoyer*, in: Rudolphi u.a. (Hrsg.), Systematischer Kommentar zum Strafgesetzbuch, 131. Lfg., Stand: März 2012, § 269 Rn. 16.
[36] *Joecks*, in: Joecks/Miebach (Hrsg.), Münchener Kommentar zum Strafgesetzbuch, Bd. 1, 2. Aufl. 2011, § 25 Rn. 53 ff.
[37] Auf Konkurrenzebene dürfte § 269 StGB jedoch von § 152b StGB verdrängt werden, vgl. *Erb*, in: Joecks/Miebach (Fn. 26), § 269 Rn. 41.
[38] § 149 StGB tritt hinter § 152b StGB zurück, sobald dort ein strafbarer Versuch begangen wird. Ob § 149 StGB auch hinter die Verabredung der gewerbs- und bandenmäßigen Fälschung von Zahlungskarten mit Garantiefunktion gem. §§ 152b, 30 Abs. 2 Var. 3 StGB zurücktritt, ist umstritten. Vom BGH wurde diese Frage zuletzt immer offen gelassen, vgl. bspw. BGH, Beschl. v. 11.8.2011 – 2 StR 91/11, oder BGH, Urt. v. 17.2.2011 – 3 StR 419/10. Teils wird vertreten, § 149 StGB werde wegen seiner geringeren Strafandrohung (Freiheitsstrafe bis zu fünf Jahre) vom Tatbestand des §§ 152b, 30 Abs. 2 Var. 3 StGB, der einen Strafrahmen von sechs Monaten bis zu elf Jahren und drei Monaten eröffnet, verdrängt (so BGH, Urt. v. 13.1.2010 – 2 StR 439/09). Nach a.A. soll Tateinheit zwischen den beiden Delikten möglich sein, da dem Vergehen nach § 152b Abs. 5 i.V.m. § 149 Abs. 1 Nr. 1 gegenüber der Verbrechensverabredung nach §§ 152b, 30 Abs. 2 Var. 3 StGB ein eigener Unrechtsgehalt zukomme, vgl. *Fischer* (Fn. 21), § 149 Rn. 12; *Hoyer* (Fn. 35), § 30 Rn. 60.
[39] *Erb* (Fn. 38), § 149 Rn. 3.
[40] *Erb* (Fn. 38), § 149 Rn. 3.
[41] Gesetz v. 22.8.2002 = BGBl. I 2002, S. 3387.
[42] *Erb* (Fn. 38), § 152a Rn. 13.
[43] Vgl. *Erb* (Fn. 38), § 152a Rn. 13; *Stein*, in: Rudolphi u.a. (Hrsg.), 67. Lfg., Stand: Oktober 2006, § 149 Rn. 2; *Puppe*, in: Kindhäuser/Neumann/Paeffgen (Hrsg.), Nomos Kommentar, Strafgesetzbuch, Bd. 2, 3. Aufl. 2010, § 149 Rn. 9; vgl. auch *Eisele*, CR 2011, 131 (134).
[44] Vgl. hierzu schon *Seidl*, jurisAZO-ITR 19/2011 Anm. 2.

Schwelle zum „jetzt geht es los“ überschreitet, es eines weiteren Willensimpulses nicht mehr bedarf und er objektiv zur tatbestandsmäßigen Angriffshandlung ansetzt, sodass sein Tun ohne Zwischenakte in die Erfüllung des Tatbestandes übergeht.[45]

Unter Heranziehung dieser Grundsätze haben sowohl der *2.* und der *3.* als auch der *5. Strafsenat* des BGH entschieden, dass ein unmittelbares Ansetzen frühestens dann anzunehmen sei, wenn der Täter mit der eigentlichen Fälschungshandlung, also dem Herstellen der falschen Zahlungskarte, beginne.[46] In den übrigen Fällen liege lediglich die Verabredung der gewerbs- und bandenmäßigen Fälschung von Zahlungskarten mit Garantiefunktion gem. §§ 152b, 30 Abs. 2 Var. 3 StGB vor.

Mit Urteil vom 27.1.2011 entschied der *4. Strafsenat* des BGH,[47] dass spätestens die Weitergabe der ausgelesenen Kartendaten das unmittelbare Ansetzen zur Tatbestandsverwirklichung i.S.d. § 22 StGB darstellt, wenn es der Täter im Rahmen eines Tatplans zur Fälschung von Zahlungskarten mit Garantiefunktion, bei dem die einzelnen Tatbeiträge eng ineinander greifen und schnell aufeinander folgen, übernommen hat, die Daten von Zahlungskarten mittels Skimmings auszuspähen, da dem Täter auf Grund des Tatplans bewusst ist, durch die Weitergabe einen gleichsam automatisierten Ablauf in Gang zu setzen. Der *4. Strafsenat* stellte dabei auf das enge Ineinandergreifen der einzelnen, einem festen Ablaufplan folgenden Tatbeiträge und auf den nach dem Tatplan engen zeitlichen Zusammenhang zwischen dem Tatbeitrag der Angeklagten und dem Beschreiben der Kartenrohlinge durch andere Bandenmitglieder als eigentliche Fälschungshandlung ab. Die dem Auslesen der Daten und der Weitergabe der Speichermedien nachfolgenden Arbeitsschritte bis hin zu den – der Tatbestandsverwirklichung des § 152b StGB nachgelagerten – Abhebungen an den Geldautomaten mussten vonstattengehen, bevor die Manipulation an den Lesegeräten in den Bankfilialen bemerkt wurde. Die schnelle zeitliche Abfolge wurde durch das eingespielte System von Tatbeiträgen gewährleistet, bei dem den im Ausland sitzenden Mittätern die einzelnen Datenübersendungen jeweils avisiert wurden. Diese wussten dadurch bereits im Voraus, dass die Erbringung ihres eigenen Tatbeitrags unmittelbar bevorstand. Es bedurfte mithin keines neuen Willensimpulses bei einem der durch die Bandenabrede verbundenen Mittäter mehr, sondern die Angeklagten setzten mit der Weitergabe der Daten – was ihnen bewusst war – gleichsam einen automatisierten Ablauf in Gang, sodass auch unter dem Gesichtspunkt der konkreten nahen Rechtsgutsgefährdung die Annahme eines unmittelbaren Ansetzens geboten sei. Dass dem Beschreiben der Kartenrohlinge die Auswertung der Speichermedien durch Abgleich von Videoaufzeichnungen und ausgelesenen Kartendaten und die Übersendung der Daten ins Ausland vorausgingen, stellt – nach Ansicht des BGH – bei der gebotenen wertenden Betrachtung keine diese Annahme hindernden Zwischenschritte dar.[48]

Die – nur auf den ersten Blick widersprüchliche – Rechtsprechung der verschiedenen BGH-*Senate* baut konsequent und widerspruchsfrei aufeinander auf.[49] Der *2.*, *3.* und *5. Strafsenat* beziehen sich zu Recht auf die von der Rechtsprechung entwickelten allgemeinen Grundsätze zur Abgrenzung von Vorbereitungshandlungen zum strafbaren Versuch. Deshalb ist auch nach diesen Entscheidungen das Beginnen mit der Fälschungshandlung als Beginnen im Sinne der allgemeinen Definition des unmittelbaren Ansetzens zu verstehen; hiervon sind auch vorgelagerte Handlungsakte umfasst, sofern diese nach der Tätervorstellung in ungestörtem Fortgang unmittelbar zur Tatbestandserfüllung führen oder mit ihr in einem unmittelbaren räumlichen und zeitlichen Zusammenhang stehen. Die drei Entscheidungen stehen mithin der Annahme einer Versuchstat im Fall des *4. Strafsenats* nicht entgegen, denn hier hätte die Weiterleitung der gewonnenen Daten nach der Vorstellung der Angeklagten bei ungestörtem Fortgang unmittelbar zur Tatbestandserfüllung führen sollen.[50]

Zum Versuch des Nachmachens setzt nach diesen Grundsätzen jedoch noch nicht an, wer die aufgezeichneten Datensätze nicht in seinen Besitz bringen und sie deshalb auch nicht an seine Mittäter, die die Herstellung der Kartendubletten vornehmen sollen, übermitteln kann. Das Anbringen einer Skimming-Apparatur an einem Geldautomaten in der Absicht, dadurch Daten zu erlangen, die später zur Herstellung der Kartendubletten verwendet werden sollen, ist als solche lediglich eine Vorbereitungshandlung. Die Tat stellt in diesem Verwirklichungsstadium daher lediglich eine Verabredung zu dem Verbrechen der banden- und gewerbsmäßigen Fälschung von Zahlungskarten dar, §§ 152b, 30 Abs. 2 Var. 3 StGB.[51]

b) Strafbarkeit des Ausspähens der PIN gem. § 202c Abs. 1 Nr. 1 i.V.m. § 202a Abs. 1 StGB

Hinsichtlich des Ausspähens der PIN macht sich der Täter nach § 202c Abs. 1 Nr. 1 i.V.m. § 202a Abs. 1 StGB strafbar, und zwar in der Form des Sichverschaffens eines Passworts. Unter einem Passwort versteht man jede Zeichenkombination, die im Rahmen einer Sicherungsabfrage den Zugang zu Daten ermöglicht, mithin nicht nur Wörter.[52] Ein Sichverschaffen ist gegeben, wenn der Täter in irgendeiner Form eigene Verfügungsgewalt am Tatobjekt begründet.[53] Unabhängig davon, ob das Ausspähen der PIN durch bloßes „Über-die-Schulter-Schauen“ oder mithilfe einer Tastatur-

[45] St. Rspr.; vgl. BGH, Urt. v. 13.1.2010 – 2 StR 439/09, und BGH, Urt. v. 7.11.2007 – 5 StR 371/07.

[46] BGH, Urt. v. 13.1.2010 – 2 StR 439/09; BGH, Beschl. v. 11.8.2011 – 2 StR 91/11; BGH, Urt. v. 17.2.2011 – 3 StR 419/10; BGH, Beschl. v. 14.9.2010 – 5 StR 336/10.

[47] BGH, Urt. v. 27.1.2011 – 4 StR 338/10.

[48] Zur Kritik an der Entscheidung des *4. Senats* vgl. *Bachmann/Goeck*, JR 2011, 425 (428).

[49] *Seidl*, jurisAZO-ITR 19/2011 Anm. 2.

[50] *Seidl*, jurisAZO-ITR 19/2011 Anm. 2.

[51] BGH, Urt. v. 13.1.2010 – 2 StR 439/09; BGH, Beschl. v. 14.9.2010 – 5 StR 336/10; BGH, Beschl. v. 11.8.2011 – 2 StR 91/11; *Bachmann/Goeck*, JR 2011, 425 (429).

[52] *Weidemann* (Fn. 18), § 202c Rn. 4.

[53] *Sternberg-Lieben*, in: Schönke/Schröder (Fn. 14), § 146 Rn. 15.

attrappe bzw. Videokamera erfolgt, sind diese beiden Voraussetzungen damit erfüllt.[54] Zu beachten ist, dass hinsichtlich der Frage, ob eine Straftat nach § 202a Abs. 1 StGB vorbereitet wird, nicht auf die auf dem Magnetstreifen befindlichen Daten abzustellen ist, da insoweit eine Strafbarkeit wegen Ausspähens von Daten – wie bereits erwähnt – ausscheidet. Vielmehr ist der Fokus auf die weiteren Kontodaten, insbesondere auf den Kontostand, zu richten. Auch bei diesem handelt es sich um ein Datum i.S.d. § 202a Abs. 2 StGB, welches zudem nur für den Kontoinhaber bestimmt und durch die vorgeschaltete PIN-Abfrage am Geldautomaten darüber hinaus besonders gesichert ist.[55] Mithilfe der erspähten PIN ist es dem Täter später in Kombination mit den manipulierten Kartendubletten nicht nur möglich, Geld abzuheben, sondern auch, den Kontostand am Geldautomaten einzusehen. Für ein Sichverschaffen des Zugangs reicht diese bloße Möglichkeit der Kenntnisnahme aus.[56]

2. Herstellung der Dubletten

a) Strafbarkeit nach § 152b Abs. 1 i.V.m. § 152a Abs. 1 Nr. 1 StGB

Die Herstellung der Kartendubletten erfüllt den Tatbestand des § 152b Abs. 1 i.V.m. § 152a Abs. 1 Nr. 1 StGB – Fälschung von Zahlungskarten mit Garantiefunktion – in der Form des „Nachmachens".[57] Bei herkömmlichen EC-Karten handelt es sich um Zahlungskarten mit Garantiefunktion i.S.d. § 152b Abs. 4 StGB.[58] Unter „nachmachen" versteht man sowohl Manipulationen an bereits verfälschten Tatobjekten, als auch das Herstellen von Totalfälschungen. Der Täter muss dabei zur Täuschung im Rechtsverkehr oder aber zur Ermöglichung einer solchen Täuschung handeln. Aufgrund dieses Erfordernisses wurde früher die Herstellung falsch codierter Magnetstreifen auf unbedruckten Karten – mangels deren Eignung zur Täuschung – für die Verwirklichung des Tatbestandes als nicht ausreichend angesehen. Heute stellt sich die Rechtslage im Hinblick auf § 270 StGB, der die Täuschung im Rechtsverkehr mit der fälschlichen Beeinflussung einer Datenverarbeitung im Rechtsverkehr gleichstellt, dagegen anders dar: Soweit es – wie bei Geldautomaten – für die Möglichkeit täuschungsgleicher Beeinflussung von Datenverarbeitungsanlagen allein auf die Codierung und die äußere Form der Karte, nicht aber auf Aufdrucke o.Ä. ankommt, reicht die Herstellung unbeschrifteter Plastikstücke mit codiertem Magnetstreifen zur Tatbestandsverwirklichung aus.[59]

Regelmäßig wird dabei auch die Qualifikation des § 152b Abs. 2 StGB wegen gewerbsmäßiger Begehung oder als Bandenmitglied begangener Straftaten nach § 152b Abs. 1 StGB erfüllt sein.

b) Strafbarkeit nach § 269 StGB

Schließlich erfüllt der Täter noch den Tatbestand des § 269 Abs. 1 StGB, und zwar in der Begehungsform des „Speicherns". Bei den ausgelesenen Magnetstreifeninformationen der Original-EC-Karte handelt es sich um beweiserhebliche Daten i.S.d. § 269 Abs. 1 StGB (s.o.). Der Täter speichert diese Daten auch, da er sie zum Zwecke der weiteren Verwendung auf einen Datenträger – den Kartenrohling – kopiert. Durch diese Speicherung entsteht sodann ein Falsifikat, das – außer der Wahrnehmbarkeit – alle Merkmale einer falschen Urkunde aufweist: Die auf dem Magnetstreifen enthaltenen Kontodaten verkörpern die Erklärung der ausstellenden Bank, der Karteninhaber sei zur Benutzung der Geldautomaten berechtigt. Der Datensatz ist auch geeignet und dazu bestimmt, für die Befugnis des Karteninhabers Beweis zu erbringen und als Aussteller ist in dem Datensatz die kartenausgebende Bank erkennbar, obwohl nicht diese, sondern der Täter die Daten auf das Blankett übertragen hat.[60] Regelmäßig wird zudem die Qualifikation des über § 269 Abs. 3 StGB anzuwendenden § 267 Abs. 4 StGB verwirklicht sein.[61]

3. Einsatz der Dubletten

a) Strafbarkeit nach § 152b Abs. 1 i.V.m. § 152a Abs. 1 Nr. 2 StGB

Der Einsatz der Dubletten zusammen mit den erspähten PINs zur Abhebung von Geldbeträgen ist nach § 152b Abs. 1 i.V.m. § 152a Abs. 1 Nr. 2 StGB in der Tatvariante des „Gebrauchens" strafbar. Bei den Dubletten handelt es sich um nachgemachte Zahlungskarten mit Garantiefunktion (s.o.). Gebrauchen meint die Verwendung der gefälschten Zahlungskarte im Zahlungsverkehr[62] und erfasst damit auch den Einsatz am Geldautomaten. Regelmäßig wird dabei der Qualifikationstatbestand des § 152b Abs. 2 StGB erfüllt sein.

[54] Die Tatbestandsmäßigkeit bejaht auch *Eisele*, CR 2011, 131 (134), der aber das Vorbereiten einer Straftat nach § 202a bzw. § 202b StGB ablehnt.

[55] *Seidl/Fuchs*, HRRS 2010, 85 (88).

[56] *Schumann*, NStZ 2007, 675 (676).

[57] Vgl. *Braun/Heidberg*, StrafRechtsReport 2010, 89 (92).

[58] St. Rspr., vgl. z.B. BGH, Urt. v. 27.1.2011 – 4 StR 338/10; explizit für Maestro-Karten vgl. BGH, Beschl. v. 13.10.2011 – 3 StR 239/11; *Fischer* (Fn. 21), § 152b Rn. 4 f.; a.A. *Heger*, wistra 2010, 281, der die Fälschung von Maestro-Karten mit gewichtigen Argumenten nur unter § 152a StGB subsumieren will. EC-Karten und Maestro-Karten sind beides Debitkarten unterschiedlicher Debitkartenanbieter (MasterCard International bei der Maestro-Karte und die Deutsche Kreditwirtschaft [DK], bis Mitte 2011 Zentraler Kreditausschuss [ZKA], bei der EC-Karte). EC steht dabei seit 2002 für electronic cash und nicht mehr für Eurocheque.

[59] Ausf. hierzu *Eisele*, CR 2011, 131 (134); *Fischer* (Fn. 21), § 152a Rn. 11; *Braun/Heidberg*, StrafRechtsReport 2010, 89 (92); a.A. *Sternberg-Lieben* (Fn. 53), § 152a Rn. 5.

[60] Vgl. *Meier*, JuS 1992, 1017 (1018); *Freund*, JuS 1994, 207 (209 f.).; *Weidemann* (Fn. 18), § 269 Rn. 9; *Hilgendorf*, JuS 1997, 130 (134).

[61] Auf Konkurrenzebene wird § 269 StGB jedoch von § 152b StGB verdrängt, vgl. *Erb* (Fn. 37), § 269 Rn. 41, und *Eisele*, CR 2011, 131 (134).

[62] *Erb* (Fn. 38), § 152a Rn. 11.

b) Strafbarkeit nach § 263a StGB

Durch die Verwendung der Kartendubletten wird zudem der Tatbestand des § 263a Abs. 1 StGB in der Begehungsform „unbefugte Verwendung von Daten“ verwirklicht.[63] Von dieser Variante ist neben der Verwendung einer im Wege verbotener Eigenmacht erlangten Originalkarte durch einen nichtberechtigten Dritten[64] auch die Verwendung von kopierten, gefälschten oder manipulierten Codekarten erfasst, und zwar unabhängig davon, ob die Herstellung bzw. Manipulation durch den Täter selbst oder durch einen Dritten erfolgt ist.[65] Durch die Tathandlung kommt es auch zu einer Beeinflussung des Ergebnisses eines Datenverarbeitungsvorgangs.[66] Eine Beeinflussung des Ergebnisses liegt vor, wenn das Ergebnis des Datenverarbeitungsvorgangs ohne die Manipulationshandlung entweder anders hätte lauten müssen oder überhaupt nicht hätte ergehen dürfen. Das Ergebnis kann also bereits inhaltlich unzutreffend oder zwar an sich richtig, aber unbefugterweise herbeigeführt sein.[67] Zudem muss die Manipulationshandlung für das Ergebnis zumindest mitursächlich sein und das Ergebnis hat unmittelbar zu einer Vermögensminderung zu führen.[68] Letzteres ist der Fall, wenn die Vermögensminderung ohne weitere wesentliche Zwischenschritte einer natürlichen Person herbeigeführt wird.[69] Die genannten Voraussetzungen sind bei der Verwendung der Dubletten zur Geldabhebung sämtlich erfüllt: Das Ergebnis des im Geldautomaten ablaufenden Datenverarbeitungsvorgangs ist zwar inhaltlich richtig, wurde vom Skimming-Täter aber unbefugterweise herbeigeführt. Die Verwendung der Dubletten – mithin die Manipulationshandlung – ist zudem mitursächlich für dieses Ergebnis, welches sich schließlich in Form der automatisch erfolgenden Geldausgabe auch unmittelbar vermögensmindernd auswirkt.

Problematisch gestaltet sich die Antwort auf die Frage, bei wem der Vermögensschaden eintritt.[70] Die Abhebung des Geldbetrages durch den Skimming-Täter erfolgt – weil ohne bzw. gegen den Willen des Kontoinhabers – ohne dessen Autorisierung i.S.d. § 675j Abs. 1 S. 1, 4 BGB, sodass ihm gem. § 675u S. 2 BGB grundsätzlich ein Anspruch gegen die Bank auf Erstattung des Zahlungsbetrages zusteht. Zu beachten ist jedoch die Regelung des § 675v Abs. 1 und Abs. 2 BGB, wonach die Bank wiederum einen Schadensersatzanspruch gegen den Kontoinhaber hat, wenn der infolge eines nicht autorisierten Zahlungsvorgangs entstandene Schaden aufgrund der missbräuchlichen Verwendung eines Zahlungsauthentifizierungsinstruments entstanden ist und der Kontoinhaber die personalisierten Sicherheitsmerkmale (insbes. die PIN) nicht sicher aufbewahrt hat (§ 675v Abs. 1 S. 2 BGB) oder der Schaden von Letzterem durch grob fahrlässige Verletzung von Pflichten aus § 675l BGB oder von vereinbarten Bedingungen für die Ausgabe und Nutzung von Codekarte und PIN herbeigeführt wurde (§ 675v Abs. 2 Nr. 1 und 2 BGB).[71] Im Falle des § 675v Abs. 1 S. 2 BGB ist der vom Kontoinhaber zu ersetzende Schaden dabei höhenmäßig auf maximal 150 Euro begrenzt und der Anspruch der Bank besteht nach h.M. nur bei Vorliegen eines Verschuldens.[72] Im Falle des § 675v Abs. 2 BGB haftet der Kontoinhaber dagegen unbegrenzt.

In dem Moment, in dem beim Skimming die PIN des Bankkunden vom Skimming-Täter ausgespäht wird, wird diese von Ersterem, der von der am Geldautomaten vorgenommenen Manipulation nichts ahnt, ordnungsgemäß verwendet. Davon, dass er die PIN zu diesem Zeitpunkt „nicht sicher aufbewahrt“, kann daher nicht die Rede sein, sodass eine (begrenzte) Haftung des Bankkunden nach § 675v Abs. 1 S. 2 BGB also nicht in Betracht kommen dürfte. Auch die (unbegrenzte) Haftung nach § 675v Abs. 2 Nr. 1 und 2 BGB scheidet aus: Nach § 675l S. 1 BGB ist der Bankkunde nur dazu verpflichtet, alle zumutbaren Vorkehrungen zu treffen, um die personalisierten Sicherheitsmerkmale vor unbefugtem Zugriff zu schützen. Zumutbar sind dabei nur solche Vorkehrungen, die die Nutzung des Zahlungsauthentifizierungsinstruments nicht derart einschränken, dass es seine praktische Brauchbarkeit für die mit ihm bezweckten Einsatzmöglichkeiten verliert. Das Gebot, bei der PIN-Eingabe

[63] Zum Meinungsstreit bzgl. des Merkmals „unbefugt“ vgl. ausf. *Eisele*, CR 2011, 131 (135).

[64] BGHSt 47, 160 (162).

[65] BGHSt 38, 120 (123); 47, 160 (162); *Wohlers* (Fn. 26), § 263a Rn. 27 subsumiert diesen Fall dagegen unter „Verwendung unrichtiger oder unvollständiger Daten“ (Var. 2), *Ranft* (wistra 1987, 78 [84]) unter „unrichtige Programmgestaltung“ (Var. 1).

[66] BGHSt 38, 120 (124). Ob die Einleitung eines Datenverarbeitungsvorgangs schon für sich gesehen als Beeinflussung des Ergebnisses eingestuft werden kann, ist umstritten, richtigerweise aber zu bejahen, da mit dem Auslösen eines Prozesses auf diesen schließlich sogar besonders intensiv Einfluss genommen wird, vgl. BGHSt 38, 120 (121); OLG Köln, Urt. v. 9.7.1991 – Ss 624/90; *Berghaus*, JuS 1990, 981; *Lackner/Kühl* (Fn. 33), § 263a Rn. 22; *Cramer/Perron*, in: Schönke/Schröder (Fn. 14), § 263a Rn. 18; *Fischer* (Fn. 21), § 263a Rn. 20.

[67] BGHSt 38, 120 (124).

[68] *Beckemper*, in: von Heintschel-Heinegg (Fn. 18), § 263a Rn. 37.

[69] *Beckemper* (Fn. 68), § 263a Rn. 39.

[70] Vgl. zur ähnlichen Problematik beim sog. Phishing *Seidl/Fuchs*, HRRS 2010, 85 (88 f.).

[71] Nach § 675l BGB ist der Kontoinhaber dazu „verpflichtet, unmittelbar nach Erhalt eines Zahlungsauthentifizierungsinstruments alle zumutbaren Vorkehrungen zu treffen, um die personalisierten Sicherheitsmerkmale vor unbefugtem Zugriff zu schützen“ (S. 1) sowie „dem Zahlungsdienstleister […] den Verlust, den Diebstahl, die missbräuchliche Verwendung oder die sonstige nicht autorisierte Nutzung eines Zahlungsauthentifizierungsinstruments unverzüglich anzuzeigen, nachdem er hiervon Kenntnis erlangt hat“ (S. 2).

[72] *Palandt*, Bürgerliches Gesetzbuch, Kommentar, 71. Aufl. 2012, § 675v Rn. 3; so auch die Gesetzesbegründung BT-Drs. 16/11643, S. 113, die von einem Verschuldenselement spricht.

am Geldautomaten stets die Tastatur abzudecken, um ein mögliches Ausspähen zu verhindern, stellt aber gerade eine solche einschränkende und damit unzumutbare Vorkehrung dar.[73] Kommt es also zu einem Ausspähen der PIN, weil der Skimming-Täter oder die von ihm installierte Kamera mangels Verdecken der Geldautomatentastatur „freie Sicht" auf das Eingabefeld hatte, so ist der Schaden nicht auf eine Pflichtverletzung des Bankkunden zurückzuführen, dessen Haftung nach § 675v Abs. 2 Nr. 1 BGB scheidet mithin aus. Dies gilt erst recht in den Fällen, in denen das Ausspähen mittels einer Tastaturattrappe erfolgt, weil hier ein Verdecken bei der PIN-Eingabe ohnehin zwecklos ist. Daneben dürfte eine Haftung nach § 675v Abs. 2 BGB zudem an fehlender grober Fahrlässigkeit des Bankkunden scheitern: Wie eingangs bereits erwähnt, ist es für einen Laien nahezu unmöglich, von Skimming-Tätern an Geldautomaten vorgenommene Manipulationen zu erkennen. Davon, dass ein argloser Bankkunde bei der Geldabhebung daher die im Verkehr erforderliche Sorgfalt in einem ungewöhnlich hohen Maß verletzt, kann im Regelfall also nicht die Rede sein. Eine Haftung des Kunden kommt folglich regelmäßig nicht in Betracht, sodass der Vermögensschaden aufgrund der Rückerstattungspflicht aus § 675u S. 2 BGB bei der Bank eintritt.[74]

In der Regel wird auch der Qualifikationstatbestand des über § 263a Abs. 2 StGB anwendbaren § 263 Abs. 5 StGB erfüllt sein.

c) Strafbarkeit nach § 269 StGB

Der Skimming-Täter macht sich durch die Benutzung der Dubletten zudem wegen Fälschung beweiserheblicher Daten nach § 269 Abs. 1 StGB in der Begehungsform des „Gebrauchens" strafbar,[75] wobei auch hier die Qualifikation des über § 269 Abs. 3 StGB anzuwendenden § 267 Abs. 4 StGB regelmäßig erfüllt sein dürfte.[76]

d) Strafbarkeit nach § 202a Abs. 1 StGB

Schließlich ist auch der Tatbestand des § 202a Abs. 1 StGB erfüllt. Mithilfe der zuvor erspähten PIN sowie der angefertigten Kartendubletten ist es dem Täter möglich, am Geldautomaten den Kontostand des jeweiligen Kontoinhabers einzusehen.[77] Darin ist ein Sichverschaffen des Zugangs zu nicht für den Täter bestimmten sowie gegen unberechtigten Zugang besonders gesicherten Daten zu sehen, das unter Überwindung einer Zugangssicherung erfolgt.[78]

4. Strafbarkeit der Herstellung bzw. des Verschaffens der Skimming-Ausrüstung

a) Strafbarkeit des Sichverschaffens bzw. der Herstellung des Magnetstreifenlesers nach § 152b Abs. 5 i.V.m. § 149 Abs. 1 Nr. 1 StGB

Für das Skimming greifen die Täter auf legal erhältliche,[79] vorgefertigte Magnetstreifen(-durchzugs- oder -einsteck-)lesegeräte aus dem Handel zurück, die sie vor ihrer Verwendung bearbeiten und verändern. Erforderlich ist neben dem Einbau der Geräte in spezielle (zur Tarnung benötigte) Gehäuse die Erweiterung um eine Batterie als Stromquelle für den mobilen Einsatz sowie das Hinzufügen eines Speicher- oder Sendemoduls, um ein Zwischenspeichern bzw. das Versenden der ausgelesenen Magnetstreifeninformationen zu ermöglichen.[80] Durch die Vornahme dieser Manipulationen wird der Tatbestand des § 152b Abs. 5 i.V.m. § 149 Abs. 1 Nr. 1 StGB in der Begehungsform des Herstellens einer „ähnlichen Vorrichtung" verwirklicht. Die veränderten Kartenlesegeräte erfüllen bei der Herstellung unechter Zahlungskarten mit Garantiefunktion die gleiche Funktion wie Platten, Formen, Druckstöcke etc. für die Herstellung von falschem Geld.[81] Nach Vornahme der genannten Manipulationen wohnt ihnen darüber hinaus auch eine spezifische Eignung zur deliktischen Verwendung inne. Gleichwohl wurde ihre Subsumtion unter § 149 Abs. 1 Nr. 1 StGB früher abgelehnt. Begründet wurde dies damit, dass durch sie die Herstellung von Falsifikaten nicht „unmittelbar ins Werk gesetzt" wird.[82] Das Kriterium der Eignung zur unmittelbaren Herstellung der Falsifikate ist jedoch auf die traditionellen Herstellungsverfahren mit Druckplatten o.Ä. zugeschnitten und bezieht dort seine Berechtigung daraus, dass diese Gegenstände typischerweise erst auf einer sehr späten Stufe des Produktionsprozesses ihre spezifische Tauglichkeit für Fälschungen erlangen.[83] Bei den von den Tätern hergestellten „Skimmern" ist dies jedoch gerade nicht der Fall, da bereits das auf einer frühen Stufe angesiedelte Auslesen der Magnetstreifen zu den hochspeziellen Fälschungsfunktionen gehört.[84] Aus diesem Grunde sind sie unter § 149 Abs. 1 Nr. 1 StGB zu subsumieren, eine Strafbarkeit ist mithin zu bejahen.[85]

---

[73] *Palandt* (Fn. 72), § 675l Rn. 2.

[74] Vgl. auch *Eisele*, CR 2011, 131 (136).

[75] *Hoyer* (Fn. 35), § 269 Rn. 16; vgl. auch *Eisele*, CR 2011, 131 (134), der weniger auf die Daten der Dublette als vielmehr auf die Eingabe der PIN abstellt.

[76] Auf Konkurrenzebene dürfte § 269 StGB jedoch von § 152b StGB verdrängt werden, vgl. *Erb* (Fn. 37), § 269 Rn. 41.

[77] So auch *Bachmann/Goeck*, JR 2011, 425 (426).

[78] S.o. unter II. 1. b) bb); vgl. auch *Tyszkiewicz*, HRRS 2010, 207 (212); a.A. *Eisele*, CR 2011, 131 (136).

[79] A.A. *Puppe* (Fn. 43), § 149 Rn. 7: Legal verfügbare Lesegeräte, die auch von Händlern im Rahmen des POS- oder POZ-Verfahrens eingesetzt werden, seien zum „skimmen" nicht geeignet, da sie vom Zentralausschuss für das Kreditwesen (ZAK) auf Sicherheit hin geprüft würden und autorisiert seien. Bei den von den Skimming-Tätern verwendeten Geräten müsse es sich deshalb um „illegal" erworbene handeln. Dabei wird jedoch verkannt, dass es sich bei den beim Skimming zum Einsatz kommenden Gerätschaften um einfache Durchzugsleser für Magnetstreifen handelt, die in jedem Elektronikfachversand frei erhältlich sind.

[80] *Eckart/Guggenbühl/Pfefferli/Fluri*, Kriminalistik 2003, 547 (551); *Braun/Heidberg*, StrafRechtsReport 2010, 89 (90).

[81] *Puppe* (Fn. 43), § 149 Rn. 7.

[82] BGH, Urt. v. 16.12.2003 – 1 StR 297/03; *Husemann*, NJW 2004, 104 (109).

[83] *Stein* (Fn. 43), § 149 Rn. 2.

[84] *Stein* (Fn. 43), § 149 Rn. 2.

[85] Vgl. *Fischer* (Fn. 21), § 149 Rn. 3; *Puppe* (Fn. 43), § 149 Rn. 7 f.; *Stein* (Fn. 43), § 149 Rn. 2; a.A. *Eisele*, CR 2011,

b) Strafbarkeit des Sichverschaffens des Schreib-/Codiergeräts samt Software

aa) Strafbarkeit nach § 152b Abs. 5 i.V.m. § 149 Abs. 1 Nr. 1 StGB

Wie die Lesegeräte sind auch die Schreibgeräte, mit denen die Dubletten beschrieben werden, frei im Handel verfügbar.[86] Damit fehlt auch ihnen grundsätzlich die spezifisch deliktische Eignung, da sie gleichermaßen für legale Zwecke eingesetzt werden können. Im Unterschied zu den Lesegeräten werden die Codiergeräte auch nicht weiterverarbeitet oder irgendwo eingebaut, sie behalten also ihr ursprüngliches Aussehen und erlangen somit auch nicht auf diese Art die erforderliche ausschließlich deliktische Verwendbarkeit. Damit scheidet hinsichtlich der Magnetstreifencodiergeräte eine Strafbarkeit nach § 152b Abs. 5 i.V.m. § 149 Abs. 1 Nr. 1 StGB aus.

bb) Strafbarkeit nach § 202c Abs. 1 Nr. 2 i.V.m. § 202a Abs. 1 StGB

Auch eine Strafbarkeit nach § 202c Abs. 1 Nr. 2 i.V.m. § 202a Abs. 1 StGB in der Form des Sichverschaffens eines Computerprogramms, dessen Zweck die Begehung einer Tat nach § 202a Abs. 1 StGB ist, scheidet aus. Durch die spätere Benutzung der mithilfe des Codiergeräts hergestellten Kartendubletten wird zwar der Tatbestand des § 202a Abs. 1 StGB verwirklicht.[87] Bei der in Kombination mit dem Codiergerät zum Beschreiben der Magnetstreifen der Dubletten verwendeten Software handelt es sich zudem um ein Computerprogramm, welches sich die Täter im Zuge des Erwerbs des Geräts verschafft haben. Eine Strafbarkeit nach § 202c Abs. 1 Nr. 2 StGB setzt aber auch voraus, dass das Computerprogramm mit der Absicht entwickelt oder modifiziert wurde, es zur Begehung der genannten Straftaten einzusetzen und dass sich diese Absicht auch objektiv manifestiert hat.[88] Die bloße Eignung zur Straftatenbegehung reicht dagegen nicht aus. Bei der in Kombination mit dem Magnetstreifencodierer zu verwendenden Software fehlt es jedoch gerade an der erforderlichen deliktischen Zweckbestimmung.

cc) Strafbarkeit nach § 263a Abs. 3 StGB

Eine Strafbarkeit nach § 263a Abs. 3 StGB scheitert bereits an der hierfür erforderlichen deliktischen Zweckbestimmung, an der es der verwendeten Software fehlt.

5. Strafbarkeit nach § 261 Abs. 2 Nr. 1, Abs. 1 S. 2 Nr. 4 lit. a StGB durch Verteilung der Beute

Das Verteilen der Beute erfüllt den Tatbestand der Geldwäsche nach § 261 Abs. 2 Nr. 1, Abs. 1 S. 2 Nr. 4 lit. a StGB, weil sich die Täter Gegenstände verschaffen, die aus der Katalogtat des § 263a StGB herrühren und diese auch gewerbsmäßig bzw. von einem Mitglied einer Bande, die sich zur fortgesetzten Begehung solcher Taten verbunden hat, begangen worden ist. Allerdings ist § 261 Abs. 9 S. 2 StGB zu beachten, wonach eine Bestrafung von Personen ausscheidet, die wegen Beteiligung an der Vortat strafbar sind. Dieser persönliche Strafausschließungsgrund wird regelmäßig bei allen Bandenmitgliedern, bei denen – wie bereits erwähnt – grundsätzlich Mittäterschaft anzunehmen ist, einschlägig sein.

III. Zusammenfassung und Ausblick

Die Strafbarkeit der Skimming-Täter ist abhängig vom jeweiligen Tatfortschritt. Das Verhältnis mehrerer verwirklichter Tatbestände zueinander ist auf Konkurrenzebene zu entscheiden.[89] Die Rechtsprechung zu den typischen Fallkonstellationen beim Skimming hat sich mittlerweile durch mehrere höchstrichterliche Entscheidungen gefestigt.[90] So werden die Angeklagten bei Tatvollendung in der Regel wegen gewerbs- und bandenmäßiger Fälschung von Zahlungskarten mit Garantiefunktion in Tateinheit mit gewerbs- und bandesmäßigem Computerbetrug verurteilt.[91] Auch die Fälle, in denen die Täter bei der Tatausführung gestört werden, z.B. wenn die Manipulationen am Geldautomaten entdeckt werden, und die Tatvollendung in der Folge durch Sicherstellung der Skimming-Anbauten durch die Polizei verhindert wird, und die damit zusammenhängende Problematik des unmittelbaren Ansetzens zur Fälschung von Zahlungskarten mit Garantiefunktion sind nunmehr weitgehend höchstrichterlich geklärt.

Spannend bleibt aber, wie es zukünftig im Kampf gegen die Skimming-Kriminalität weitergehen wird. Obwohl die seit 2011 verbindliche Einführung der EMV-Chip-Technologie[92] in den SEPA-Staaten zur Bekämpfung der Skimming-Kriminalität augenscheinlich erfolgreich ist – die Angriffe auf Geldautomaten sind im ersten Halbjahr 2011 im Vergleich zum Vorjahr um 60 %, insgesamt im Jahr 2011 um rund 50 % zurückgegangen –, dürfte der Kampf noch nicht endgültig gewonnen sein.

Es ist zu befürchten, dass die rückläufigen Zahlen auf eine Phase der Umorganisation der kriminellen Banden zurückzuführen sind, die in den neuen Absatzstaaten, in denen sie weiterhin die manipulierten Zahlungskarten zum Geldabheben verwenden können, erst die erforderlichen Strukturen aufbauen müssen.[93] Nach diesem Stadium der Neuausrichtung

131 (134). Eine Strafbarkeit nach § 202c Abs. 1 Nr. 2 StGB scheidet entgegen der Ansicht von *Braun/Heidberg*, StrafRechtsReport 2010, 89 (91), mangels Strafbarkeit des Auslesens der Magnetstreifeninformationen nach § 202a StGB dagegen grundsätzlich aus.

[86] A.A. *Puppe* (Fn. 43), § 149 Rn. 7.

[87] S.o. unter II. 3. d).

[88] BVerfG, Beschl. v. 18.5.2009 – 2 BvR 2233/07, 2 BvR 1151/08, 2 BvR 1524/08 = ZUM 2009, 745 (749).

[89] Vgl. zu den Konkurrenzen beim Skimming *Bachmann/Goeck*, JR 2011, 425 (426 f.).

[90] Vgl. insbes. BGH, Beschl. v. 6.7.2010 – 4 StR 555/09.

[91] Vgl. z.B. BGH, Urt. v. 27.1.2011 – 4 StR 338/10.

[92] Vgl. hierzu *Seidl/Fuchs*, HRRS 2011, 265 (274).

[93] *Seidl*, jurisAZO-ITR 19/2011 Anm. 2.

dürften ähnlich hohe Angriffszahlen zu erwarten sein wie bisher.[94]

Dies ist vor allem deshalb der Fall, weil eine Umsetzung des EMV-Standards in diversen außereuropäischen Staaten – wie beispielsweise den USA – nicht geplant ist und sich daher auch auf neu ausgegebenen Karten wieder ein Magnetstreifen befinden wird, um die internationale Einsatzfähigkeit dieser Karten zu sichern.[95] An den EMV-kompatiblen Geldautomaten der SEPA-Staaten werden zwar nur noch die EMV-Chips ausgelesen, die auf dem Magnetstreifen gespeicherten Daten können aber nach wie vor kopiert werden. Ein Abheben mittels Kartendubletten ist innerhalb Europas somit zwar nicht mehr möglich, weil Karten ohne Chip von den Terminals als Fälschung entlarvt werden. Zu einem Versiegen der Skimming-Kriminalität wird dies jedoch nicht führen. Ohne flankierende Maßnahmen werden die Täter lediglich die Verwertung der erlangten Kartendubletten in Nicht-Chip-Länder verlagern, in denen mangels Einsatzes EMV-kompatibler Geldautomaten weiterhin Abhebungen mit Kartendubletten vorgenommen werden können.[96]

Wünschenswert wären also die weltweite Einführung des EMV-Standards und die damit einhergehende Abschaffung der Magnetstreifen. Denkbar wäre aber auch eine „europäische Lösung", wonach die Karten innerhalb Europas nur noch mit EMV-Chips versehen werden, im außereuropäischen Raum dagegen eine zweite, mit Magnetstreifen ausgestattete Karte zum Einsatz kommt.[97]

Am praktikabelsten erscheint jedoch das sog. „Magstripe-Controlling", gemeint sind damit Mechanismen, die eine bewusste Kontrolle von Magnetstreifenumsätzen ermöglichen.[98] Dieses „Magstripe-Controlling" beinhaltet z.B. Maßnahmen wie die Festlegung von Limits für Auslandsabhebungen, die unverzügliche Benachrichtigung von Kunden per SMS bei erfolgten Auslandstransaktionen oder die grundsätzliche Deaktivierung der Karte für den Einsatz in Nicht-SEPA-Staaten.[99] Möchten die Kunden ihre Zahlungskarte dann aber in diesen Ländern einsetzen, müssen sie zuvor den Magnetstreifen ihrer Karte bei ihrer Bank „aktivieren" lassen – ein im Vergleich zum Skimming-Risiko verschmerzbar geringer Aufwand.[100]

---

[94] *Seidl*, jurisAZO-ITR 19/2011 Anm. 2.
[95] *Seidl/Fuchs*, HRRS 2011, 265 (274).
[96] *Seidl*, jurisAZO-ITR 19/2011 Anm. 2.
[97] *Seidl/Fuchs*, HRRS 2011, 265 (274).
[98] Vgl. hierzu BKA, Gemeinsame Pressekonferenz der EURO Kartensysteme GmbH und des Präsidenten des Bundeskriminalamtes: Aktuelle Zahlen zur Zahlungskartenkriminalität 2010 in Deutschland, S. 4 f., im Internet abrufbar unter: http://www.bka.de/nn_233110/SharedDocs/Downloads/DE/Presse/Pressearchiv/Presse__2011/pm110510__ZahlungskartenkriminalitaetBundeslagebild,templateId=raw,property=publicationFile.pdf/pm110510_ZahlungskartenkriminalitaetBundeslagebild.pdf (16.8.2012).
[99] *Seidl*, jurisAZO-ITR 19/2011 Anm. 2.
[100] *Seidl*, jurisAZO-ITR 19/2011 Anm. 2.

Strafbarkeitsrisiken beim IT-Outsourcing

Zum externen IT-Dienstleister als Gehilfen im Sinne des § 203 Abs. 3 S. 2 StGB*

Von Wiss. Assistent Dr. **Mesut S. Çekin**, Istanbul**

I. Einführung

Der ständig herrschende Kosten- und Zeitdruck zwingt heute zahlreiche Unternehmen dazu, die einzelnen Prozesse effizienter und flexibler zu gestalten, um Wettbewerbsvorteile zu erreichen. Die Auslagerung von IT-Dienstleistungen (oder neudeutsch: das IT-Outsourcing[1]) auf einen externen Dienstleister ist dabei eine gängige Methode in der heutigen Welt der Wirtschaft.[2] Der Grund liegt insbesondere in der heutigen, auf Arbeitsteilung angelegten Gesellschafts- und Rechtsordnung. Um den Einsatz von Spezialisten zu ermöglichen, aber auch um konkurrenz- und existenzfähig zu bleiben, muss die Unternehmensleitung personelle und sachliche Ressourcen rationell nutzen. Auf der anderen Seite führt die Auslagerung von Datenverarbeitung in rechtlicher Sicht vor allem zu Konflikten mit dem Schutz von Daten und tangiert damit verfassungsrechtlich gewährleistete Positionen der Betroffenen.[3]

Im deutschen Verfassungsrecht wurde die Befugnis des Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen, aus dem Recht auf informationelle Selbstbestimmung abgeleitet.[4] Darüber hinaus hat das BVerfG[5] in jüngster Zeit klargestellt, dass das allgemeine Persönlichkeitsrecht auch das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme erfasst und sowohl die Vertraulichkeit der Daten als auch die Integrität des IT-Systems schützt.[6] Schließlich hat auch der Europäische Gerichtshof festgestellt, dass nach seiner ständigen Rechtsprechung „das in Art. 8 EMRK verankerte Recht auf Achtung des Privatlebens, das sich aus den gemeinsamen Verfassungsüberlieferungen der Mitgliedstaaten herleitet, ein von der Gemeinschaftsordnung geschütztes Grundrecht“ darstellt.[7]

Als Ausfluss dieser verfassungsrechtlichen Grundlagen wird das Offenbaren fremder Geheimnisse in § 203 StGB unter Strafe gestellt. Es wird bestraft, wer unbefugt ein fremdes Geheimnis, namentlich ein zum persönlichen Lebensbereich gehörendes Geheimnis oder ein Betriebs- oder Geschäftsgeheimnis, offenbart, das ihm als eine der enumerativ aufgezählten Personen anvertraut worden oder sonst bekanntgeworden ist. Insofern stellt sich die bis dato noch wenig geklärte Frage, wie das Weitergeben von Informationen an einen externen IT-Dienstleister im Lichte des § 203 StGB zu beurteilen ist. Es soll im Folgenden dargelegt werden, dass externe IT-Dienstleister im Sinne des § 203 Abs. 3 S. 2 StGB als „Gehilfen“ der in § 203 Abs. 1 und 2 StGB genannten Berufs- und Personengruppen zu qualifizieren sind, solange die strengen Mindestvoraussetzungen des Bundesdatenschutzgesetzes eingehalten werden. Solange dies der Fall ist, ist mit anderen Worten ein IT-Outsourcing gem. § 203 StGB straflos.

---

* Bei dem Text handelt es sich um das überarbeitete und um Fußnoten ergänzte Manuskript des *Autors* für den Vortrag am 14.10.2012 im Rahmen der Konferenz „Cyber Crime: Legal Perspectives in Turkey and Germany“ an der Bilgi Universität in Istanbul.

** Der *Verf.* ist ehemaliger wissenschaftlicher Mitarbeiter an der Juristischen Fakultät der Universität Tübingen, Lehrstuhl Prof. *Dr. Dr. Dr. h.c. Kristian Kühl*.

[1] Das Wort Outsourcing setzt sich zusammen aus den Worten „outside, resource und using“ (vgl. *Wurl/Lazanowski*, in: WISU – Das Wirtschaftsstudium 2002, S. 1541) und könnte sich etwa mit „Nutzung externer Ressourcen“ übersetzen lassen (*Nagenast*, Outsourcing von Dienstleistungen industrieller Unternehmen – eine theoretische und empirische Analyse, 1997, S. 47). IT hingegen ist die Abkürzung von Information Technology. Dabei bedeutet Outsourcing in der Ökonomie – sehr vereinfacht – die Abgabe von Unternehmensaufgaben und -strukturen an Drittunternehmen (vgl. *Lux/Schön*, Outsourcing der Datenverarbeitung, 1997, S. 3). Beim IT-Outsourcing geht es also um die Auslagerung der Datenverarbeitung als Unternehmensaufgabe.

[2] Vgl. etwa Handelsblatt, Dienstleister entlasten gestresste IT-Abteilungen, abrufbar unter: http://www.handelsblatt.com/unternehmen/mittelstand/dienstleister-entlasten-gestresste-it-abteilungen/3423514.html [Stand: Juli 2012].

[3] Vgl. hierzu allgemein *Müthlein/Heck*, Outsourcing und Datenschutz, 4. Aufl. 2010.

[4] Vgl. das Volkszählungsurteil des BVerfG, BVerfGE 65, 1 = NJW 1984, 419; vgl. hierzu auch *Hilgendorf*, in: Sieber u.a. (Hrsg.), Festschrift für Klaus Tiedemann, 2008, S. 1125 (S. 1127).

[5] BVerfGE 120, 274 = NJW 2008, 822; hierzu auch *Fink*, in: Spindler/Schuster (Hrsg.), Recht der elektronischen Medien, Kommentar, 2. Aufl. 2011, Allgemeines C. Rn. 63-65.

[6] Auch das türkische Verfassungsrecht kennt das Recht auf informationelle Selbstbestimmung. Durch das Verfassungsreferendum im Jahr 2010 wurde dieses Recht in Art. 20 der Türkischen Verfassung ausdrücklich normiert. Art. 20 der Türkischen Verfassung lautet: „Jedermann hat ein Recht auf den Schutz seiner personenbezogenen Daten. Dieses Recht gestattet jedem Einzelnen die Information über die eigenen persönlichen Daten, die Möglichkeit eines Zugriffs auf diese Daten, Korrektur oder Löschung dieser Daten und die Information über den zweckmäßigen Gebrauch dieser Daten. Die Verarbeitung der personenbezogenen Daten ist gestattet, wenn dies gesetzlich vorgesehen ist oder die betroffene Person ausdrücklich darin eingewilligt hat.“

[7] Vgl. jüngst EuGH EuZW 2010, 939 (941 Rn. 52), der auch auf die Rspr. des EGMR (EGMR, Urt. v. 16.2.2000 – App. Nr. 27798/95 [Amann v. Schweiz] = Recueil des arrets et décisions 2000-II, § 65 und EGMR, Urt. v. 4.5.2000 – App. Nr. 28341/95 [Rotaru v. Rumänien] = Recueil des arrets et décision 2000-V, § 43) Bezug nimmt; vgl. darüber hinaus die Präambel der Datenschutzrichtline 95/46/EG; *Fink* (Fn. 5), Allgemeines B. Rn. 32.

Um dies darzulegen, werden zunächst die Grundlagen des § 203 StGB in Erinnerung gerufen (unten II.), bevor dann auf den Gehilfenbegriff des § 203 Abs. 3 S. 2 StGB im Kontext des IT-Outsourcing eingegangen wird (unten III.).

II. Grundlagen des § 203 StGB

§ 203 StGB ist als Sonderdelikt konzipiert, d.h. als Täter kommen nur die in der Vorschrift genannten geheimhaltungspflichtigen Personen in Betracht.[8] Strafbar macht sich daher nur der Mitteilende.[9] Anders als z.B. in Art. 378 des französischen Code penal, der generell alle Personen zur Geheimhaltung verpflichtet, denen kraft ihres Berufes Geheimnisse anvertraut werden, hat sich der deutsche Gesetzgeber für eine sektorale Lösung entschieden;[10] d.h. die Vorschrift bezieht sich nur auf die dort genannten Personen bzw. Personengruppen.[11] Dieser fragmentarische Charakter der Vorschrift entfacht stets Diskussionen über die Einbeziehung von Berufsgruppen in den Täterkreis der Vorschrift.[12]

Als entsprechende Täter werden in § 203 StGB u.a. Ärzte, Tierärzte, Apotheker, Berufspsychologen, Rechtsanwälte, Patentanwälte, Notare, Wirtschaftsprüfer und Ehe-, Familien- oder Jugendberater sowie Angehörige eines Unternehmens der privaten Kranken-, Unfall- oder Lebensversicherungen genannt; damit sind Berufe betroffen, bei denen der Berufstätige tiefe Einblicke in die privaten Verhältnisse seines Gegenüber erhält. Abs. 2, 2a und 3 des § 203 StGB erweitern den Anwendungsbereich dieser Vorschrift auf weitere Personen.

Die relevante Tathandlung ist das unbefugte Offenbaren eines fremden Geheimnisses. Ein Geheimnis i.S.d. § 203 StGB wird beschrieben als „eine Tatsache, die nur einem begrenzten Personenkreis bekannt oder zugänglich ist, die derjenige, dessen Sphäre sie entstammt, nicht aus dem Kreis hinausgelangen lassen will und an deren Geheimhaltung er ein von seinem Standpunkt aus verständliches Interesse hat."[13] In den meisten Fällen wird es sich um besonders heikle bzw. sensible Informationen handeln, die den jeweiligen Berufsträgern anvertraut werden, so dass regelmäßig Geheimnisse im Sinne der Vorschrift vorliegen werden.[14]

Offenbaren ist jede Hinausgabe von Tatsachen aus dem Kreis der Wissenden oder der zum Wissen Berufenen.[15] Vom Begriff des Offenbarens ist eine interne Weitergabe der Daten innerhalb bestimmter Funktionseinheiten desselben Unternehmens jedoch nicht erfasst.[16] Das Offenbaren erfolgt unbefugt, wenn es an einem tatbestandsausschließenden Einverständnis oder an sonstigen Rechtfertigungsgründen fehlt.[17] Das Einholen eines Einverständnisses ist häufig aus Praktikabilitätsgründen sehr schwierig oder auch unwirtschaftlich,[18] so dass im Folgenden von einer fehlenden Einwilligung der jeweils Betroffenen ausgegangen wird.[19]

III. Der externe IT-Dienstleister als Gehilfe i.S.v. § 203 Abs. 3 S. 2 StGB

Ob bei einem Outsourcing der Datenverarbeitung an einen IT-Dienstleister eine Offenbarung i.S.d. dieser Vorschrift zu sehen ist,[20] hängt davon ab, wie der IT-Dienstleister zu qualifizieren ist.[21] Die Vorschrift des § 203 erweitert in Abs. 3 S. 2

[8] BGHSt 4, 355 (359); *Schünemann*, in: Laufhütte/Rissing-van Saan/Tiedemann (Hrsg.), Strafgesetzbuch, Leipziger Kommentar, Bd. 6, 12. Aufl. 2010, § 203 Rn. 1; vgl. auch *Eisele*, in: Schönke/Schröder, Strafgesetzbuch, Kommentar, 28. Aufl. 2010, § 203 Rn. 12 und *Lackner/Kühl*, Strafgesetzbuch, Kommentar, 27. Aufl. 2011, § 203 Rn. 2.

[9] *Hilgendorf* (Fn. 4), S. 1125 (S. 1128); *Kargl*, in: Kindhäuser/Neumann/Paeffgen (Hrsg.), Nomos Kommentar, Strafgesetzbuch, Bd. 2, 3. Aufl. 2010, § 203 Rn. 28.

[10] Im türkischen Strafgesetzbuch (tStGB) ist nach Art. 136 keine Eingrenzung vorgesehen. Stattdessen sieht Art. 137 Nr. 2 eine hälftige Straferhöhung für den Fall vor, dass der Täter die Geheimnisse während seiner Berufsausübung erlangt.

[11] *Kargl* (Fn. 9), § 203 Rn. 1; vgl. darüber hinaus auch BGHSt 4, 355 (359); *Schünemann* (Fn. 8), § 203 Rn. 1; vgl. auch *Eisele* (Fn. 8), § 203 Rn. 12 und *Lackner/Kühl* (Fn. 8), § 203 Rn. 2.

[12] *Kargl* (Fn. 9), § 203 Rn. 1.

[13] *Schünemann* (Fn. 8), § 203 Rn. 19; vgl. ferner OLG Köln NJW 2000, 3656; OLG Hamm NJW 2001, 1957; *Cierniak*, in: Joecks/Miebach (Hrsg.), Münchener Kommentar zum Strafgesetzbuch, Bd. 3, 2003, § 203 Rn. 11, 18; *Eisele* (Fn. 8), § 203 Rn. 5; *Lackner/Kühl* (Fn. 8), § 203 Rn. 14.

[14] Vgl. *Lilie*, in: Dannecker u.a. (Hrsg.), Festschrift für Harro Otto, 2007, S. 673 (S. 677), der insbesondere im Rahmen des § 203 StGB im Zusammenhang mit IT-Outsourcing einen sehr weiten Geheimnisbegriff befürwortet.

[15] RGSt 38, 62 (65); BGHSt 27, 120 (121); BGH NJW 1995, 2915 (2916); *Lackner/Kühl* (Fn. 8), § 203 Rn. 17; *Cierniak*, (Fn. 13), § 203 Rn. 48 m.w.N. unter Fn. 223.

[16] VG Münster MedR 1984, 118; LG Bonn NJW 1995, 2419 (2420); *Lackner/Kühl* (Fn. 10), § 203 Rn. 18; *Cierniak* (Fn. 13), § 203 Rn. 51; *Schünemann* (Fn. 8), § 203 Rn. 43.

[17] Vgl. etwa *Cierniak* (Fn. 13), § 203 Rn. 83.

[18] Das Einholen eines Einverständnisses insbesondere bei großen Versicherungsunternehmen kann bei bereits langjährigen Kunden sehr problematisch werden. Auch ist es nicht ausgeschlossen, dass zahlreiche Kunden mit der Weitergabe ihrer Daten nicht einverstanden sein werden. Was die Einholung von Einwilligungen für die Zukunft angeht, so ist ebenfalls höchst bedenklich, ob die Vereinbarung einer Einwilligung bzw. die Einbeziehung einer Einwilligungserklärung durch allgemeine Geschäftsbedingungen zivilrechtlich überhaupt zulässig ist.

[19] Vgl. auch *Lensdorf/Mayer-Wegelin/Mantz*, CR 2009, 62 (67).

[20] Bejahend etwa *Schünemann* (Fn. 8), § 203 Rn. 41; *Hilgendorf* (Fn. 4), S. 1125 (S. 1131 ff.); *ders*., in: Hilgendorf (Hrsg.), Informationsstrafrecht und Rechtsinformatik, 2004, S. 81 ff.; *Lilie* (Fn. 14), S. 673 (S. 675 f.).

[21] Es wird aber auch vorgeschlagen, eine Strafbarkeit des „Outsourcenden" wegen der Sozialadäquanz des Outsourcingprozesses abzulehnen (*Meier*, Der rechtliche Schutz patientenbezogener Gesundheitsdaten, 2003, S. 158). Dass Outsourcing jedoch nicht einen Grad an Normalität erreicht hat, dass es von weiten Teilen der Gesellschaft akzeptiert

den Kreis der möglichen Täter auf „berufsmäßig tätige Gehilfen“ und Personen, die bei den in Abs. 1 S. 1 genannten Berufsträgern zur Vorbereitung auf den Beruf tätig sind. Die Offenbarung der Geheimnisse an diese Gehilfen ist nicht strafbar.[22] Der „Outsourcende“ würde sich also durch die Übermittlung der Daten nicht strafbar machen, wenn der externe IT-Dienstleister als Gehilfe i.S.d. § 203 Abs. 3 S. 2 StGB qualifiziert werden könnte. Kann er nämlich als Gehilfe i.S.v. § 203 Abs. 3 S. 2 StGB angesehen werden, so werden die Tatsachen aus dem Kreis der zum Wissen Berufenen nicht hinausgegeben. Kann der externe IT-Dienstleister dagegen nicht als Gehilfe qualifiziert werden, so wird regelmäßig das Tatbestandsmerkmal des Offenbarens erfüllt sein, d.h. der „outsourcende“ Geheimträger i.S.d. Abs. 1 und 2 des § 203 StGB setzt sich Strafbarkeitsrisiken aus. Damit hat der Gehilfenbegriff in § 203 Abs. 3 S. 2 StGB in zweierlei Hinsicht Bedeutung, nämlich um den Täterkreis bestimmen zu können, aber auch, um festzulegen, ob ein Offenbaren von Geheimnissen „möglich“ ist. Denn: Die Weitergabe eines Geheimnisses an einen Gehilfen ist keine Offenbarung des Geheimnisses im Rechtssinne.

Was unter dem Gehilfenbegriff im Allgemeinen zu verstehen ist, ist umstritten. Eine obergerichtliche Rechtsprechung zu dieser Frage existiert nicht. Entsprechend kontrovers wird die Frage im Schrifttum diskutiert. Im groben Überblick:[23]

Die wohl herrschende Meinung stellt bei der Bestimmung des Gehilfen auf organisatorische Gesichtspunkte ab.[24] Dabei wird eine organisatorische Einbindung des Gehilfen in den Betrieb des Berufsträgers vorausgesetzt, die mit der Weisungsabhängigkeit des Helfers einhergeht. Begründet wird dies mit dem Zweck des § 203 StGB. Nach dieser Vorschrift soll die Geheimnisverwendung auf den vom Schweigepflichtigen persönlich kontrollierten Bereich beschränkt werden. Darüber hinaus wird auf die Vorschriften des Bundesdatenschutzrechts Bezug genommen, in deren §§ 3 Abs. 8 S. 2, 11 BDSG eine Auftragsdatenverarbeitung ausdrücklich geregelt ist. Da eine solche Ausnahme in § 203 StGB nicht gegeben sei, lehnt diese Ansicht mit einem argumentum e contrario die Qualifizierung des IT-Dienstleisters als Gehilfen ab. Schließlich sollen nicht nur der Bestimmtheitsgrundsatz und das Analogieverbot gemäß Art. 103 Abs. 2 GG gegen die Qualifizierung des IT-Dienstleisters als Gehilfen sprechen, sondern auch der Umstand, dass die Ausdehnung der Strafdrohung auf externe Dienstleister ins Uferlose führen würde.[25]

Eine weitere Ansicht erweitert den Kreis der zum Wissen berufenen ausnahmsweise auch auf externe Dritte wie Sachverständige, Detektive oder Dolmetscher als Gehilfen (etwa eines Rechtsanwalts), wenn sie in den informationellen Schutzbereich des Berufsgeheimnisträgers einbezogen sind. Voraussetzung dafür sei allerdings, dass der Dritte mit der Ausführung von Aufträgen betraut wird, die eine besonders enge Beziehung zum Aufgabenkreis des Schweigepflichtigen aufweist.[26]

Schließlich stellt eine neuere Auffassung auf die effektive Steuerungsmacht als maßgebliches Kriterium ab. Die Anforderungen an das Direktionsrecht und an die organisatorische Einbindung der herrschenden Ansicht seien nämlich unklar und in der dogmatischen Herleitung noch nicht abgeschlossen. Maßgeblich sei deswegen darauf abzustellen, ob der primär Schweigepflichtige eine Steuerungsmacht in dem Sinne innehat, dass er die Herrschaft über die zur Verfügung gestellten Informationen behält, diese Herrschaft tatsächlich ausüben kann und dies auch tut. Es entspräche nicht mehr den Erfordernissen einer modernen Arbeitswelt, die organisatorische Einbindung von Hilfspersonen zu verlangen.[27]

1. Der Gehilfenbegriff in begrifflicher und systematischer Auslegung

Begrifflich ist es nach hier vertretener Ansicht durchaus möglich, externe IT-Dienstleister als Gehilfen des Outsourcenden zu qualifizieren, auch wenn sie organisatorisch nicht in die Abläufe des outsourcenden Geheimnisträgers eingebunden sind. Insbesondere ist gegen die herrschende Meinung und ihr „organisatorisches Einbindungserfordernis“ Folgendes zu erinnern: § 203 Abs. 1 Nr. 6 StGB erklärt (bestimmte) Angehörige von (bestimmten) Unternehmen zu tauglichen Tätern eines Geheimnisverrates. Da sich Abs. 3 S. 2 auf alle Nummern des § 203 StGB, damit auch auf Abs. 1 Nr. 6 bezieht, muss Abs. 3 S. 2 über die Angehörigen des Unternehmens hinausgehen, da die Vorschrift ansonsten leer laufen würde.[28] In diesem Zusammenhang ist auch eine relativ junge Ent-

---

wird, zeigt gerade die gesetzgeberische Entwicklung in Form des Bundesdatenschutzgesetzes und auf europäischer Ebene die Datenschutzrichtlinie, die allesamt die steigende Sensibilisierung der Betroffenen bei der Verwendung ihrer Daten und das Bedürfnis nach gesetzlicher Regelung und Kontrolle widerspiegeln.

[22] Vgl. BGH NJW 1995 2915 (2916); BGH CR 1992, 24; *Otto*, wistra 1999, 201 (203).

[23] Einen sehr guten Überblick zum Streitstand mit zahlreichen weiteren Fußnoten geben: *Jahn/Palm*, Rechtsgutachten zur Frage der straf- und berufsrechtlichen Bewertung des Services „Anwaltssekretariat“ der ebuero AG, Berlin, S. 19 ff., abrufbar unter: http://www.rak-berlin.de/site/DE/int/PDF_Mitglieder_Skripten/280610_Rechtsgutachten_ProfJahn.pdf (Stand: Juli 2012).

[24] *Sieber*, in: Arnold u.a. (Hrsg.), Festschrift für Albin Eser, 2005, S. 1155 (S. 1181); *Lilie* (Fn. 14), S. 673 (S. 676 f.); *Schünemann* (Fn. 8), § 203 Rn. 41 und 79; *Hilgendorf* (Fn. 20), S. 81 (S. 92); *ders.* (Fn. 4), S. 1125 (S. 1129); *Fischer*, Strafgesetzbuch und Nebengesetze, Kommentar, 59. Aufl. 2012, § 203 Rn. 21.

[25] Vgl. etwa *Schünemann* (Fn. 8), § 203 Rn. 79.

[26] *Cierniak* (Fn. 13), § 203 Rn. 115, 117, unter Hinweis auf OLG Köln StV 1991, 506; LG Frankfurt NJW 1959, 589, und LG Verden StV 1996, 371.

[27] *Heghmanns/Niehaus*, NStZ 2008, 57; *Lensdorf/Mayer-Wegelin/Mantz*, CR 2009, 62; *Kort*, NStZ 2011, 193 (194 f.); ebenso für das sog. „Anwaltssekretariat“ *Jahn/Palm* (Fn. 23), S. 39.

[28] *Heghmanns/Niehaus*, NStZ 2008, 57 (59).

scheidung des BGH[29] von Belang, auf die namentlich *Kort*[30] im Zusammenhang mit IT-Outsourcing hingewiesen hat. In seiner Entscheidung stellt der BGH fest, dass der Datenaustausch zwischen einem Versicherungsunternehmen und deren Handelsvertretern unter dem Gesichtspunkt der Arbeitsteiligkeit, welcher in § 203 Abs. 3 S. 2 StGB Anerkennung findet, privilegiert ist und deswegen kein Verstoß gegen § 203 StGB vorliege. Der Gehilfenbegriff muss sich mithin auch auf Nicht-Angehörige eines Organisationsverbundes erstrecken. Zur Verdeutlichung: Wenn selbst externe, selbstständige Agenten eines Versicherungsunternehmens mittlerweile als Angehörige des Unternehmens gelten,[31] so muss der Kreis der sonstigen Gehilfen begrifflich auch Dritte erfassen können, wobei auf die Voraussetzungen dieser Erfassung noch zurückzukommen ist.

Ein weites Verständnis des Gehilfenbegriffs des § 203 StGB legen auch die entsprechend weiten Gehilfenbegriffe in § 278 BGB und § 53a StPO nahe: § 278 BGB setzt keine organisatorische Einbindung des sog. Erfüllungsgehilfen in den Betrieb des Schuldners voraus.[32] Und § 53a StPO zeigt ebenfalls, dass kein festes Dienst- oder Arbeitsverhältnis erforderlich ist, um als Gehilfe zu fungieren.[33]

Gegen diese Verweise auf §§ 203 Abs. 1 Nr. 6 StGB, 278 BGB, 53a StPO kann allerdings angeführt werden, dass der Gesetzgeber in bestimmten Bereichen die Auslagerung der Datenverarbeitung explizit vorgesehen hat. Insbesondere das Sozialrecht kennt in § 302 Abs. 2 S. 1 bis 3 SGB V die Möglichkeit, eine elektronische Abrechnung gegenüber Krankenkassen durch sog. Rechenzentren vornehmen zu lassen, womit die Zulässigkeit von IT-Outsourcing verbunden wird.[34] Auch andere Landeskrankenhausgesetze enthalten Regelungen, die die Weitergabe sensibler Patientendaten regeln.[35] Es ließe sich insofern argumentieren: Wäre der Gesetzgeber von der grundsätzlichen Zulässigkeit des IT-Outsourcing ausgegangen, so hätte in diesen Gesetzen ein Hinweis auf die Vorschriften des Bundesdatenschutzgesetzes (BDSG) ausgereicht und es hätte keiner Spezialregelung in den genannten Gesetzen bedurft.

2. Der Gehilfenbegriff im Lichte des Datenschutzrechts

Da eine systematische Auslegung also zu keinem eindeutigen Ergebnis führt, soll ein Blick auf die Wertungen des Datenschutzrechts geworfen werden.

Dem Datenschutzrecht lässt sich die Wertung des Gesetzgebers entnehmen, dass eine Datenübermittlung zulässig sein kann, wenn die Voraussetzungen des § 11 BDSG vorliegen, so dass eine zulässige Einschränkung des Persönlichkeitsrechts vorliegt. Klarzustellen ist an dieser Stelle aber, dass der Begriff des Geheimnisses i.S.d. § 203 StGB nicht deckungsgleich mit dem der „personenbezogenen Daten" i.S.d. § 3 Abs. 1 BDSG ist.[36] Personenbezogene Daten können nämlich auch scheinbar belanglose oder selbst offenkundige Tatsachen sein, so dass personenbezogen nicht gleichzusetzen ist mit höchstpersönlich oder sensibel.[37] Mithin kann eine zulässige Auslagerung personenbezogener Daten die strafrechtliche Verantwortlichkeit gemäß § 203 StGB nicht per se ausschließen.[38]

Gemäß § 3 Abs. 7 BDSG gelten sowohl der Auftraggeber als auch der Auftragnehmer als verantwortliche Stellen. Während der Auftragnehmer gemäß § 3 Abs. 8 S. 3 BDSG nicht Dritter ist, „bleibt der Auftraggeber als Herr der Daten für die Beachtung der datenschutzrechtlichen Vorgaben für die von ihm veranlassten Verarbeitungen verantwortlich."[39] Dabei muss das auslagernde Unternehmen auf die technischen und organisatorischen Maßnahmen des IT-Dienstleisters besonders achten. Der schriftlich erteilte Auftrag muss darüber hinaus insbesondere folgende Punkte enthalten:[40]

- den Umfang, die Art und den Zweck der vorgesehenen Erhebung, Verarbeitung oder Nutzung von Daten, die Art der Daten und den Kreis der Betroffenen;
- die Kontrollrechte des Auftraggebers und die entsprechenden Duldungs- und Mitwirkungspflichten des Auftragnehmers;
- den Umfang der Weisungsbefugnisse, die sich der Auftraggeber gegenüber dem Auftragnehmer vorbehält.

Das auslagernde Unternehmen bzw. der Outsourcende hat sich vor Beginn der Datenverarbeitung und sodann regelmäßig von der Einhaltung der beim Auftragnehmer getroffenen

[29] BGH NJW 2010, 2509.
[30] *Kort*, NStZ 2011, 193 (194).
[31] Vgl. *Kargl* (Fn. 11), § 203 Rn. 36. Gerade im Versicherungswesen wird es in der Regel der im Außendienst tätige Versicherungsagent sein, der zuerst mit den relevanten Geheimnissen i.S.d. Vorschrift in Berührung kommt; die Entgegennahme der Daten beim Kunden vor Ort ermöglicht es dem jeweiligen Versicherungsunternehmen erst, überhaupt tätig zu werden; vgl. hierzu *Kort*, NStZ 2011, 193 (194): „Erst recht muss sich der Gedanke der möglichen Arbeitsteiligkeit bei einer strengen Auflagen unterliegenden Auftragsdatenverarbeitung in der Ausgestaltung eines stark den Auftragnehmer und dessen Mitarbeiter bindenden Datenschutzvertrags wiederfinden."
[32] Vgl. zu § 278 BGB jüngst BGH NJW 2011, 139 (140 Rn. 18): keine „Bindung an die Weisungen des Schuldners"; dem folgend *Grüneberg*, in: Palandt, Bürgerliches Gesetzbuch, Kommentar, 72. Auf. 2012, § 278 Rn. 7.
[33] *Meyer-Goßner*, Strafprozessordnung, Kommentar, 55. Aufl. 2012, § 53a Rn. 2.
[34] *Schünemann* (Fn. 8), § 203 Rn. 119; näher *Lips/Schönberger*, NJW 2007, 1567.
[35] Eingehend *Hartmann*, Outsourcing in der Sozialverwaltung und Sozialdatenschutz, 2002, passim.
[36] Vgl. *Schneider*, in: Schneider (Hrsg.), Handbuch des EDV-Rechts, 4. Aufl. 2009, B. Rn. 252 und 253.
[37] Vgl. ausführlich *Weichert*, in: Däubler/Klebe/Wedde/Wiechert, Bundesdatenschutzgesetz, Kompaktkommentar, 3. Aufl. 2010, § 3 Rn. 2 ff.
[38] Deutlich hierzu *Cierniak* (Fn. 13), § 203 Rn. 51, der sich gegen eine an § 11 BDSG orientierte Auslegung ausspricht.
[39] *Gola/Schomerus*, Bundesdatenschutzgesetz, Kommentar, 10. Aufl. 2010, § 3 Rn. 50.
[40] Vgl. § 11 BDSG.

technischen und organisatorischen Maßnahmen zu überzeugen. Das Ergebnis ist zu dokumentieren.[41]

In der Kautelarpraxis werden dem Auftragnehmer zur Konkretisierung dieser Vorschrift mehrere Pflichten auferlegt. So hat dieser bereits dafür zu sorgen, dass das eingesetzte Personal im Hinblick auf die Wahrung des Datenschutzes vertrauenswürdig ist.[42] Auch der Kreis der von der Datenverarbeitung betroffenen Personen kann von Beginn an eingeschränkt werden. Darüber hinaus erfolgt die Verarbeitung der übermittelten Daten ausschließlich nach den Weisungen des Auftraggebers gemäß § 11 Abs. 3 BDSG. Dabei kann sich das auslagernde Unternehmen ein umfassendes Weisungsrecht über Art, Umfang und Verfahren der Datenverarbeitung vorbehalten, das er durch Einzelanweisungen konkretisieren kann.[43] Dies hängt von der Komplexität der Datenverarbeitung und der Sensibilität der verarbeiteten Daten ab, so dass umfangreiche Outsourcing-Maßnahmen mit sensiblem Dateninhalt höhere Anforderungen mit sich bringen können. Hieraus wird zugleich ersichtlich, welchen Einfluss das auslagernde Unternehmen insbesondere durch die umfassenden Weisungsrechte im Hinblick auf Art, Umfang und Verfahren der Datenverarbeitung gegenüber dem IT-Dienstleister ausüben kann. Schließlich kann die Einhaltung der vertraglichen Verpflichtungen durch interne (Innenrevision) und externe Kontrollen (Wirtschaftsprüfer und Aufsichtsbehörden) regelmäßig überprüft werden.[44]

3. Der Gehilfenbegriff des § 203 StGB im Lichte des Sinns und Zwecks der Vorschrift

Schließlich ist eine nähere Analyse der teleologischen Argumente der herrschenden Meinung vorzunehmen, wonach es der Zweck des § 203 StGB gebiete, die Geheimnisverwendung auf den vom Schweigepflichtigen persönlich kontrollierten Bereich einzuschränken. An dieser Stelle möchte ich beispielhaft auf eine in der Praxis übliche Vertragsklausel eingehen, wonach „der Auftraggeber […] sich im Rahmen der in dieser Vereinbarung betroffenen Auftragsbeschreibung ein umfassendes Weisungsrecht über Art, Umfang und Verfahren der Datenverarbeitung vor[behält], das er durch Einzelanweisungen konkretisieren kann." Ob ein einzelner Mitarbeiter nun dem eigenen Betrieb des nach § 203 Abs. 1 und 2 StGB Geheimnispflichtigen angehört oder diesem nicht eingegliedert ist, spielt für den relevanten Aspekt der Risikoerhöhung im Hinblick auf die missbräuchliche Geheimnisverwendung keine Rolle. Wenn durch ausreichende Maßnahmen die Steuerungs-, Weisungs- und Kontrollrechte des zur Verschwiegenheit Verpflichteten abgesichert werden und diese darüber hinaus durch interne und externe Kontrollmechanismen (Revision des Versicherers und Wirtschaftsprüfer) kontrolliert werden können, so ist nicht ersichtlich, warum es einen Unterschied macht, ob ein weisungs- und kontrollgebundener Dienstleister anders behandelt werden soll als der bei dem auslagernden Unternehmen angestellte Mitarbeiter.[45] Im Gegenteil: Der IT-Dienstleister wird aufgrund seiner wirtschaftlichen Abhängigkeit vom Outsourcenden eher darauf bedacht sein, die ihm anvertrauten Daten vor missbräuchlichem Umgang zu schützen, so dass die Auslagerung der Datenverarbeitung nicht per se zu einer Risikoerhöhung im Hinblick auf den Missbrauch der relevanten Daten führt. Gerade die jüngsten Geschehnisse um Société Générale und UBS zeigen zudem, dass interne Kontrollmechanismen auch nicht zwingend in der Lage sind, eigene Mitarbeiter von missbräuchlichem Umgang mit eigenen Daten abzuhalten. Darüber hinaus sind IT-Dienstleister eher darauf spezialisiert, durch organisatorische und technische Maßnahmen mögliche Missbrauchsfälle zu verhindern, aber auch Angriffe von außen abzuwehren. Es macht also einerseits keinen Unterschied, ob es der eigene Mitarbeiter ist, der überwacht wird, oder ein Dritter, der sowohl durch interne, als auch durch externe Personen bzw. Institutionen geprüft und kontrolliert wird und andererseits ist der Schutz der relevanten Daten durch den darauf spezialisierten IT-Dienstleister besser gewährleistet.

Das Argument der herrschenden Ansicht, das Analogieverbot und das Bestimmtheitsgebot nach Art. 103 Abs. 2 GG sprächen gegen die Qualifizierung des IT-Dienstleisters als Gehilfen, ist ebenso nicht haltbar. Das Bestimmtheitsgebot besagt, dass die Straftatbestandsvoraussetzungen gesetzlich konkretisiert sein müssen. Es verpflichtet den Gesetzgeber, die Voraussetzungen der Strafbarkeit so genau zu umschreiben, dass Tragweite und Anwendungsbereich der Straftatbestände für den Normadressaten schon aus dem Gesetz selbst zu erkennen sind und sich durch Auslegung ermitteln und konkretisieren lassen.[46] Der Gehilfenbegriff lässt sich durch Auslegung ermitteln. Das Gebot der Gesetzesbestimmtheit geht nicht so weit, dass der Gesetzgeber gezwungen wäre, sämtliche Straftatbestände ausschließlich mit rein deskriptiven, exakt fassbaren Tatbestandsmerkmalen zu umschreiben. Vielmehr sind Generalklauseln oder unbestimmte, wertausfüllungsbedürftige Begriffe im Strafrecht nicht von vornherein verfassungsrechtlich zu beanstanden, um der Mannigfaltigkeit des Lebens Herr zu werden. Zu unterscheiden ist eine unzulässige Analogie zulasten des Täters von einer bloßen Konkretisierung eines Rechtssatzes durch eine Auslegung.[47] Qualifiziert man den IT-Dienstleister als Gehilfen, so wird keine Analogie zum Gehilfenbegriff gebildet, sondern dieser Begriff lediglich – und noch dazu: zu Gunsten des Täterkreises des § 203 Abs. 1 und 2 StGB – ausgelegt.

[41] Vgl. zur Datenschutzproblematik im Hinblick auf Outsourcing-Projekte *Heghmann/Niehaus*, wistra 2008, 161.

[42] *Heymann/Scheja*, in: Redeker (Hrsg.), Handbuch der IT-Verträge, Bd. 3, 5.4 Rn. 18.

[43] *Bierekoven*, in: Redeker (Fn. 42), 7.2 Rn. 17.

[44] *Lensdorf/Mayer-Wegelin/Mantz*, CR 2009, 62 (65).

[45] *Heghmanns/Niehaus*, NStZ 2008, 57 (61 f.); *Lensdorf/Mayer-Wegelin/Mantz*, CR 2009, 62 (64 f.).

[46] Vgl. BVerfGE 71, 108 (114); 87, 209 (223); 105, 135 (153); BVerfG NJW 2008, 3346; BVerfG NJW 2010, 47 (54) und BVerfG NJW 2010, 754; BGH NJW 2004, 2990; BVerfG NJW 2005, 374 (375); *Lackner/Kühl* (Fn. 8), § 1 Rn. 2 m.w.N. aus der Literatur.

[47] BVerfGE 11, 126 (130); BGHSt 24, 40; *Kudlich*, ZStW 115 (2003), 1 (6); *Lackner/Kühl* (Fn. 8), § 1 Rn. 5.

Schließlich sprechen auch allgemeine wirtschaftsstrafrechtliche Erwägungen für die Qualifizierung des externen IT-Dienstleisters als Gehilfe des Outsourcenden. Danach ist eine Delegation bestimmter Aufgaben zulässig, wenn die Delegation genau, speziell und zeitlich begrenzt ist und nur einen Teil der Aufgaben betrifft.[48] Darüber hinaus müssen die Delegationsempfänger die persönliche und fachliche Kompetenz aufweisen.[49] Bei näherer Betrachtung der oben erwähnten vertraglichen Gesichtspunkte ist an einer allgemeinen Zulässigkeit der Delegation nach diesen Kriterien nicht zu zweifeln, da die Auftragsdatenverarbeitung ausschließlich nach Weisungen des Auftraggebers erfolgen muss, der Auftraggeber hierfür geeignet sein muss und der genaue Umfang der Datenverarbeitung bereits zu Beginn der Datenverarbeitung festgelegt wird.

IV. Ergebnis und Ausblick

Damit komme ich zum Ergebnis, dass aus den oben genannten Gründen der IT-Dienstleister als Gehilfe im Sinne des § 203 Abs. 3 S. 2 StGB qualifiziert werden kann, so dass eine Strafbarkeit aus der Sicht des „Outsourcenden" nur dann in Betracht kommt, wenn die strengen Mindestvoraussetzungen des Bundesdatenschutzgesetzes nicht eingehalten werden.[50]

Auch wenn – wie oben aufgezeigt – gute Gründe für die Qualifizierung des IT-Dienstleisters als Gehilfe im Sinne des § 203 Abs. 3 S. 2 StGB sprechen, ist dies für die Praxis kein Grund zur völligen Entwarnung, da die Problematik höchstrichterlich noch nicht geklärt ist. Andererseits kann angesichts der Vielzahl von externen Dienstleistungsangeboten der dringende Bedarf einer juristischen Klärung nicht geleugnet werden. Der sinnvollste Weg, die juristisch unsichere Lage de lege lata zu beseitigen, scheint wohl darin zu bestehen, den Gesetzgeber ins Spiel zu rufen. In diesem Zusammenhang kann dem Vorschlag der Großen Strafrechtskommission des Deutschen Richterbundes zugestimmt werden, § 203 Abs. 3 S. 2 StGB wie folgt zu erweitern: Den in Absatz 1 und S. 1 Genannten stehen ihre berufsmäßig tätigen Gehilfen, ebenso die zu ihrer ordnungsgemäßen Berufsausübung herangezogenen IT-Dienstleister sowie die Personen gleich, die bei ihnen zur Vorbereitung auf den Beruf tätig sind.[51]

[48] Diese Voraussetzungen ähneln im Übrigen den im Gesellschaftsrecht anerkannten Grundsätzen, wonach die Auslagerung bzw. Delegation bestimmter Aufgaben, die dem Vorstand bzw. Geschäftsführer obliegen, an externe Dritte, zulässig ist, wenn originäre Leitungsaufgaben nicht übertragen werden und der Geschäftsleiter die Auswahl- und Einweisungssorgfalt wahrt und schließlich den Delegationsempfänger überwacht; vgl. zur grundsätzlichen Zulässigkeit der Delegation bestimmter Aufgaben an externe Dritte LG Darmstadt AG 1987, 218 (220); für das Aktienrecht: *Spindler*, in: Goette/Habersack (Hrsg.), Münchener Kommentar zum Aktiengesetz, 3. Aufl. 2008, § 76 Rn. 19 ff., 26; *Fleischer*, in: Spindler/Stilz (Hrsg.), Aktiengesetz, Kommentar, § 76 Rn. 60, 66 ff.; allgemein zur Delegation von Organpflichten eingehend *Schmidt-Husson*, in: Hauschka (Hrsg.), Corporate Compliance, 2. Aufl. 2010, § 7.

[49] Vgl. *Tiedemann*, Wirtschaftsstrafrecht, Einführung und Allgemeiner Teil, 3. Aufl. 2010, Rn. 239.

[50] Die Frage, wie das angesprochene Problem aus der Perspektive des türkischen Rechts behandelt wird, wurde an die Diskussionsrunde im Anschluss des Vortrags weitergereicht.

[51] Große Strafrechtskommission des Deutschen Richterbundes, Auslagerung von Dienstleistungen durch Berufsgeheimnisträger und Datenaustausch zwischen Behörden, S. 117.

Der Videostream und seine urheberstrafrechtliche Bewertung

Von Wiss. Mitarbeiter **Mustafa Temmuz Oğlakcıoğlu**, Erlangen

I. Das Urheberrecht im Wandel der Zeit

Kein anderes Rechtsgebiet wird vom technischen Fortschritt so beeinflusst und fordert deswegen auch derart kontinuierlich gesetzgeberische Reaktionen heraus wie das Urheberrecht. Das digitalisierte Fernsehen von heute hat fast nichts mehr mit der Medienlandschaft der Neunziger Jahre gemein[1] und zeichnet sich v.a. durch erhöhte Flexibilität aus.[2] Dies äußert sich zum einen in der abnehmenden „Verkörperlichung" der Werke: Der Umlauf urheberrechtlich relevanter Inhalte erfolgt über die „nackte Datei" und „klebt" nicht mehr zwingend an einem bestimmten Träger (sodass auch nicht mehr das Medium – die Kassette, die CD, die DVD – als Einheit vervielfältigt werden muss, wenn eine Kopie erwünscht ist).[3] Flexibler ist zum anderen auch der „Filmgenuss" selbst geworden, da nun die Möglichkeit besteht, Filme, Dokumentationen und Kinderprogramme auf Abruf ansehen zu können. Außerdem ist die Sendung (urheberrechtlich geschützter Werke) dank der fortschreitenden Entwicklung des Internetangebots und kabelloser Netzwerke nicht mehr an das Medium „Fernseher" gebunden; vielmehr kann auch vom heimischen PC, Laptop, Tablet-PC oder Smartphone jederzeit und überall auf die gewünschte Sendung zugegriffen werden.[4] Inzwischen muss man nicht einmal mehr im „Besitz" einer nackten Datei sein,[5] vielmehr kann die Sendung wie im Fernsehen direkt angesehen werden. Die hierbei verwendete Technik, welche u.a. auch bei YouTube, Clipfish und MyVideo zur Anwendung kommt, ist das sog. „Streaming-Verfahren".

Die mit dieser Technik einhergehende Flexibilität vereinfacht aber auch die Verletzung fremder Urheberrechte. User von Videoportalen können ohne besondere Hürden Musiktitel, Filme und sonstige Werke anderer schlicht hochladen und somit einem millionenfachen Publikum zugänglich machen. Während die Urheberrechtswidrigkeit derartiger Verbreitungen und auch deren Strafbarkeit wohl außer Frage steht,[6] wird derzeit nach wie vor darüber diskutiert, ob auch die „Zuschauer" urheberrechtswidrig handeln bzw. sich sogar strafbar machen, wenn sie mittels der Streaming-Technik auf offensichtlich rechtswidrige Quellen zugreifen, also „urheberrechtswidrig fernsehen". Dass auch dieser Personenkreis (die Nutzer) ins Visier der Ermittler gerückt ist, überrascht in Zeiten der Instrumentalisierung des Strafverfahrens für zivilrechtliche Schadensersatzansprüche nicht:[7] Wenn nach geltendem Recht der „Download zum Eigengenuss",[8] sprich auch derjenige erfasst wird, der sich eine Filmdatei herunterlädt, anschaut und wieder löscht, liegt es zumindest auf den ersten Blick nahe, auch denjenigen haften zu lassen, der sich die Datei direkt ansieht, ohne sie abzuspeichern.

Dass man diese Rechtsfrage häufig am Phänomen „kino.to"[9] aufhängt bzw. mit diesem in Verbindung bringt, mag v.a. dem Umstand geschuldet sein, dass die Popularität derartiger Seiten einerseits, die Etablierung der Streaming-Technik andererseits zeitlich ungefähr zusammenfielen;[10] die auf kino.to erfolgte Verbreitung illegaler Filmkopien in einer noch

[1] Als Stichwörter seien genannt: „Betamax vs. VHS"; die Ablösung der Musikkassette durch die Compact-Disc; Bezahlfernsehen mit einem einzigen Sender (sodass auch die Frage, welches Bundesligaspiel am Samstag übertragen wird, von der „Wichtigkeitseinschätzung" der Regie abhing; eine Vorstellung, die in Zeiten der Konferenzschaltung dem einen oder anderen FC Nürnberg-, Eintracht Frankfurt- oder SC Freiburg-Fan einen kalten Schauer über den Rücken laufen lässt).

[2] Zu diesen Überlegungen auch *Neurauter*, GRUR 2011, 691.

[3] Vgl. *Gruhl*, in: Müller-Gugenberger/Bieneck (Hrsg.), Wirtschaftsstrafrecht, 5. Aufl. 2011, § 55 Rn. 105.

[4] Zur DSL-Verbindung als viertem, neuen „Rundfunkübertragungsweg vgl. *Neurauter*, GRUR 2011, 691, der in diesem Zusammenhang auch auf den neuen „Trend zur Selbstverwertung" und der Abnabelung größerer Fernsehgesellschaften wie RTL von GEMA und Co. hinweist.

[5] Zu dieser Erkenntnis vgl. auch *Borghi*, International Review of Intellectual Property and Competition Law 2011, 316 (346).

[6] *Stieper*, MMR 2012, 12; *Busch*, GRUR 2011, 496; *Dreier*, in: Dreier/Schulze, Urheberrechtsgesetz, Kommentar, 3. Aufl. 2008, § 19a UrhG Rn. 10. Fraglich kann allerdings sein, inwiefern die Betreiber für Fremdinhalte haften, indem sie Framelinks setzen bzw. diese dulden, vgl. hierzu *Ullrich*, ZUM 2010, 853.

[7] Monographisch *Schäfer*, Die Bedeutung des Urheberstrafverfahrensrechts bei der Bekämpfung der Internetpiraterie, Instrumentalisierung des Strafverfahrens zur Durchsetzung urheberzivilrechtlicher Interessen, 2010, passim.

[8] Dieses aus dem Betäubungsmittelrecht übernommene Bild sei an dieser Stelle sogleich abgerundet (auch wenn damit das Ergebnis in gewissem Grade vorweggenommen wird): auch dort ist schließlich der Konsumakt als solcher straflos, während der Erwerb der Drogen zum Eigenkonsum gem. § 29 Abs. 1 BtMG strafbar ist. Begründet wird dies damit, dass beim Erwerb immer noch die abstrakte Gefahr der Weitergabe besteht (wie beim Vervielfältigen einer mpeg4-Datei auf dem Memory-Stick oder dem Brennen einer DVD eben auch), während beim Konsumakt als solches keine fremde – schützenswerte – Rechtsgutsbeeinträchtigung mehr in Betracht kommt. Schließlich soll auch das Vervielfältigungsrecht nach § 16 UrhG als Vorfeldrecht nicht den „illegalen" Genuss des Rezipienten verhindern, sondern einer weiteren Verbreitung gegen den Willen des Urheberrechtsinhabers entgegenwirken; zum Vervielfältigen als Gefährdungsdelikt vgl. *Gruhl* (Fn. 3), § 55 Rn. 104; *Loewenheim*, in: Schricker/Loewenheim (Hrsg.), Urheberrecht, Kommentar, 4. Aufl. 2010, § 16 UrhG Rn. 11, 13; *Dustmann*, in: Fromm/Nordemann, Urheberrecht, Kommentar, 10. Aufl. 2008, § 16 UrhG Rn. 3.

[9] Die Top Level Domain „to" steht für das Pazifikarchipel Tonga, vgl. hierzu *Fangerow/Schulz*, GRUR 2010, 677 (682).

[10] Freilich soll damit nicht suggeriert werden, dass es die Streaming-Technik nicht bereits vorher gab.

nie dagewesenen Form (70.000 Filme, 350.000 Serientitel[11]) und die millionenfachen Klicks, derer sich die Betreiber erfreuen konnten,[12] brachten zudem besonders deutlich zu Tage, dass der Gesetzgeber noch weit entfernt von jenem umfassenden Urheberrechtsschutz war, den er sich mit seinem „Zweiten Korb" als Ziel gesteckt hatte. Hinzu kommt die wirtschaftliche Dimension der illegalen Verbreitung über kino.to, die durch Statistiken des Statischen Bundesamtes zum Vorschein kam, wonach zwischen den Jahren 2003 und 2008 die Zahl der Kinobesucher um 23,63 % zurückgegangen ist (freilich soll damit nicht suggeriert werden, dass das Online-Angebot allein ursächlich für diese Zahlen ist, was v.a. im Hinblick auf die gesamtweltwirtschaftlichen Entwicklungen in diesem Zeitraum bezweifelt werden darf).[13] Im Übrigen ist diese Assoziation missglückt, wenn man bedenkt, dass die bei kino.to zur Verfügung gestellten Inhalte nicht ausschließlich mittels Streaming-Technik zur Verfügung gestellt wurden (teils war auch ein Download als fertige mpeg4-Datei möglich).

Dies sollte gleich im „Vorspann" geklärt werden, da mit den folgenden Ausführungen keine pauschale Einordnung des Besuchens und Nutzens der Seite als legal oder illegal bezweckt wird. Dem folgenden Beitrag, der auf einem Vortrag[14] zum ersten deutsch-türkischen „Cybercrime-Rechtsdialog"[15] basiert, kann im Hinblick auf die (keinesfalls negativ zu bewertende) „Publikationsflut" zum Stream[16] in den Jahren 2010 und 2011 in erster Linie nur die Funktion zukommen, nach einer knappen Erläuterung der rechtlichen (vgl. II.) und technischen Grundbegrifflichkeiten (III.), den bisherigen Stand in der urheberrechtlichen Literatur zusammenzufassen (insb. wie man sich zum Stream und seiner Einordnung unter das Vervielfältigungsrecht des § 16 UrhG verhält bzw. unter welchen Voraussetzungen der Abruf eines Streams als „illegal" bewertet wird). In diesem Zusammenhang gilt es einen Aspekt hervorzuheben, der im Rahmen dieser Debatte nicht immer ausreichend hervorgehoben wurde; nämlich, dass das deutsche Urheberstrafrecht als akzessorische Nebenstrafrechtsmaterie konzipiert ist und folglich durch Begrifflichkeiten „reguliert" und „definiert" wird, die in erster Linie eine umfassende Schadensersatz- und Unterlassungshaftung gewährleisten sollen. Just am 4.10.2011 hat sich der EuGH im Fall „FAPL/Murphy", in dem die Vermarktung der Satellitenübertragung von Fußballspielen durch die Football Association Premier League (FAPL) im Mittelpunkt stand, auch zum Umfang des urheberrechtlichen Vervielfältigungsrechts beim Streaming geäußert.[17] Diese (teils sicherlich überraschenden[18]) Ausführungen zum Stream konnten zwar noch nicht im Rahmen des Vortrags, aber wenigstens nunmehr Berücksichtigung erfahren.[19]

II. Rechtliche Grundlagen: Der strafrechtliche Urheberschutz nach den §§ 106 ff. UrhG

Die §§ 106 ff. UrhG regeln die strafrechtlichen Folgen von Urheberrechtsverletzungen.[20] Strafrechtliche Folgen soll allerdings vorrangig nur die Verletzung von Verwertungsrechten (also das Verbreiten, Vervielfältigen und öffentliche Wiedergeben) haben, während die Beeinträchtigung urheberpersönlichkeitsrechtlicher Befugnisse nur im begrenzten Umfang strafrechtlichen Schutz erfährt (§ 107 UrhG).[21] Der Gesetzgeber hatte schon vor der Etablierung der Streaming-Technik die strafrechtlichen Vorschriften (§§ 106 ff. UrhG) mehrmals verschärft und erweitert, wozu er sich v.a. aufgrund des immer „gefährlicher" werdenden Begehungsorts „Internet" (Stichwort „Tauschbörsen" bzw. „peer-to-peer-Netzwerke"[22]) ver-

[11] Vgl. *Radmann*, ZUM 2010, 387 m.w.N.

[12] Vgl. die Statistik bei www.alexa.com/topsites/countries/DE (15.7.2012).

[13] Vgl. de.statista.com/statistik/daten/studie/2194/umfrage/entwicklung-der-anzahl-der-kinobesucher-in-deutsch-land-seit-1993 (15.7.2012).

[14] Das Symposium fand an der Bilgi Universität in Istanbul im Oktober 2011 statt. Weitere Infos auf: http://www.jura.uni-tuebingen.de/professoren_und_dozenten/vogel/aidp/FlyerIstanbulDt.pdf.

[15] Freilich sind auch dem „Stream" als supranationalem Phänomen und Problem die typischen Fragestellungen des Cybercrime vorgeschaltet: Tatsächlich schon deswegen, weil jede Internetseite von überall aus abrufbar ist und zudem auch in jedem Land spezifische Seiten existieren, die sich an das inländische Publikum richten (was in Deutschland „kino.to" ist, ist in den USA „alluc.org" und in der Türkei „diziizle.net"). Rechtlich führt dies zu den grundsätzlichen Problemstellungen des „Cybercrime", die an dieser Stelle nicht vertieft aufgegriffen werden können (man denke u.a. an die komplexen Zurechnungsfragen bei Verlinkungen im Netz, an die Probleme beim Strafanwendungsrecht oder auch an die strafprozessualen Unzulänglichkeiten, die bei der Verfolgung von internetbezogenen Straftaten auftreten, sei es was die Identifikation, sei es was die regelmäßig fehlende Zuständigkeit der Verfolgungsbehörden über die Grenze hinaus anbelangt).

[16] Vgl. nur *Fangerow/Schulz*, GRUR 2010, 677; *Koch*, GRUR 2010, 574; *Radmann*, ZUM 2010, 387; *Büscher/Müller*, GRUR 2009, 558; *Hullen*, Der IT-Rechts-Berater 2008, 230; *Stieper*, MMR 2012, 12; *Busch*, GRUR 2011, 496; *Neurauter*, GRUR 2011, 691; *Borghi*, International Review of Intellectual Property and Competition Law 2011, 316.

[17] EuGH MMR 2011, 817.

[18] So *Stieper*, MMR 2012, 12.

[19] Insb. die dort gemachten Ausführungen einbeziehend auch *Stieper*, MMR 2012, 12.

[20] Zusammenfassend *Tiedemann*, Wirtschaftsstrafrecht, Besonderer Teil, 3. Aufl. 2011, Rn. 645 ff.; *Hellmann/Beckemper*, Wirtschaftsstrafrecht, 3. Aufl. 2010, Rn. 604 ff.; *Gruhl* (Fn. 3), § 55 Rn. 97; *Eisenmann/Jautz*, Grundriss Gewerblicher Rechtsschutz, 9. Aufl. 2012, Rn. 73n.

[21] Übersicht bei *Heinrich*, in: Joecks/Miebach (Hrsg.), Münchener Kommentar zum Strafgesetzbuch, Band 6/1, 2010, § 106 UrhG Rn. 2.

[22] Vgl. zu diesen Tauschbörsen im Internet *Beck/Kreißig*, NStZ 2007, 304; *Berger*, ZUM 2004, 257; *Bosch/Röhl*, NJW 2008, 1415; *Braun*, GRUR 2001, 1106; *Kreutzer*, GRUR 2001, 193, *ders*., GRUR 2001, 307; *Reinbacher*, GRUR 2008, 394; *Rösler*, MMR 2006, 503.

anlasst sah.[23] Währenddessen wurden immer mehr Stimmen laut, wonach das Urheberstrafrecht auf diesem Wege seinen Charakter als „Ausnahmeinstitut" bei besonders gravierenden Urheberrechtsverstößen verlöre. Stattdessen verkümmere es zu einem alternativen Reaktionsweg, der dazu prädestiniert sei, zur Durchsetzung zivilrechtlicher Schadensersatzansprüche instrumentalisiert zu werden.[24] Der Gesetzgeber ließ sich nicht davon beirren und wollte durch die Novellierungen des Zweiten Korbs im Jahre 2008 insb. auch Downloads von Film- und Musikdateien aus p2p-Netzwerken und Sharehostern (wie RapidShare) erfasst wissen.[25]

Jetzt stehen er und die Rechtswissenschaft mit der Stream-Technik vor einer neuen Herausforderung: schließlich ist diese – wie bereits erläutert – zumindest auf den ersten Blick nicht mit einem Download vergleichbar, da man das Werk (Film, Musik) wie im Fernsehen direkt abspielen und ansehen kann, ohne im „Besitz" eines bestimmten Trägers (gebrannte DVD) oder einer Datei zu sein. Zumindest muss diese nicht erst einmal in ihrer Gesamtheit heruntergeladen werden, um sie wiedergeben zu können. Schließlich war im „analogen Zeitalter" unumstritten, dass die bloße Rezeption (also der Genuss des Werkes) urheberrechtsfrei war, selbst wenn es sich um eine rechtswidrige Kopie handelte (niemand würde auf die Idee gekommen, die gesamten Teilnehmer eines Filmabends wegen des „Schauens" eines Films zu belangen, obwohl diese wissen, dass der Gastgeber den Film in urheberrechtswidriger Weise erlangt hat). Daher überrascht es auch nicht, dass der Stream nicht selbstverständlich bzw. a priori unter die Verwertungsrechte des UrhG subsumiert wurde, sondern die zum Stream erschienenen Abhandlungen sich (sehr ausführlich und differenziert) mit der Technik als solche auseinandersetzen, bevor sie eine urheberrechtliche Bewertung vornehmen.[26]

III. Technische Grundlagen: Die unterschiedlichen Arten des Streams

Man könnte bereits mit den beim Stream zur Anwendung kommenden verschiedenartigen Techniken einen ganzen Beitrag füllen, sodass die folgenden Ausführungen eigentlich nur zur Klärung der Grundbegrifflichkeiten dienen, v.a. aber auch das Bewusstsein dafür schärfen sollen, dass es nicht *den* „Stream" gibt, der einer einheitlichen urheberrechtlichen Betrachtung unterfiele.[27] Der Begriff „Stream" wird allgemein als gleichzeitiges Empfangen und Abspielen von Audio- und/oder Videodaten definiert,[28] wobei eine kontinuierliche Datenübertragung zwischen einem sendenden Server und dem Empfangsgerät stattfindet und die Wiedergabe bzw. Decodierung der empfangenen Daten durch einen Plug-In-Player (ein browserinternes Abspielprogramm in der Funktion eines Client) ermöglicht wird.[29] Kategorisieren lässt sich das Streaming-Verfahren zunächst in zwei Obergruppen, die sich nicht nur in der Technik, sondern bereits im „Wesen" unterscheiden, wie ihr Name bereits vermuten lässt: Dem Stream auf Anfrage (On Demand Stream) und dem sog. Live-Simulcast (bzw. Live-Stream[30]).

Beim On-Demand-Stream werden auf einen Klick des Nutzers Datenpakete vom Server des Anbieters (der seinerseits die Daten auf dem Server „zwischengespeichert" hat) mittels Internet zum Empfangsgerät (Client) transportiert.[31] Die Festlegung erfolgt hierbei auf einem Zwischenspeicher („Cache"), wobei damit auch Schwankungen während der Übertragung vorgebeugt und somit eine fortlaufende Ausgabe des Streams gewährleistet wird.[32] Dies äußert sich im sog. „Buffering"[33] am Anfang der Übertragung[34] (bei YouTube bspw. startet das aufgerufene Video nicht sofort mit dem Beginn der Datenübertragung, sondern verzögert, weil zunächst die ersten Sekunden des Films vollständig in den Zwischenspeicher abgelegt werden. Der hellroten Leiste lässt sich entnehmen bis zu welcher Stelle der Film bereits zwischengespeichert wurde). Im Normalfall dauert die Zwischenspeicherung so lange an, wie der Player im Internetbrowser mit der Wiedergabe als Stream oder pausiert befasst ist.[35]

---

[23] Zusammenfassungen der Historie des Urheberrechts bei *Dreier* (Fn. 6), Einl. Rn. 54-58; *Heinrich* (Fn. 21), Vorb. UrhG Rn. 6.

[24] S.o. Fn. 7.

[25] BGBl. I 2007, S. 2513; hierzu *Zypries*, MMR 2007, 545; *Spindler*, GRUR 2008, 9.

[26] *Stieper*, MMR 2012, 12 (13); *Fangerow/Schulz*, GRUR 2010, 677 (678); *Koch*, GRUR 2010, 574 (575); *Radmann*, ZUM 2010, 387 (388).

[27] Hierzu ausführlich *Kurose/Ross*, Computernetzwerke – Der Top-Down-Ansatz, 4. Aufl. 2008, S. 120 ff. Die Notwendigkeit einer technisch-differenzierten Betrachtung postulieren unter anderem *Heerma*, in: Wandtke/Bullinger, (Hrsg.), Praxiskommentar zum Urheberrecht, 3. Aufl. 2009, § 16 UrhG Rn. 10 (13 f.); *Dustmann* (Fn. 8), § 16 UrhG Rn. 26; *Dreyer*, in: Dreyer/Kotthoff/Meckel (Hrsg.), Urheberrecht, Kommentar, 2. Aufl. 2008, § 16 UrhG Rn. 26, 30; *Loewenheim* (Fn. 8), § 16 UrhG Rn. 21.

[28] *Busch*, GRUR 2011, 496 (497); *Büscher/Müller*, GRUR 2009, 558; *Stieper*, MMR 2012, 12.

[29] Vgl. hierzu näher *Busch*, GRUR 2011, 496 (497).

[30] Soweit es nur um die Kabelweitersendung geht, wäre diese Technik unter dem Oberbegriff „Internetfernsehen" dem WEB-TV zuzuordnen, der sich vom IP-TV dadurch unterscheidet, dass die Übertragungstechnologie nicht an ein *bestimmtes* Netz gebunden ist, wie etwa Zattoo. Die Telekom bspw. dagegen verwendet die leistungsstärkere IP-TV-Technik und verwendet für ihre Übertragung ein eigenes, geschlossenes Netz, wobei sich insb. die Frage stellt, ob bei der Benutzung von Glasfaser- oder Breitbandkabelnetzen eine Kabelweitersendung i.S.d. § 20b UrhG vorliegt, hierzu ausführlich *Neurauter*, GRUR 2011, 691 (692 f.).

[31] Sog. „unicast", vgl. *Koch*, GRUR 2010, 574; *Radmann*, ZUM 2010, 387 (388).

[32] Ausführlich *Busch*, GRUR 2011, 496 (498) m.w.N.

[33] Wobei man die Begrifflichkeiten des „Buffering" und des „Caching" dennoch nicht gleichsetzen darf: Während das „Buffern" Zwischenspeicherung einmaliger Übertragungen betrifft, soll das „Caching" den mehrmaligen Abruf ermöglichen.

[34] *Busch*, GRUR 2011, 496 (498).

[35] *Radmann*, ZUM 2010, 387 (388).

Wurde alles zwischengespeichert, ist auch ein Vor- und Zurückspulen innerhalb des Videos möglich.[36] Anders beim True-On-Demand Streaming, bei dem solch eine Gesamtübertragung nicht stattfindet, d.h. noch während der Übertragung zwischengespeicherte Abschnitte wieder gelöscht werden, wobei Umfang und Vollständigkeit der Zwischenspeicherungen auch vom verwendeten Transportprotokoll (insb. TCP und UDP[37]) abhängen können. Dies schränkt die Vor- und Zurückspulmöglichkeit ein und ist – bspw. bei myvideo.de – daran erkennbar, dass die jeweilige Stelle komplett neu angefordert wird und je nach Bandbreite eine gewisse Ladezeit in Anspruch nimmt.

Soweit die Datei insgesamt zwischengespeichert wird (teils auch Progressive Download genannt[38]), kann sie auch dauerhaft gemacht werden.[39] Dies erfordert allerdings zusätzliche „Vorkehrungen" des Nutzers, wobei zumindest ein Zugriff auf die temporären Systemordner und regelmäßig eine Umbenennung bzw. Verschiebung der Datei notwendig ist. Inzwischen existiert auch Konvertierungssoftware, welche die dauerhafte Speicherung und Umwandlung der gestreamten Datenpakete in einzelne Video- oder Musikdateien durch ein paar einfache „Klicks" ermöglicht (so kann etwa beim YouTubeConverter der Videolink in das Programm kopiert werden, das dann die flv-Stream Datei direkt herunterlädt und für den Nutzer in ein immer wieder abrufbares mp3- bzw. mpeg-Format bringt).[40] Teils werden die Dateien auch als gesamte Datei (im mpeg4- oder avi-Format in der DivX-Kompression) angeboten.[41] Der Speicherprozess als solches kann dann der oben erläuterten Technik entsprechen, d.h. der Nutzer kann sich den Film ansehen, während die Datei mehr und mehr anwächst, bis der ganze Film abgespeichert ist (optional wäre auch ein einfacher Download der gesamten Datei ohne gleichzeitiges Ansehen denkbar). Die Filmdatei bleibt im entsprechenden Ordner auch nach Schließung des Browsers erhalten, sodass ein mehrmaliger Abruf sowie Vor-und Zurückspulen möglich sein kann.

Beim Live-Stream findet naturgemäß eine einmalige Übertragung vom Server an beliebig viele Empfänger statt, wobei die Datenströme nicht bereits auf dem Server „deponiert" sind, sondern ihrerseits mit einer konstanten Rate auf den Server übertragen werden.[42] Aufgrund des konstanten Stroms könnte der Live-Simulcast daher dem Senderecht zugeordnet werden.[43] Dieser Fallgruppe kommt v.a. bei der urheberrechtswidrigen Übertragung von Sportereignissen eine wichtige Rolle zu.[44] Zwar besteht auch hier die Möglichkeit, mittels komplexer Konvertierungssoftware die Datei so zu speichern, dass am Ende der Übertragung eine komplette Datei abgespeichert werden kann. Der Nutzer hat allerdings regelmäßig kein Interesse daran.[45] Jedenfalls müssen auch hier zum Ausgleich etwaiger Schwankungen der Bandbreiten bei der Datenübertragung Abschnitte zwischengespeichert („gepuffert") werden.[46]

IV. Rechtliche Einordnung der Streaming-Technik

1. Die unterschiedlichen Bezugspunkte der urheberrechtlichen Vorschriften – Zivilrechtliche Haftung contra strafrechtliche Sanktion

Für eine urheberstrafrechtliche Relevanz müssten die verschiedenen Spielarten des Streams zunächst einmal „urheberprivatrechtliche" Bedeutung aufweisen. Was schon zivilrechtlich nicht schützenswert ist, kann erst Recht keinen strafrechtlichen Schutz genießen. Solch eine Akzessorietät kennt man auch aus anderen Bereichen des Wirtschaftsstrafrechts, etwa bei der Untreue gem. § 266 StGB.[47] Damit ist man bereits an einen zentralen Punkt der Überlegungen zur strafrechtlichen Bewertung des Streams angelangt. Denn im

[36] Vgl. *Büscher/Müller*, GRUR 2009, 558. Spult man dagegen vor, ohne dass alles zwischengespeichert wurde, erfolgt eine neue Anfrage ab der angeforderten Stelle, das je nach Bandbreite eine gewisse Ladezeit in Anspruch nehmen kann; eine kurzzeitige Unterbrechung ist allein schon aufgrund der Neuanfrage aber unvermeidlich (wobei dann je nach Streaming-Art die „übersprungenen" Teile des Streams nachgeladen werden, oder eben erst gar nicht mehr die Ressourcen beanspruchen).

[37] *Stieper*, MMR 2012, 12 (13); detailliert *Busch*, GRUR 2011, 486 (497), insb. wiederum Bezug nehmend auf *Kurose/Ross* (Fn. 27), S. 311 ff., 645. Während TCP durch eine Empfangsabfrage sicherstellt, dass die gesendeten Pakete ankommen, pumpt UDP ohne Kontrolle die Daten „hinaus", ist dafür aber schneller bzw. leistungsfähiger.

[38] Vgl. *Busch*, GRUR 2011, 496; *Radmann*, ZUM 2010, 387.

[39] *Koch*, GRUR 2010, 574 (575); *Busch*, GRUR 2011, 496 (497).

[40] Die Verbreitung und der Verkauf derartiger Programme müsste dann (die Strafbarkeit des Downloads unterstellt, vgl. noch im Folgenden) unter dem Topos „Anstiftung bzw. Beihilfe durch berufsbedingtes Verhalten" diskutiert werden. Insb. im Hinblick darauf, dass auch eine legale Nutzung des Programms möglich ist (Umwandlung von urheberrechtsfreien Streams), wird eine Teilnehmerstrafbarkeit nach allgemeinen Grundsätzen kaum zu bejahen sein, vgl. hierzu statt vieler *Kudlich*, in: Sieber u.a. (Hrsg.), Strafrecht und Wirtschaftsstrafrecht, Dogmatik, Rechtsvergleich, Rechtstatsachen, Festschrift für Klaus Tiedemann zum 70. Geburtstag, 2008, S. 221 (S. 232).

[41] *Radmann*, ZUM 2010, 387 (389). Freilich sagt aber das Format bzw. das Angebot als Stream oder eben als fertige Datei nichts über die „Rechtmäßigkeit" der Quelle aus. Schließlich dürfte der Privatnutzer bei einer rechtmäßigen Quelle eine Privatkopie gem. § 53 UrhG anfertigen, s.u.

[42] *Busch*, GRUR 2011, 496 (498); *Bullinger*, in: Wandtke/Bullinger (Fn. 27), § 19a UrhG Rn. 34; *Kurose/Ross* (Fn. 27), S. 633.

[43] *Büscher/Müller*, GRUR 2009, 558.

[44] So auch im eingangs zitierten Fall des EuGH, Urt. v. 4.10.2011 – C403/08, C-429/08 (FAPL v. Murphy) = MMR 2011, 817.

[45] Anders bei Live-Übertragungen von Serien oder Filmen, vgl. Fn. 76.

[46] *Stieper*, MMR 2012, 12 (13); *Busch*, GRUR 2011, 496 (498).

[47] *Kudlich/Oğlakcıoğlu*, Wirtschaftsstrafrecht, 2011, Rn. 339.

Übrigen dürfte man auch im Urheberstrafrecht (und das obwohl sich die Vorschriften innerhalb des gleichen Gesetzes befinden) von einer „asymmetrischen" Akzessorietät auszugehen haben. Dies soll heißen: Obwohl die Straftatbestände auf die Begrifflichkeiten und Handlungen des Urheber-„Deliktsrechts" Bezug nehmen (was im Hinblick auf die Ausgestaltung als Nebenstrafrecht nur eine typische Konsequenz ist), so kann die Auslegung der jeweiligen Merkmale durchaus divergieren, nämlich im Hinblick auf die unterschiedlichen Schutzzwecke der Regelungsmaterien, auf das Bestimmtheitsgebot bzw. Analogieverbot und auf den fragmentarischen Charakter des Strafrechts. In zivilrechtlicher Hinsicht erfordert ein umfassender Urheberrechtsschutz eine weite bzw. extensive Auslegung der Merkmale einerseits, eine eher zurückhaltende Anwendung von Schranken andererseits. Im Strafrecht dagegen müssen umgekehrt das Werk als Straftatbestandsmerkmal, die Tathandlungen des Vervielfältigens oder des Verbreitens eher eng ausgelegt werden (während man bei der Anwendung von Tatbestandsausschließungsgründen womöglich großzügiger sein wird). Im Ergebnis besteht schließlich Einigkeit darüber, dass man den Endverbraucher nicht durch ein extensives Verständnis der §§ 106 ff. UrhG in die Kriminalität drängen will. Schließlich ist die Etablierung einer „Schulhofkriminalität"[48] ebenso wenig erwünscht, wie das Fördern einer „Pechvogelmentalität", die einem seriösen Normbefehl eher zuwiderlaufen, als dessen Befolgung fördern würde (v.a. im Hinblick auf die verfolgungsstrukturellen Probleme). Freilich ist es dennoch schief, von einer asymmetrischen Akzessorietät zu sprechen, da die Tathandlungen des § 106 UrhG an anderer Stelle des Gesetzes bereits auftauchen und der Gesetzgeber somit einen einheitlichen Begriffskatalog zugrunde gelegt zu haben scheint. Das Phänomen der sog. „Normspaltung" lässt sich allerdings nicht vermeiden, wenn das UrhG einerseits einen umfassenden zivilrechtlichen Schutz des Urhebers gewährleisten,[49] andererseits als Nebenstrafrechtsmaterie nur flankierende Wirkung haben soll. Strafrecht und Zivilrecht können schlicht nicht pauschal einheitlich definiert werden; die Normspaltung kann dann allerdings nur innerhalb des Zivilrechts erfolgen, d.h.: Grundsätzlich ist das Urheberrecht einheitlich restriktiv auszulegen, während im zweiten Schritt Analogien und extensive Auslegung bei zivilrechtlichen Fragestellungen ohnehin nicht als kritisch zu betrachten sind. Daher kann die meist schon im Urheberprivatrecht strittige Auslegung eines bestimmten Merkmals (bspw. der offensichtlich rechtswidrigen Vorlage) nicht präjudiziell für das Strafrecht sein, vielmehr steckt das Strafrecht die „Mindestgrenzen" zivilrechtlicher Haftung ab. Dies ergibt sich schon daraus, dass alle im Haftungstatbestand genannten Merkmale (insb. auch die Merkmale der Schrankenregelungen) zugleich Vorsatzbezugspunkte darstellen, da eine fahrlässige Verletzung fremder Verwertungsrechte nicht unter Strafe gestellt ist. Dieser Aspekt der zwei unterschiedlichen Bezugspunkte der urheberrechtlichen Vorschriften wird i.R.d. folgenden Ausführungen immer wiederkehren.

[48] Vgl. hierzu *Köhler/Arndt/Fetzer*, Recht des Internet, 6. Aufl. 2008, S. 195.

[49] Vgl. nur *Lettl*, Urheberrecht, 2008, S. 172.

2. Der Stream als urheberrechtliche Vervielfältigung gem. § 16 UrhG

Unproblematisch handelt es sich bei Film und Musik, die der Nutzer abruft, um Werke i.S.d. § 2 Abs. 1 Nr. 6 UrhG.[50] Im Hinblick auf die Nutzer kommt hier nur ein Eingriff in das Vervielfältigungsrecht des Berechtigten gem. § 16 UrhG in Betracht, da im Gegensatz zu Tauschbörsen nicht zeitgleich urheberrechtlich relevante Inhalte hochgeladen werden. Im Allgemeinen wird unter Vervielfältigung jede körperliche Festlegung eines Werkes verstanden, die geeignet ist, das Werk den menschlichen Sinnen auf irgendeine Weise unmittelbar oder mittelbar wahrnehmbar zu machen.[51] Hierbei ist es unerheblich, ob die Festlegung auf Dauer erfolgt, was sich bereits aus der Existenz des § 44a UrhG ergibt (näher dazu weiter unten), welcher der Umsetzung der EG-Richtlinie 2001/29/EG[52] dient.[53] Ebenso wenig kommt es darauf an, auf welche Art und Weise die Wahrnehmbarmachung ermöglicht wird und ob hierfür ggf. bestimmte Zwischenschritte notwendig sind.[54] Im Zusammenhang mit diesem extensiven Vervielfältigungsbegriff wird häufig darauf hingewiesen bzw. klargestellt, dass die bloße Anzeige als solche (auf dem Bildschirm) noch keine Vervielfältigung darstelle.[55] Allerdings handelt es sich bei den Zwischenspeicherungen beim Progressive Download oder dem „Caching" i.R.d. Betrachtens von YouTube-Videos jedenfalls um Vervielfältigungen i.S.d. § 16 UrhG, wenn das Werk am Ende in seiner Gesamtheit zwischengespeichert, also in einer (temporären) Datei zusammengefasst wird.[56]

Problematischer wird es beim True-Streaming, da dort Teile des Gesamtwerkes schon während der Wiedergabe wieder gelöscht werden und die einzelnen Partikel des Films allenfalls Teilvervielfältigungen darstellten, die nur dann urheberrechtlichen Schutz genießen, wenn sie für sich schöpferischen Inhalt i.S.d. § 2 Abs. 2 UrhG aufweisen.[57] Fraglich ist also beim True-Stream nicht, ob eine Vervielfältigung vorliegt, sondern ob überhaupt ein schützenswertes „Werk" angenommen werden kann. Bei Streaming-Datenpartikeln in der Länge von wenigen Sekunden könnte eine Überschreitung der sog. „Schöpfungshöhe" gem. § 2 Abs. 2 UrhG niemals

[50] Zum Werkbegriff des § 2 Abs. 1 Nr. 6 UrhG vgl. *Bullinger* (Fn. 42), § 2 UrhG Rn. 112 m.w.N.

[51] Vgl. hierzu *Schulze*, in: Dreier/Schulze (Fn. 6), § 16 UrhG Rn. 6 m.w.N.; aus der Rechtsprechung BGHZ 17, 266 (270).

[52] Auch als InfoSoc-RL bezeichnet und im Internet abrufbar.

[53] *Fangerow/Schulz*, GRUR 2010, 677; *Stieper*, MMR 2012, 12 (13).

[54] *Heerma* (Fn. 27), § 16 UrhG Rn. 2 f.

[55] *Heerma* (Fn. 27), § 16 UrhG Rn. 13 m.w.N.

[56] *Busch*, GRUR 2011, 496 (499); *Löwenheim* (Fn. 8), § 16 UrhG Rn. 21; *Schulze* (Fn. 51), § 16 UrhG Rn. 13; *Stieper*, MMR 2012, 12 (14); *Heerma* (Fn. 27), § 16 UrhG Rn. 16.

[57] *Loewenheim* (Fn. 8), § 16 UrhG Rn. 14; *Dreyer* (Fn. 27), § 16 UrhG Rn. 15; *Dustmann* (Fn. 8), § 16 UrhG Rn. 16; BGH GRUR 1953, 299; *Schulze* (Fn. 51), § 16 UrhG Rn. 9.

bejaht werden[58] (wobei man auch herausstellen muss, dass eine Pufferung von unter zwei Sekunden technisch keinen Sinn macht).[59]

Um den Schutz daher nicht von der verwendeten (und manipulierbaren) Technik abhängig zu machen, wird in der Literatur ein normativer Vervielfältigungsbegriff vorgeschlagen:[60] Dementsprechend soll bei sukzessiven, chronologisch geordneten Teilvervielfältigungen der Tatbestand des § 16 UrhG bejaht werden können, wenn bei wertender Betrachtung letztlich doch eine Vervielfältigung des ganzen Werkes erfolgt. Dem ist entgegenzutreten, da eine solche wertende Betrachtung eine körperliche Festlegung des Werks zulasten des Nutzers fingieren würde. Beim True-Stream müsste also festgestellt werden, ob die gestreamten Partikel für sich bereits urheberrechtlich relevanten Inhalt aufweisen. In diese Richtung tendiert auch der EuGH in seiner eingangs zitierten Entscheidung „FAPL/Murphy", wenn er eine Vervielfältigung i.S.d. Art. 2 Info-RL (der nach h.M. als Unionsrecht verbindlich die äußersten Grenzen des Schutzes festlegt)[61] von der Frage abhängig macht, ob das „zusammengesetzte Ganze" (gemeint ist seinerseits das Teilfragment, nicht das gesamte Werk!) schutzfähige Elemente i.S.e. eigenen geistigen Schöpfung enthält.[62]

Freilich darf diese Streitfrage nicht überbewertet werden, da auch kleinere Partikel des Werks jedenfalls unter das Leistungsschutzrecht des Urhebers gem. §§ 85, 94, 95 UrhG fallen (die eben nicht die individuell-schöpferische Arbeit, sondern die organisatorisch-wirtschaftliche Leistung der Aufzeichnung schützen). Wie *Stieper* hervorhebt, bestehen Kinofilme aus 24 Einzelbildern pro Sekunde, sodass die Zwischenspeicherung beim Stream (auch nur beim 1-Second-Stream) über die Aufnahme einzelner Lichtbilder hinausgeht.[63] Auf den Punkt gebracht: Kann nicht nachgewiesen werden, dass die Zwischenspeicherung mehr als einige Sekunden angedauert (und somit die Schöpfungshöhe überschritten worden ist), kann jedenfalls ein Eingriff in das Leistungsschutzrecht bejaht werden.[64] In allen anderen Fällen liegt ohnehin ein Eingriff in das Vervielfältigungsrecht vor.

Da der Täter durch seinen „Klick auf Play" diese Vervielfältigungen verursacht, wäre bei unbefangener Betrachtung ein „Vervielfältigen" i.S.d. § 106 UrhG auch erst einmal anzunehmen. Dies bedeutet allerdings noch nicht, dass der Nutzer aus strafrechtlicher Perspektive auch tatbestandlich gehandelt hat.

3. Schranken des Vervielfältigungsrechts

Das Vervielfältigungsrecht i.S.d. § 16 UrhG ist – wie alle Verwertungsrechte des Urhebers – nicht schrankenlos gewährleistet. Im Bezug auf die strafrechtlichen Vorschriften fungieren die Schrankenregelungen des UrhG zeitgleich als Tatbestandsausschließungsgründe. Als einschlägige Schranken kommen hier insb. § 44a UrhG (vorübergehende Vervielfältigungen) und die Kopie zum Eigengebrauch gem. § 53 UrhG in Betracht.

a) Der Stream als vorübergehende Vervielfältigung, § 44a UrhG

Die im Jahre 2003 eingefügte Schrankenregelung des § 44a UrhG hat die Funktion, den weitreichenden Vervielfältigungsbegriff des § 16 UrhG angemessen einzuschränken.[65] Sie soll dem Umstand Rechnung tragen, dass im digitalen Zeitalter der Genuss des Werkes (und der damit einhergehende Verarbeitungsprozess) u.U. bereits für sich eine „Vervielfältigung" erfordert. Kurzzeitige, vorübergehende Vervielfältigungen als integraler Bestandteil eines technischen Verfahrens sollen ausgeklammert werden, wenn sie lediglich eine rechtmäßige Nutzung ermöglichen sollen und keine eigenständige wirtschaftliche Bedeutung haben.

aa) Vorübergehende Vervielfältigung

Somit fallen schon einmal alle „Streams" aus dem Raster, die durch Handlungen des Nutzers dauerhaft gemacht wurden (Klick auf „Speichern unter"); eine andere Frage ist, ob derartige „Downloads" bzw. Kopien von § 53 UrhG erfasst sind (dazu noch bb). In allen anderen Fällen dient die Zwischenspeicherung beim Stream nur dazu, Schwankungen der Übertragungsrate auszugleichen und ist somit integraler und wesentlicher Bestandteil eines technischen Verfahrens. Entscheidend bleibt somit, ob diese Technik eine „rechtmäßige Nutzung" ermöglicht, ohne „eigenständige wirtschaftliche Bedeutung" zu haben.

bb) Rechtmäßige Nutzung

Der Wortlaut der Vorschrift ist, was die Wendung „rechtmäßige Nutzung" anbelangt, etwas missglückt. Jedenfalls kann damit nicht der deklaratorische Verweis auf die übrigen Schranken des UrhG gemeint sein, da § 44a UrhG selbst als Schrankenregelung ausgestaltet ist und solch ein Verständnis dazu führen würde, dass die Handlung dann ohnehin aufgrund anderer Schranken erlaubt wären (solch eine inhaltsleere Regelung wird nicht gewollt sein).[66] Daher geht die h.M. davon aus, dass damit über die Schranken des UrhG hinaus

[58] Hierzu ausführlicher *Busch*, GRUR 2011, 496 (499).
[59] *Stieper*, MMR 2012, 12 (14).
[60] *Busch*, GRUR 2011, 496 (499) m.w.N.
[61] BGH GRUR 2009, 840 („Maximalschutz").
[62] EuGH MMR 2011, 817 (823 Rn. 157, 159).
[63] *Stieper*, MMR 2012, 12 (14).
[64] Lediglich beim Live-Simulcast fallen organisatorisches „Aufzeichnen" und „Senden" zusammen, weswegen die h.M. beim „Simulcasting" kein Vorgehen gegen die Speicherung kleinster Teile ihrer Funksendungen zulässt, vgl. *Stieper*, MMR 2012, 12 (14); so auch *Dreier* (Fn. 6), § 87 UrhG Rn. 12; *Busch*, GRUR 2011, 496 (500).

[65] *Heinrich* (Fn. 21), § 106 UrhG Rn. 80; *Dreier* (Fn. 6), § 44a UrhG Rn. 1; *Wiebe*, in: Spindler/Schuster (Hrsg.), Recht der elektronischen Medien, Kommentar, 2. Aufl. 2011, § 44a UrhG Rn. 1; *v. Welser*, in: Wandtke/Bullinger (Fn. 65), § 44a UrhG Rn. 1.
[66] Vgl. hierzu KG MMR 2004, 540 (544); *Lauber/Schwipps*, GRUR 2004, 293 (295); *v. Welser* (Fn. 65), § 44a UrhG Rn. 20; *Fangerow/Schulz*, GRUR 2010, 677 (681); *Busch*, GRUR 2011, 496 (502).

existente gesetzgebungstechnische, systematische oder verfassungsrechtliche „Schranken" gemeint sein müssen.[67] An dieser Stelle wird daher diskutiert, ob nach dieser Vorschrift der rezeptive Werkgenuss ausgeklammert wird.

Schließlich scheint § 44a Abs. 1 Nr. 2 UrhG perfekt auf den Stream zu passen (Nr. 1 scheitert bereits daran, dass sie nur den Vermittler und nicht den Nutzer privilegiert), soll die Vorschrift ja auch laut Kommentarliteratur insb. Browsing- und Caching-Prozesse erfassen.[68] Man soll sich nicht dem Vorwurf urheberrechtswidrigen Handelns ausgesetzt sehen, bevor man die Urheberrechtswidrigkeit der Seite überhaupt wahrnehmen konnte. Insofern spricht einiges dafür (insb. der eingangs erläuterte Aspekt, dass im analogen Zeitalter urheberrechtswidriges Fernsehen nicht zu einer Haftung führte), den Stream stets unter den § 44a Abs. 1 Nr. 2 UrhG zu subsumieren.

Dennoch gibt es einige Stimmen, welche den Stream als Sonderfall des rezeptiven Werkgenusses nicht unter diese Vorschrift subsumieren wollen: Die Grundlage der Urheberrechtsfreiheit des rezeptiven Werkgenusses sei inzwischen weggefallen, weil sie auf einem funktionierenden Stufensystem zur mittelbaren Erfassung der Endverbraucher basiere.[69] Wenn Partizipation an der Verbreitung zusehends versagt und der Rechteinhaber nicht mehr die Früchte seiner Arbeit ziehen kann, müsse der rezeptive Werkgenuss auch wieder erfasst sein. Daher wird vorgeschlagen, den Rechtsgedanken des § 53 UrhG, wonach offensichtlich rechtswidrige Vorlagen aus dem privilegierten Bereich herausfallen, auf den § 44a UrhG zu übertragen. Zumindest bei offensichtlich rechtswidrigen Vorlagen soll der Nutzer nicht in den Genuss der Privilegierung kommen. Hiergegen wird wiederum eingewandt, dass der Gesetzgeber auch in anderen Fällen des rezeptiven Werkgenusses nicht an die Rechtmäßigkeit der Quelle anknüpft.[70] Dem schließt sich der EuGH in seiner Entscheidung FAPL/Murphy an, wenn er betont, dass nicht die Rechtmäßigkeit der Sendung, sondern die Rechtmäßigkeit des Empfangs maßgeblich sei,[71] dem nichts entgegensteht, soweit kein Verstoß gegen Zugangsregelungen vorliege (was bspw. bei einer Umgehung einer Verschlüsselung angenommen werden kann, vgl. auch § 202a StGB[72]). Alles in allem bleibt der rezeptive Werkgenuss frei, es sei denn, den Zwischenspeicherungen käme eigenständige wirtschaftliche Bedeutung zu.

cc) Keine eigenständige wirtschaftliche Bedeutung

Jedenfalls muss der wirtschaftliche Wert über die Streaming-Leistung hinausgehen. Der Aspekt, dass ohne die Zwischenspeicherung keine verzögerungsfreie Übertragung möglich wäre, genügt daher – auch nach Ansicht des EuGH[73] – nicht, da dieser „Vorteil" in der rechtmäßigen Nutzung (dem Genuss des Werks) aufgeht bzw. dieser immanent ist.[74] Auch allein die Möglichkeit, den Zwischenspeicher dauerhaft zu machen, dürfte i.S.e. „Option" noch nicht ausreichen, um eine eigenständige wirtschaftliche Bedeutung anzunehmen,[75] zumal die Fälle der tatsächlichen Manipulation (gemeint sind die Fälle dauerhafter Speicherung) sowieso aus dem Raster des § 44a UrhG fallen, s.o. Von Relevanz bleiben also nur noch diejenigen Fälle, in denen der Nutzer die Zwischenspeicherung zwar nicht aktiv veranlasst, diese aber über den Client-Nutzungsvorgang hinaus im temporären Speicher erhalten bleibt.[76] Hierbei darf nicht maßgeblich sein, von welchen Parametern die Löschung der temporären Datei abhängt (Schließung des Clients, Herunterfahren des PC, Entfernen des Ordners), sondern ob diese nach einer bestimmten Zeit (wobei die dazwischenliegende Spanne keine 24 Stunden überschreiten sollte) automatisch, also ohne Zutun des Nutzers, gelöscht wird. Ist dies der Fall, scheidet eine tatbestandsmäßige Vervielfältigung gem. § 44a Abs. 1 Nr. 2 UrhG aus.

b) Der Stream als „Privatkopie" gem. § 53 UrhG

Soweit die Vervielfältigung im Client-Puffer erhalten bleibt (der temporäre Ordner also erst durch den Nutzer aktiv gelöscht werden muss)[77] oder – als praktisch wohl wichtigerer Fall – der Täter den Puffer zielgerichtet dauerhaft gespeichert hat[78] (sog. „Stream-Rippen"[79]), kommt immer noch ein Tat-

[67] Differenzierend *Lauber/Schwipps*, GRUR 2004, 293 (295); *Busch*, GRUR 2011, 496 (502), will den Rechtsgedanken des § 53 Abs. 1 UrhG auf § 44a UrhG übertragen und stellt daher auf die offensichtliche Rechtswidrigkeit der Vorlage ab.

[68] *Heinrich* (Fn. 21), § 106 UrhG Rn. 80; *v. Welser* (Fn. 65), § 44a UrhG Rn. 1; *Wiebe* (Fn. 65), § 44a UrhG Rn. 3.

[69] Zu diesen Erwägungen vgl. *Busch*, GRUR 2011, 496 (502); zum Ganzen *Fangerow/Schulz*, GRUR 2010, 677 (681 f.); BVerfGE 31, 255 (267); *Rehbinder*, Urheberrecht, 16. Aufl. 2010, Rn. 10, 299 ff.

[70] *Stieper*, MMR 2012, 12 (16).

[71] EuGH MMR 2011, 817 (823 Rn. 171).

[72] Ob hierzu auch die Umcodierung der IP-Adresse zählt, um zu Angeboten zu gelangen, die im Inland nicht von der GEMA genehmigt worden sind, darf angezweifelt werden.

[73] EuGH MMR 2011, 817 (824 Rn. 179).

[74] Dagegen spricht auch der Zweck von Art. 5 Abs. 1 Info-RL, auf der § 44a UrhG beruht und der eben die Entwicklung und den Einsatz neuer Technologien – sprich die Digitalisierung – ermöglichen soll, ohne stets eine Vervielfältigung i.S.d. § 16 UrhG annehmen zu müssen, vgl. *Stieper*, MMR 2012, 12 (16).

[75] Krit. auch *Busch*, der einer wirtschaftlichen Bedeutung nur aufgrund der Möglichkeit des „Vor- und Zurückspulens" ebenfalls kritisch gegenübersteht, allerdings im Folgeschritt diese Frage mit dem der rechtmäßigen Nutzung verknüpft bzw. vermengt, vgl. *Busch*, GRUR 2011, 496 (501 f.).

[76] So im Ergebnis auch *Stieper*, MMR 2012, 12 (16).

[77] Wobei man aus strafrechtlicher Sicht dem Täter (zumindest dann, wenn er die nach wie vor existente Zwischenspeicherung erst im Nachhinein erkennt) die Nichtaufhebung eines urheberrechtswidrigen Zustands vorwerfen würde und es somit fraglich ist, ob im Hinblick auf § 13 StGB eine Unterlassungsstrafbarkeit in Betracht kommt. Zwar könnte man eine Ingerenzgarantenstellung wegen pflichtwidrigem Vorverhalten bejahen, doch würde man auf ein vollständig anderes Unrecht (Besitz einer durch aktives Tun verursachten urheberrechtswidrigen Vervielfältigung) abstellen.

[78] Zur Aufnahme von illegalen Live-Streams (etwa wenn eine Serie „gesendet" und nicht als On-Demand-Stream angeboten wird) vgl. *Stieper*, MMR 2012, 12 (17).

bestandsausschluss gem. § 53 UrhG in Betracht.[80] Nach dieser Vorschrift sind gewisse Vervielfältigungen zum privaten und zum sonstigen eigenen Gebrauch ohne Zustimmung des Urhebers gestattet. Da ein umfassendes Verbot weder angemessen noch praktikabel erscheint, legt die Vorschrift im Allgemeininteresse die erlaubnisfreie Kopie urheberrechtlich geschützter Werke fest.[81] Als Ausgleich für die zustimmungsfreie Beeinträchtigung des Vervielfältigungsrechts sieht das Gesetz eine Vergütung für Kopiergeräte und Leerträger vor (§§ 54 Abs. 1, 54c Abs. 1 UrhG). Da es den Nutzern von kino.to, YouTube etc. regelmäßig nur auf den privaten Filmgenuss ankommt (und sie nicht etwa eine vergütete Filmkritik schreiben wollen), dürfte es sich um eine Privatkopie i.S.d. § 53 UrhG handeln.[82] Doch hat der Gesetzgeber die Zulässigkeit der Privatkopie an die Rechtmäßigkeit der Vorlage gekoppelt. Die Kopie ist nicht von § 53 UrhG gedeckt und folglich rechtswidrig, wenn die Vorlage ihrerseits offensichtlich rechtswidrig hergestellt oder zumindest offensichtlich rechtswidrig öffentlich zugänglich gemacht wurde.[83] Der Kopierende muss nicht Eigentümer des Originals sein. Strittig ist indessen, ob die Vorlage ihrerseits eine rechtmäßig hergestellte Kopie darstellen kann. Ebenfalls diskutiert wird, ob sich die Vorlage im rechtmäßigen Besitz des Kopierenden befinden muss. All diese Fragen können zumindest bei kino.to (nunmehr kinox.to) dahinstehen, da die Betreiber dieser Seite gewerbsmäßig handelten und die Zwischenspeicherung der abrufbaren Filme auf dem Server durch diese ohne Einwilligung des Berechtigten erfolgt. Die Vorlage ist somit jedenfalls rechtswidrig.[84]

Ohnehin wird der Schwerpunkt der Überlegungen stets bei der Frage liegen, ob die Werkvorlage auch „offensichtlich" rechtswidrig ist.[85] An dieser Stelle kommt das Phänomen der unterschiedlichen Auslegungsmöglichkeiten erstmals besonders deutlich zum Vorschein. Stimmen, die einen besonders effektiven Urheberrechtsschutz (im Sinne zivilrechtlicher Haftung) befürworten, legen den Begriff der Offensichtlichkeit weit aus und bejahen ihn, wenn der Nutzer keine oder ungewöhnlich niedrige Preise für die Nutzung zu leisten hat.[86]

Aus strafrechtlicher Sicht erscheint solch eine Auffassung kaum haltbar.[87] Insb. den Kostenfaktor als Indiz heranzuziehen, ist nicht unproblematisch. Schließlich versucht die Musik- und Filmindustrie mit den illegalen Angeboten gleichzuziehen und kalkuliert das Medium Internet mehr und mehr in ihre Vermarktung ein. Dementsprechend mehren sich legale sowie kostenlose Angebote im Internet (die sich aus Werbung und Registrierung auf den entsprechenden Seiten finanzieren). Außerdem hat man vom Internet aus Zugriff auf verschiedene Rechtsordnungen und Anbieter, von denen der Nutzer nicht auf Anhieb wissen muss, ob das abgerufene Video in dem jeweiligen Land urheberrechtsfrei ist bzw. ob der jeweilige User verbreitungsberechtigt ist. In YouTube bspw. gibt es Channels der Interpreten selbst, die als User eigene Inhalte hochladen, dann die Channels der Plattenfirmen, dann solche, die mit den Rechteinhabern Verträge geschlossen haben und die normalen User bzw. „Fake"-User, denen gar keine Rechte eingeräumt worden sind. Auf den ersten Blick ist hier nie erkennbar, in welchem Land der Abruf rechtmäßig ist (es sei denn aufgrund der IP wird der Zugriff automatisch gesperrt) und welcher User rechtmäßig Inhalte hochlädt. Umgekehrt existieren kostenpflichtige Seiten und Downloadangebote, auf denen dennoch urheberrechtswidrige Materialien zur Verfügung gestellt werden. Außerdem wird die Erkennbarkeit der Illegalität durch die Werbung seriöser Unternehmen auf den Seiten kaschiert, denen die Urheberrechtswidrigkeit der dort gemachten Angebote anscheinend selbst nicht bewusst ist.

Da dem Nutzer keine „unerfüllbaren Prüfpflichten" auferlegt werden dürfen, darf nicht allzu schnell von einer Offensichtlichkeit ausgegangen werden, zumindest soweit es um die Eigenschaft des § 53 UrhG als Tatbestandsausschließungsgrund geht. Bei den Angeboten von kino.to müsste man aber selbst bei einem äußerst engen Verständnis von einer „Offensichtlichkeit" des Angebots ausgehen, handelt es sich doch nicht selten um Vorabveröffentlichungen von Filmen, die noch nicht in deutschen Kinos angelaufen sind bzw. nicht als DVD zum Kauf zur Verfügung stehen.[88] Auch bei YouTube dürften die Aufmachung des Videos (schlichter Songtext vor

[79] *Koch*, GRUR 2010, 574 (575) m.w.N.

[80] A.A. *Koch*, GRUR 2010, 574 (577), der darauf hinweist, dass § 53 UrhG bei Verwendung von Ripping-Software per se nicht zur Anwendung kommen darf; zur „Kopie-Sperre" des § 96 Abs. 2 UrhG *Stieper*, MMR 2012, 12 (17).

[81] *Lüft*, in: Wandtke/Bullinger (Fn. 27), § 53 UrhG Rn. 1; *Heinrich* (Fn. 21), § 106 UrhG Rn. 93.

[82] *Fangerow/Schulz*, GRUR 2010, 677 (679).

[83] Zu § 53 Abs. 1 UrhG im Allgemeinen *Aschenbrenner*, ZUM 2005, 145; *Berger*, ZUM 2004, 257; *Braun*, ZUM 2005, 100; *Flechsig*, GRUR 1993, 532; *Grassmuck*, ZUM 2005, 104; *Jani*, ZUM 2003, 842; *Krüger*, GRUR 2004, 204; *Melichar*, ZUM 2005, 119; *Mönkemöller*, GRUR 2000, 663; *Poll*, ZUM 2006, 96; *Stickelbrock*, GRUR 2004, 736.

[84] Dieses Ergebnis kann man schon aus systematischen Gründen nicht dadurch umgehen, dass man auf die zwischenzeitlich rechtmäßige Vervielfältigung gem. § 44a Abs. 1 Nr. 2 UrhG abstellt, die dem endgültigen Speichern vorgeht. § 53 UrhG erfasst wohl gerade keine Vorlagen, die rechtmäßig sind, weil sie ursprünglich nur als „Zwischenspeicherung" gedacht waren. Anderenfalls würde man denjenigen, der die Datei direkt herunterlädt erfassen, während derjenige, der sich erst den Stream ansieht und diesen dann speichert, in den Genuss der Privilegierung kommen soll.

[85] Vgl. hierzu *Stieper*, MMR 2012, 12 (17); *Fangerow/Schulz*, GRUR 2010, 677 (680); *Koch*, GRUR 2010, 574.

[86] *Dreyer* (Fn. 27), § 53 UrhG Rn. 26.

[87] Vgl. etwas detaillierter *Fangerow/Schulz*, GRUR 2010, 677 (680).

[88] Insofern ist *Radmann*, ZUM 2010, 387 (389), jedenfalls zuzustimmen; vgl. auch *Stieper*, MMR 2012, 12 (17); *Lüft* (Fn. 81), § 53 UrhG Rn. 16; *Loewenheim* (Fn. 28), § 53 UrhG Rn. 14c.

einem rosa Hintergrund)[89] und der Nutzername ausreichendes Indiz dafür sein, dass der Channel-Inhaber keine Lizenz für die Zugänglichmachung hat.[90] Viele Nutzer manipulieren das Werk auch so, dass die speziellen Softwareprogramme, die von den YouTube-Betreibern zur Auffindung und Sperrung urheberrechtlich geschützten Materials verwendet werden, versagen, indem sie das Video spiegelverkehrt hineinstellen oder das Lied etwas verlangsamen.[91] Auch dies dürfte als Indiz für die Illegalität der Quelle ausreichen.

V. Vorsatz und Unrechtsbewusstsein

Basierend auf den voranstehenden Überlegungen kommt es beim bloßen Stream (ohne dauerhafte Speicherung) nicht auf den subjektiven Tatbestand an, weil der Täter schon gar nicht den objektiven Tatbestand des § 106 UrhG verwirklicht (sei es, weil es sich nicht um eine offensichtlich rechtswidrige Quelle i.S.d. § 53 UrhG handelt oder sei es, weil bereits § 44a UrhG einschlägig ist). Die häufig zu lesende Floskel, dass die Strafbarkeit des Nutzers regelmäßig am Vorsatz scheitere, ist somit irreführend. Es hat aber seine Richtigkeit, dass auch diese Stufe nicht nur die tatsächlichen bzw. vorsatztypischen Nachweisschwierigkeiten mit sich bringt, sondern rechtlich einige Hürden existieren, was den Inhalt und die Bezugspunkte des Vorsatzes anbelangt. Insb. stellt sich das im Wirtschaftsstrafrecht häufiger auftretende Problem, wie sich Irrtümer über zivilrechtliche Vorfragen auf die Strafbarkeit des Täters auswirken. So mag selbst bei demjenigen („professionellen“) Nutzer, der um derartige Zwischenspeicherungsvorgänge weiß, fraglich sein, ob dessen Wissen um das kurzzeitige Speichern im „Cache“ für eine Bedeutungskenntnis („Parallelwertung in der Laiensphäre“) in Bezug auf das Vervielfältigen ausreichen kann. Was das Unrechtsbewusstsein anbelangt, dürfte dies in gewissem Grade in jedem von uns schlummern, allein schon aufgrund der Nähe von Urheberrechtsverstößen zum achten Gebot („du sollst kein geistiges Eigentum stehlen“). Der Stabilisierung eines einheitlichen Unrechtsbewusstseins wirkt allerdings die Eigenschaft des Urheberrechts als „kontinental parzelliertes Unrecht“ entgegen. Während an einem Ort die gestreamten Inhalte (mit einer entsprechenden IP) frei verfügbar sind, soll in einem anderen Land der kostenlose Stream verbotsbewehrt sein. Vor allem was das urheberrechtswidrige Fernsehen anbelangt braucht es also wohl noch länger, bis sich hier ein allseits akzeptiertes „Unrechtsminimum“ entwickelt hat.

VI. Fazit

Bei Lektüre und Analyse der urheberrechtlichen Literatur fiel auf, dass die meisten Meinungsstreitigkeiten rund um den Stream Resultat des doppelten Bezugspunkts des Urheberrechts sind. Weil man sich gegen das Phänomen der Normspaltung sträubt (das zugegebenermaßen eine Einbuße an verfassungsrechtlicher Bestimmtheit bedeutete), entwickeln sich einerseits Ansichten, die einen extensiven Urheberschutz und somit auch eine weitreichende Kriminalisierung bis hinunter auf den rezeptiven Werkgenuss durch den Nutzer befürworten. Dagegen schränken die Gegenansichten den Urheberschutz insgesamt ein, um die strafrechtliche Verantwortlichkeit einzudämmen. Die momentan „übersichtlichste“ Lösung wäre eine gesetzeszweckorientierte Auslegung des § 44a UrhG, unter die jeder vorübergehende Stream, der nicht als Datei endgültig abgespeichert wurde, zu subsumieren ist. Soweit man allerdings den rezeptiven Werkgenuss zumindest privatrechtlichen Schutz genießen lassen will, betrifft dies nur die zivilrechtliche Haftung und hat keinen Aussagehalt für § 106 UrhG. Schließlich würde es merkwürdig anmuten, die Strafbarkeit des Täters von der Art des „Filmgenusses“ abhängig zu machen: Derjenige, der eine offensichtlich rechtswidrig hergestellte Kopie als Datei bspw. auf einem Memory-Stick „erwirbt“ und selber keine Vervielfältigungshandlungen vornimmt, bliebe in Bezug auf den bloßen Filmgenuss weiterhin straflos, obwohl er sich den Film noch mehrmals mit anderen Freunden ansehen könnte. Dagegen soll derjenige, der sich die Datei im Internet ansieht, ohne nochmals Zugriff auf die Datei zu haben, strafbar sein. Dies kann nicht erwünscht sein.

Rechtspolitisch bleiben noch einige Fragen offen. So stellt sich die berechtigte Frage, ob der „reverse sting“ gegen die Nutzer überhaupt die richtige Option ist: Wird das Austrocknen des Marktes nicht besser dadurch gewährleistet, dass gegen die Einnahmequellen der Streaming-Seiten vorgegangen wird? Jedenfalls würde man Unternehmen und deren Verantwortliche, die bewusst auf derartigen Seiten Werbung schalten und die Kriminalität somit finanzieren, einfacher verfolgen und sanktionieren können.

Schließlich ließe sich auch noch der Überlegung nachgehen, ob der Filmgenuss bzw. der Abruf des Films eine Beteiligung an der (jedenfalls strafbaren) Verbreitung darstellt. Da die Anbieter von kinox.to aber wohl als „omnimodo facturus“[92] einzustufen wären, käme insofern allenfalls eine Beihilfe (soweit für das Angebot nichts bezahlt wurde – wiederum nur in psychischer Form) in Betracht. Aber auch hier

[89] Was seinerseits nicht dafür ausreicht eine neue geistige Schöpfung anzunehmen, vgl. auch Fn. 63.

[90] Wobei man aber auch nicht aus den Augen verlieren darf, das die meisten Interpreten und Urheberrechtsinhaber derartige Plattformen zu Promo-Zwecken benutzen und in eigenen Channels rechtmäßig zur Verfügung stellen. Die Zusammenarbeit mit den jeweiligen Unternehmen führt auch dazu, dass diese die Angebote der Nutzer ständig überprüfen, sodass v.a. bei bekannteren Interpreten wie Beyonce Knowles, Lady Gaga oder Rihanna urheberrechtswidrige Inhalte auf YouTube und Co nun auch wesentlich seltener zu finden sind, als früher (insb. deren „Single-Auskopplungen“ werden von der konkurrierenden Website myvideo.de angeboten). Dann wäre eine „Aufnahme“ derartiger Videos ebenso unbedenklich, wie in analogen Zeiten, als man die Videos seiner Lieblingsbands (etwa Take That oder Backstreet Boys) auf VHS-Kassette aufnahm.

[91] Dieser „Taschenspielertrick“ führt – entgegen verbreiteter Auffassung in einigen Foren – natürlich keinesfalls zu einer eigenen „Schöpfung“, welche die Quelle legal machte.

[92] Zum Begriff des „omnimodo facturus“ *Kühl*, Strafrecht, Allgemeiner Teil, 6. Aufl. 2008, § 20 Rn. 177; *Wessels/Beulke*, Strafrecht Allgemeiner Teil, 41. Aufl. 2011, Rn. 569.

bewegt man sich als Strafverfolgungsbehörde auf dünnem Eis, da beim – ohnehin grundsätzlich strittigen – Konstrukt der psychischen Beihilfe das bloße Dulden bzw. Billigen der Straftat gerade nicht ausreicht, um eine Gehilfenstellung anzunehmen.[93] Die h.M. lehnt eine Strafbarkeit des Erwerbers bzw. Nutzers rechtswidriger Kopien als Teilnahme an der Haupttat „illegales Verbreiten" (ausschließlich im Bezug auf den Erwerb bzw. die Nutzung!) ohnehin ab, da die Verbreitung als Tathandlung ausgestaltet sei, welche die Mitwirkung eines Dritten zwingend voraussetze.[94] Nach allgemeinen Grundsätzen (Stichwort „notwendige Teilnahme"[95]) scheide eine Strafbarkeit a priori aus. Dagegen ließe sich einwenden, dass das Verbreiten für eine Vollendungsstrafbarkeit nicht zwingend den Wechsel der Verfügungsmacht (i.S.d. Inverkehrbringens) voraussetzt, sondern bereits dann angenommen werden kann, wenn dem potentiellen Erwerber das Angebot gemacht wird. Nicht in jedem Fall ist also das Mitwirken des Erwerbers „notwendig", um zu einer Strafbarkeit zu gelangen. Das Problem bleibt also vielmehr der Nachweis der Gehilfentätigkeit als solcher, insb. im Falle von kinox.to, bei dem das Klicken des Einzelnen den Betreibern keinen zusätzlichen Ansporn zur Wiederholung und Fortführung der Straftaten geben dürfte.

[93] Krit. zur psychischen Beihilfe *Hruschka*, JR 1982, 177; zusammenfassend *Kudlich*, Die Unterstützung fremder Straftaten durch berufsbedingtes Verhalten, 2004, S. 369 ff., *ders*., in: v. Heintschel-Heinegg (Hrsg.), Beck'scher Online-Kommentar, Strafgesetzbuch, § 27 Rn. 94; *Kühl* (Fn. 92), § 20 Rn. 226 f.

[94] *Heinrich* (Fn. 21), § 106 UrhG Rn. 131; *Schlüchter*, NStZ 1988, 53 (57); *Hildebrandt*, in: Wandtke/Bullinger (Fn. 27), § 106 UrhG Rn. 44; *Dreier* (Fn. 6), § 106 UrhG Rn. 2; a.A. wohl *Heghmanns*, NStZ 1991, 112 (113).

[95] *Wessels/Beulke* (Fn. 92), Rn. 587.

Analogie und Verhaltensnorm im Computerstrafrecht

Am Beispiel der Datenveränderung (§ 303a StGB und Art. 4 Convention on Cybercrime)

Von Dr. **Jan C. Schuhr**, Erlangen

I. Überblick

1. Analogie als Regelungstechnik

Zahlreiche Tatbestände des Computerstrafrechts sind zustande gekommen, indem der Gesetzgeber sich einen „klassischen" Deliktstatbestand, der nichts mit elektronischer Datenverarbeitung zu tun hat, als Vorbild nahm und in Analogie dazu einen neuen Tatbestand des Computerstrafrechts erließ. Die folgenden Überlegungen werden sich mit diesem Einsatz von „Analogie als Regelungstechnik" im Computerstrafrecht beschäftigen. Sie beschränken sich auf den vermeintlich unproblematischen Fall, dass der Gesetzgeber den mittels Analogie entwickelten Tatbestand im Gesetz selbst ausformuliert. Es geht nicht um Analogieschlüsse, die der Rechtsanwender von sich aus zieht, und nur am Rande um solche, die der Gesetzgeber ausdrücklich vom Rechtsanwender verlangt.

Das im deutschen Recht sicher geläufigste Beispiel einer gesetzlichen Analogie ist § 263a StGB (Computerbetrug). Dort spricht der BGH ausdrücklich von einer „betrugsspezifischen Auslegung".[1] In der Cybercrime-Convention des Europarats[2] hat Art. 8 („Computer-related fraud") eine ganz entsprechende Struktur und Überschrift.

Am stärksten ausgeprägt ist diese Verwendung der Analogie wohl im Tatbestand der Fälschung beweiserheblicher Daten (§ 269 StGB). Dessen Tatobjekt sind Daten, bei deren Wahrnehmung eine Urkunde vorläge. Hier wird die Analogie bis auf die Tatsachenebene hinabgezogen, so dass letztlich doch dem Richter und anderen Rechtsanwendern ein eigener (wenngleich im Gesetz angeordneter) Analogieschluss abverlangt wird. Das ist wiederum in Art. 7 der Cybercrime-Convention („Computer-related forgery") ganz ähnlich.

Die Liste dieser Beispiele ließe sich fortsetzen. Sie finden sich sowohl im deutschen StGB als auch in den Strafgesetzbüchern vieler anderer Länder. Beispiele ließen sich ebenso außerhalb des Computerstrafrechts finden. Zu älteren Tatbeständen analog konstruierte Tatbestände sind zwar für strafrechtliche Regelungen des Umgangs mit neuen Techniken und damit gerade für das Computerstrafrecht charakteristisch. Deshalb betreffen Fragen dieser Regelungstechnik das Computerstrafrecht besonders und ist umgekehrt das Computerstrafrecht der prädestinierte Ort zur Untersuchung des Einsatzes von Analogie als Regelungstechnik. Die gefundenen Ergebnisse betreffen aber letztlich das ganze Strafrecht.

2. Gegenstand der folgenden Überlegungen

Diese vom Gesetzgeber selbst formulierte Analogie wird im Folgenden näher untersucht werden. Zunächst (unten II.) werden Wert, Nutzen und Grenzen dieser Regelungstechnik dargestellt. Das liefert die Grundlage für eine Analyse von Fehlerbeispielen (unten III.). Sie entstammen dem Tatbestand der Datenveränderung. Schon seit längerer Zeit wird von namhaften Vertretern vorgetragen und überzeugend begründet, dass die deutsche Vorschrift (§ 303a StGB) verfassungswidrig unbestimmt ist.[3] Zu den nötigen praktischen Konsequenzen hat dieser Befund indes noch nicht geführt. Die vermeintlichen Fortschritte bei der Interpretation des Tatbestandes[4] beruhen darauf, dass sowohl die technischen Gegebenheiten als auch die rechtliche Situation außerhalb des Strafrechts in verzerrender Weise ausschnittartig wahrgenommen werden. In dieser Fehlentwicklung manifestiert sich das Scheitern der mit § 303a StGB versuchten Analogie. Um dieser Entwicklung entgegenzusteuern, sind die zugrundelie-

[1] Vgl. BGHSt 47, 160 (162 f.); BGH NStZ 2005, 213; BGH NJW 2008, 1394, die sich jeweils auf die Grundsatzentscheidung BGHSt 38, 120 (124) stützen. Diese Wendung bezieht sich zwar grundsätzlich auf den ganzen § 263a StGB, ist aber vor allem für die Variante der unbefugten Verwendung von Daten von Bedeutung. Die Anlehnung an den Betrug (§ 263 StGB) ist schon anhand der systematischen Stellung offensichtlich und wurde im Gesetzgebungsverfahren auch reflektiert (insb. BT-Drs. 10/318, S. 19). Zu einer Analyse der dort gewählten Gesetzgebungstechnik und ihrer Fehler siehe z.B. *Lackner*, in: Jescheck (Hrsg.), Festschrift für Herbert Tröndle zum 70. Geburtstag am 24. August 1989, 1989, S. 41, und *Schuhr*, ZWH 2012, 48, jeweils m.w.N.

[2] Convention on Cybercrime v. 23.11.2001 = ETS Nr. 185, in Kraft getreten am 1.7.2004, von der Bundesrepublik Deutschland unterzeichnet am 23.11.2001, ratifiziert am 9.3.2009 und in Deutschland in Kraft getreten am 1.7.2009 gemäß Gesetz v. 5.11.2008 (BGBl. II 2008, S. 1243; BGBl. II 2010, S. 218). Von der Türkei wurde die Konvention am 10.11.2010 unterzeichnet, aber noch nicht ratifiziert. Sie ist in Kraft getreten u.a. für Frankreich, Italien, Spanien, das United Kingdom und die USA. Eine vollständige Aufstellung der bereits teilnehmenden Staaten, der Konventionstext und weitere Materialien sind unter http://conventions.coe.int/ (12.7.2012) abrufbar, unter http://www.coe.int/tcy (12.7.2012) sind weiterführende Informationen des Convention Committee on Cybercrime abrufbar.

[3] *Welp*, IuR 1988 Sonderheft, 434 (439) unter Verw. auf *Samson*; *Meinhardt*, Überlegungen zur Interpretation von § 303a StGB, 1991, S. 88 ff., insb. S. 166; *Tolksdorf*, in: Jähnke/Laufhütte/Odersky (Hrsg.), Strafgesetzbuch, Leipziger Kommentar, Bd. 8, 11. Aufl. 2005, § 303a Rn. 7 (anders nunmehr in der 12. Aufl. *Wolff*); *Zaczyk*, in: Kindhäuser/Neumann/Paeffgen (Hrsg.), Nomos Kommentar, Strafgesetzbuch, Bd. 2, 3. Aufl. 2010, § 303a Rn. 4; *Popp*, in: Leipold/Tsambikakis/Zöller (Hrsg.), AnwaltKommentar StGB, 2011, § 303a Rn. 3; *Maurach/Schroeder/Maiwald*, Strafrecht, Besonderer Teil, Bd. 1, 10. Aufl. 2009, § 36 Rn. 35; *Weber*, in: Arzt/Weber/Heinrich/Hilgendorf, Strafrecht, Besonderer Teil, 2. Aufl. 2009, § 12 Rn. 48 Fn. 55; *Guder*, Computersabotage (§ 303b StGB), 2000, S. 234.

[4] Vgl. z.B. *Wolff*, in: Laufhütte/Rissing-van Saan/Tiedemann (Hrsg.), Strafgesetzbuch, Leipziger Kommentar, Bd. 10, 12. Aufl. 2008, § 303a Rn. 2.

genden Fehler vollständiger aufzuzeigen und zu erläutern, als dies bislang geschehen ist.

Dabei ist ein Zusammenhang besonders zu berücksichtigen: § 303a StGB war einerseits ein Vorbild für Art. 4 der Cybercrime-Convention („Data interference"), andererseits ist er nun Umsetzungsakt zu diesem. Eine Betrachtung der nationalen Vorschrift ohne das korrespondierende europäische Strafrecht wäre deshalb unvollständig. Vorschläge für eine hinreichend bestimmte Umsetzung müssen sowohl auf die Cybercrime-Convention als auch auf die Europäische Menschenrechtskonvention (EMRK) abgestimmt sein.

Unter dem Gesichtspunkt der Regelungstechnik beleuchtet, zeigen die gefundenen Ergebnisse schließlich systematische Gesetzgebungsfehler auf, die es künftig zu vermeiden gilt (unten IV.).

II. Wert und Grenzen von Analogie als Regelungstechnik

1. Das Gesetzlichkeitsprinzip im positiven Recht

Im Strafrecht gilt das Gesetzlichkeitsprinzip: „nullum crimen, nulla poena sine lege". Die deutsche Verfassung enthält es in Art. 103 Abs. 2 GG, die EMRK in Art. 7 Abs. 1; Gleiches gilt für zahlreiche weitere internationale Abkommen, Verfassungen und Strafgesetzbücher.

Diese stimmen keineswegs völlig überein. Der Gesetzes- bzw. Rechtsbegriff in Art. 7 EMRK wirft hinsichtlich der Gegenüberstellung von geschriebenem Gesetz (der „lex scripta") und common law sowie case law einige Probleme auf.[5] In deren Folge (zusammen mit anderen Gründen) weichen die Anforderungen an die Bestimmtheit und Handhabung der Normen bzw. die Vorhersehbarkeit der Gefahr der Strafverfolgung und -verurteilung durchaus voneinander ab.

Diese Unterschiede können hier aber unberücksichtigt bleiben. Das liegt vor allem daran, dass es im Folgenden nur um den Erlass und die Anwendung geschriebener Gesetze gehen wird und es nur auf die Grundzüge des Gesetzlichkeitsprinzips ankommen wird. Auch diese formulieren das BVerfG und der EGMR recht unterschiedlich. In der Sache sind sich die Ausformungen und Lesarten des Gesetzlichkeitsprinzips aber so ähnlich, dass sie meist gemeinsam behandelt werden können. Das geschieht im Folgenden primär in der deutschen Terminologie und nach deutscher Konstruktion des Gesetzlichkeitsprinzips. Es ließen sich aber jeweils unmittelbare Entsprechungen in der Vorhersehbarkeits-Dogmatik des EGMR formulieren.

2. Das Analogieverbot

Art. 103 Abs. 2 GG verbietet dem Rechtsanwender Analogieschlüsse und den Rückgriff auf Gewohnheitsrecht. Art. 7 EMRK verbietet eine das jeweils einschlägige (nationale) Rechtsquellensystem und den zugehörigen Methodenkanon verlassende Anwendung des Strafrechts in einer Weise, die (insbesondere wegen dieses methodischen Fehlers) zu für den Beschuldigten unvorhersehbaren bzw. nicht vernünftigerweise zu erwartenden und ihm nachteiligen Ergebnissen führt.[6] Dieses „Analogieverbot" richtet sich in keinem Fall an den Gesetzgeber, sondern immer nur an den Anwender der Gesetze. Solange der Gesetzgeber – wie beim Computerbetrug – nicht den Rechtsanwender zu Analogieschlüssen auffordert, sondern diese selbst zieht, die sich ergebenden Normen selbst ausformuliert und als Gesetz erlässt, ist das Analogieverbot nicht berührt.

Die Analogie darf auch bei der Auslegung des Tatbestands aufgegriffen werden (was z.B. bei der „betrugsspezifischen Auslegung" des § 263a StGB geschieht), ohne das Analogieverbot zu verletzen. Ausgelegt wird die Norm zwar durch den Rechtsanwender, Auslegung ist aber zulässiger und gewollter (weil notwendiger) Teil der Rechtsanwendung. Erst wenn über die Auslegung der Vorschriften hinaus de facto neue Deliktstatbestände konstruiert bzw. strafbarkeitseinschränkende Erlaubnisse und Entschuldigungen reduziert werden, ist das Gesetzlichkeitsprinzip (das Analogieverbot) verletzt.

Der Einsatz von Analogie als Regelungstechnik hat mit dem Verhalten des späteren Rechtsanwenders erst einmal nichts zu tun. Ihm bleibt es verboten, Tatbestände auf Fälle auszudehnen, die sie nicht selbst erfassen. Die dabei erforderliche Grenzziehung zwischen einer zulässigen (auch weiten) Auslegung und verbotener (selbst wenn nur dem Gesetzeszweck geschuldeter) Analogie ist immer schwierig. Aus der speziellen Regelungstechnik ergeben sich insoweit aber keine Besonderheiten. Deshalb ist das Analogieverbot für die hier anzustellenden Überlegungen ohne weitere Bedeutung.

3. Der Bestimmtheitsgrundsatz

Für den Gesetzgeber ergeben sich aus dem Gesetzlichkeitsprinzip das Verbot rückwirkender Gesetzgebung und das Gebot hinreichend bestimmter Gesetzgebung. Die Adressaten von Straftatbeständen müssen im Voraus angemessen erkennen können, für welches Verhalten ihnen eine Strafverfolgung (und welche Bestrafung) drohen würde. Dieses „Bestimmtheitsgebot" ist die rechtliche Basis der folgenden Überlegungen.

[5] Grundlegend (allerdings zu Art. 10 Abs. 2 EMRK) EGMR (P), Urt. v. 26.4.1979 – 6538/74 (Sunday Times v. Vereinigtes Königreich [Nr. 1]), Rn. 47 f. = Serie A Nr. 30, darauf bezogen später (zu Art. 7 EMRK) u.a. EGMR (GK), Urt. v. 12.2.2008 – 21906/04 (Kafkaris v. Zypern), Rn. 139 und EGMR, Urt. v. 17.9.2009 – 10249/03 (Scoppola v. Italien [Nr. 2]), Rn. 99. Vgl. auch *Frowein*, in: Frowein/Peukert, EMRK-Kommentar, 3. Aufl. 2009, Art. 7 Rn. 4, Art. 5 Rn. 26.

[6] Näher zur Abhängigkeit des Art. 7 EMRK vom Rechtsquellensystem des jeweiligen Vertragsstaats s. EGMR (GK), Urt. v. 12.2.2008 – 21906/04 (Kafkaris v. Zypern), Rn. 139 sowie EGMR (P), Urt. v. 18.6.1971 – 2832/66, 2835/66 und 2899/66 (De Wilde, Ooms und Versyp v. Belgien), Rn. 93 = Serie A Nr. 12; EGMR, Urt. v. 25.3.1985 – 8734/79 (Barthold v. Deutschland), Rn. 46 = Serie A Nr. 90; EGMR (GK), Urt. v. 22.3.2001 – 34044/96, 35532/97 und 44801/98 (Streletz, Kessler und Krenz v. Deutschland), Rn. 57, 67-76; EGMR (GK), Urt. v. 10.11.2005 – 44774/98 (Leyla Şahin v. Türkei), Rn. 88; EGMR, Urt. v. 3.5.2007 – 11843/03, 11847/03 und 11849/03 (Custers, Deveaux und Turk v. Dänemark), Rn. 84 ff.

a) Der Strafgesetzgeber muss sich so ausdrücken, dass sowohl die Bürger als auch die öffentlichen Stellen, die das Strafgesetz vollziehen sollen, das Gesetz verstehen können. Um verstanden zu werden, muss der Gesetzgeber an vorhandene Vorstellungen anknüpfen und Wörter in etablierten Wortbedeutungen verwenden. Einen bei Juristen, EDV-Fachleuten und Bürgern gemeinsam etablierten Sprachgebrauch, auf den der Gesetzgeber hätte zurückgreifen können, als er 1986 das deutsche Computerstrafrecht neu geschaffen hat,[7] gab es jedoch kaum. Um strafbare Handlungen unmittelbar und knapp zu formulieren, fehlten ihm schlicht die Worte. Das hat sich bis heute vielleicht ein wenig, aber nicht grundlegend geändert. Für den Gesetzgeber bestand daher – und besteht auch heute noch – keine andere Möglichkeit, als in praktisch jedem einzelnen Deliktstatbestand des Computerstrafrechts einen gedanklichen Bogen zu schlagen:

Der Gesetzgeber muss an Vorstellungen anknüpfen, die seinem Leser geläufig sind, und Wörter in etablierten Wortbedeutungen verwenden. Deshalb geht er von den Verboten der klassischen Deliktstatbestände aus, bezieht sich auf sie und formuliert Besonderheiten und Abweichungen. So entsteht ein neuer, zu dem klassischen Verbot analoger Tatbestand.

Der regelungstechnische Rückgriff auf Analogien ist im Computerstrafrecht ein zielführender, unter Umständen sogar der einzige und regelmäßig jedenfalls der beste Weg, um hinreichend bestimmte Tatbestände zu formulieren. Hierin liegt der Wert von Analogie als Regelungstechnik.

Ein weiterer Vorteil kann hinzutreten: Die mit neuen technischen Möglichkeiten entstehende Kriminalität ist selten genuin neuartig. Meist ist sie das Resultat einer Verlagerung bisheriger krimineller Aktivitäten. Die Analogie kann diese Verlagerung dokumentieren und dazu beitragen, dass sich die strafrechtliche Behandlung ähnlich gearteter Kriminalität nicht sachwidrig aufspaltet, sondern gemeinsam fortentwickelt.

b) Das eingangs angeführte Beispiel der beweiserheblichen Daten in § 269 StGB zeigt, dass der Gesetzgeber gelegentlich doch vom Rechtsanwender zu ziehende Analogien anordnet.[8] Der Rechtsanwender hat dort zu prüfen, ob bei der Wahrnehmung der Daten eine Urkunde vorläge, die Daten also ein Urkundsanalogon darstellen.

Wiederum kann das strafrechtliche Analogieverbot so nicht verletzt werden, denn es richtet sich nicht an den Gesetzgeber, und der Rechtsanwender hält sich im Rahmen der gesetzlichen Vorgabe. Die Anordnung einer vom Anwender zu ziehenden Analogie kann aber mit dem Bestimmtheitsgebot in Konflikt geraten. Aus dem Gesetz selbst muss der Adressat seine Pflicht erkennen können und nicht erst aus der Entscheidung eines Rechtsanwenders. Diesem darf der Gesetzgeber auch nicht die Kompetenz verleihen, Tatbestandsmerkmale im Einzelfall ad hoc per Analogie auszudehnen.

Der Gesetzgeber darf hingegen die Konkretisierung von Tatbeständen in gewissem Umfang der Praxis überlassen. Auslegung und Subsumtion sind ohnehin notwendiger Bestandteil der Rechtsanwendung und nicht ohne Spielräume denkbar. Die Frage, ob ein konkreter Umstand eines Falles unter ein Merkmal des Tatbestandes zu subsumieren ist, wird dabei regelmäßig auch anhand von Ähnlichkeitserwägungen mit Bezug auf bereits entschiedene Fälle, „klare Fälle“ etc. zu beurteilen sein; in diesem Sinne hat die Rechtsanwendung stets eine „analogische“ Struktur.[9]

In § 269 StGB wird der Urkundsbegriff des § 267 Abs. 1 StGB aufgegriffen und statt der Verkörperung der Gedankenerklärung ihre Manifestation in Daten verlangt. Dadurch werden alle Unbestimmtheiten des Urkundsbegriffs in § 269 StGB übertragen (und es wäre schon in § 267 StGB wünschenswert, dass die erhebliche Abweichung seiner Begrifflichkeit vom Alltagssprachgebrauch in der Norm zumindest angedeutet würde). Die Analogie fügt auch weitere Vagheit hinzu, denn viele Daten haben keine eindeutige Darstellung (eine bestimmte Wahrnehmung durch Menschen ist nur selten ihr Zweck). Diese Auslegungs- und Subsumtionsprobleme unterscheiden sich von anderen Begriffsbildungen aber nicht spezifisch. Die Analogie ist hier nur eine Ausdrucksweise, in der ein Tatbestandsmerkmal umschrieben wird. Sie eröffnet dem Rechtsanwender aber keine zusätzlichen Spielräume und beinhaltet somit keine unzulässige Kompetenzübertragung.

4. Wert und Grenzen (Zwischenergebnis)

Der Gesetzgeber ist also oft gut beraten, neue Tatbestände in Analogie zu klassischen Tatbeständen zu entwickeln. Es ist ihm auch nicht verwehrt, dabei neue Begriffe in Analogie zu bekannten Begriffen zu bilden.

Der Gesetzgeber darf hingegen keine Aufforderung zu Analogieschlüssen des Rechtsanwenders in die Tatbestände aufnehmen, die beinhalten, dass dieser letztlich erst seine eigenen Begriffe, eigene Verhaltensnormen oder eigene Sanktionsnormen zu entwickeln hat. Deshalb muss die Analogie insbesondere stets soweit im Gesetz ausgeführt werden, dass – in dem für Straftatbestände zu fordernden Maß an Bestimmtheit[10] – klar wird, von welchem klassischen Tatbestand bzw. Begriff sie ausgeht, in welchen Merkmalen von diesen abgewichen wird und welche anderen Kriterien die entstehenden Leerstellen füllen sollen. Zu einem methodengerechten Analogieschluss gehört es ohnehin, die Abweichung zu benennen, die einer unmittelbaren Anwendung der Ausgangsregel entgegensteht, und die Ähnlichkeit herauszu-

[7] 2. Gesetz zur Bekämpfung der Wirtschaftskriminalität v. 15.5.1986 = BGBl. I 1986, S. 721.

[8] Weitere Beispiele bei *Grünwald*, ZStW 76 (1964), 1 (7 f.).

[9] Näher *Hassemer/Kargl*, in: Kindhäuser/Neumann/ Paeffgen (Hrsg.), Nomos Kommentar, Strafgesetzbuch, Bd. 1, 3. Aufl. 2010, § 1 Rn. 95 m.w.N.

[10] Die dabei heranzuziehenden Kriterien anzugeben, ist eines der in letzter Konsequenz bis heute ungelösten Probleme des strafrechtlichen Gesetzlichkeitsprinzips (*Roxin*, Strafrecht, Allgemeiner Teil, Bd. 1, 4. Aufl. 2006, § 5 Rn. 69 ff. m.w.N.). Diesem Problem kann hier nicht weiter nachgegangen werden. Es genügt festzustellen, dass der Einsatz von Analogie als Regelungstechnik insoweit keine besonderen Kriterien erfordert.

arbeiten, die die Erstreckung der Ausgangsregel gleichwohl begründet.[11]

III. Probleme bei der Datenveränderung

Die Einhaltung dieser Grenzen und damit die Anwendung dieser Regelungstechnik sind dem Gesetzgeber nicht immer gut gelungen. Das soll im Folgenden am Tatbestand der Datenveränderung (§ 303a StGB[12]) aufgezeigt und näher untersucht werden.

1. Sachbeschädigung als Vorbild

Der Tatbestand ist demjenigen der Sachbeschädigung (§ 303 StGB) nachgebildet.[13] Das fällt im deutschen Strafrecht durch die systematische Stellung und die Formulierung der Vorschrift unmittelbar ins Auge. Für Art. 4 der Cybercrime-Convention führt § 60 des Explanatory Reports dies ausdrücklich aus. Um diese Analogie näher zu untersuchen, werden im Folgenden die ersten beiden Absätze von § 303a und § 303 StGB einander gegenübergestellt.[14]

Das Tatobjekt der Sachbeschädigung sind Sachen; ihnen korrespondieren bei der Datenveränderung die Daten. Als Tathandlung nennt die Sachbeschädigung das Beschädigen oder Zerstören der Sache; dem korrespondiert bei der Datenveränderung das Löschen, Unterdrücken, Unbrauchbarmachen und Verändern der Daten. Bei der Sachbeschädigung muss die Sache fremd sein. Der Tatbestand spricht auch davon, dass das Verhalten rechtswidrig sein muss. Das ist aber nach ganz herrschender Auffassung nicht als Tatbestandsmerkmal zu verstehen, sondern nur als (entbehrliche) Erinnerung daran, dass nach allgemeinen Rechtfertigungsgründen gerechtfertigtes Verhalten keine Straftat ist.[15] Dem Tatbestandsmerkmal der Fremdheit der Sache für den Täter bei der Sachbeschädigung korrespondiert das Tatbestandsmerkmal der Rechtswidrigkeit bei der Datenveränderung.

All diese Beziehungen bedürfen einer näheren Betrachtung. Das gilt insbesondere für die sehr unterschiedliche Behandlung des Wortes „rechtswidrig“ in beiden Tatbeständen, das in den parallel aufgebauten Sätzen doch an jeweils gleicher Stelle steht und grammatisch in beiden eine völlig übereinstimmende Funktion hat.

2. Daten vs. Sachen

Sachen sind körperliche Gegenstände (vgl. § 90 BGB). Man wird den Sachbegriff als einen der klarsten Rechtsbegriffe ansehen dürfen, die wir haben.[16] Er ist daher sicher auch eine besonders geeignete Grundlage für Analogien.

Wenn diese Klarheit bei der Analogie in gewissem Umfang getrübt wird, muss sich daraus noch kein rechtlicher Problemfall ergeben. Im Gegenteil wird man es bei einer neu eingeführten Begrifflichkeit (wie dem Datenbegriff 1986) als „normal“ anzusehen haben, dass sie das Maß an Klarheit etablierter Begriffe und erst recht so klarer Begriffe wie dem der Sache zumindest nicht sofort zu erreichen vermögen. Zu untersuchen ist vielmehr, an welchen Stellen durch die Analogie Klarheit verloren geht, ob diese Verluste vermeidbar wären, ob sie an anderer Stelle im Tatbestand kompensiert werden und ob sich insgesamt noch eine hinreichend bestimmte Verhaltensnorm ergibt.

a) Substanz

Der in § 303a Abs. 1 StGB dem Merkmal „Daten“ beigegebene Verweis auf § 202a Abs. 2 StGB suggeriert eine Legaldefinition. Die steht dort aber nicht, sondern nur einzelne Aspekte des Begriffs: Daten müssen elektronisch, magnetisch oder sonst nicht unmittelbar wahrnehmbar gespeichert sein oder übermittelt werden. Dadurch wird gegenüber dem Begriff der Sache zunächst insoweit abstrahiert, als Daten keine Substanz – d.h. keine Materie – haben müssen.

Tatsächlich wird unter den Datenbegriff jegliche in einer der genannten Weisen gespeicherte oder übertragene[17] Information gefasst. In einigen deutschen Straftatbeständen

[11] *Larenz*, Methodenlehre der Rechtswissenschaft, 6. Aufl. 1991, II. Teil 5 Kap. 2. lit. b.

[12] Auch dieser wurde 1986 eingeführt (Fn. 7), war allerdings erst im Rechtsausschuss dem Gesetzentwurf hinzugefügt worden. Die Ergänzung der Vorschrift im 41. Strafrechtsänderungsgesetz zur Bekämpfung der Computerkriminalität v. 7.8.2007 = BGBl. I 2007, S. 1786 (zur Umsetzung des Übereinkommens des Europarates über Computerkriminalität und der Umsetzung des Rahmenbeschlusses 2005/222/JI des Rates vom 24.2.2005 über Angriffe auf Informationssysteme = ABl. EU 2005 Nr. L 69, S. 67), betrifft die folgenden Überlegungen nicht.

[13] Statt aller BT-Drs. 10/5058, S. 34.

[14] § 303a Abs. 1 StGB lautet: „Wer rechtswidrig Daten (§ 202a Abs. 2) löscht, unterdrückt, unbrauchbar macht oder verändert, wird mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe bestraft.“
§ 303 Abs. 1 StGB lautet: „Wer rechtswidrig eine fremde Sache beschädigt oder zerstört, wird mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe bestraft.“

[15] Statt aller *Zaczyk* (Fn. 3), § 303a Rn. 21.

[16] Streitfälle entstehen praktisch nur dort, wo ein Gebilde zwar eine bestimmte Funktion hat, sein Körper sich aber nicht recht abgrenzen lässt, etwa bei der Frage, ob eine Langlaufloipe eine Sache ist (abl. BayObLG NJW 1980, 132).

[17] Daten müssen sich nicht einmal in einer Speicherzelle oder an anderer Stelle in einem Gerät physisch manifestieren. Dass sie z.B. als Lichtblitze, elektromagnetische Wellen etc. gerade übertragen werden, genügt. In der Regel arbeiten technische Übertragungen zumindest auf niedriger Ebene aber mit Kontrollprotokollen, nach denen die gerade übertragenden Daten bei der Sendeeinheit gespeichert bleiben, bis die Empfangseinheit den Transfer bestätigt. Strikt unidirektionale Übertragungen (ohne Antwortmöglichkeit der Empfangseinheit) ohne anderweitige Absicherung der Übertragung (bei der die Daten wiederum gespeichert werden) sind relativ selten. Der besseren Lesbarkeit wegen wird deshalb im Folgenden nur von gespeicherten Daten die Rede sein, ohne dass das als Ausgrenzung lediglich übertragener Daten gemeint ist.

wird ein noch weiterer Datenbegriff verwendet.[18] Art. 1 lit. b der Cybercrime-Convention hingegen enthält einen insoweit engeren Begriff, als er nur Computerdaten erfasst, während der deutsche Datenbegriff sich gerade nicht auf eine Datenverarbeitungsanlage festlegt und z.B. neben digitalen auch analoge Daten erfasst.[19] Diese Unterschiede sind für die folgenden Überlegungen nicht von Bedeutung. Entscheidend ist, dass bei all diesen Datenbegriffen viel mehr als nur die Substanz der Sache verloren geht:

b) Funktion

Bei der Sachbeschädigung ist heute anerkannt, dass die Funktion der Sachen geschützt werden soll. Dass Sachen eine Funktion oder auch viele Funktionen haben, ist ein wesentliches Charakteristikum.

Datenträger sind meist so beschaffen, dass sie in jeder beschreibbaren bzw. lesbaren Einheit einen definierten Zustand aufweisen. Ihr Inhalt muss weder einen Sinn ausdrücken noch gezielt einer Funktion zugeführt werden können. Aus der Systemperspektive eines Computers lässt sich sinntragende Information oft nicht einmal von sinnlosen Speicherinhalten unterscheiden. Eine ordentlich verschlüsselte E-Mail z.B. sieht immer wie eine gänzlich zufällige Zeichenfolge aus. Ob sie irgendeinen Sinn enthält, können die zahlreichen Computersysteme, die mit der Verarbeitung dieser E-Mail beschäftigt sind, schon deshalb nicht entscheiden, weil sie sie nicht entschlüsseln können.

Der Datenbegriff des StGB wird daher so verstanden, dass Daten keine Funktion und nicht einmal ein Verwendungszweck zukommen müssen.[20] Neben die Abstraktion von der Substanz der Sache tritt also auch eine Abstraktion von ihrer Funktion. Übrig bleibt schon hier lediglich ein Abstraktum, das zwar sinnvolle Information beinhalten und damit auch eine Funktion besitzen kann, aber nicht muss.[21]

c) Einheit

Eine Sache muss immer einen gewissen Umfang und eine gewisse Einheit aufweisen. Die zivilrechtlichen Probleme bei der Unterscheidung von Bestandteilen, Zubehör und selbstständigen Sachen stellen sich bei der Sachbeschädigung so nicht. Doch nur als Einheit kann die Sache einen Sinn und eine Funktion haben, und darauf kommt es auch im Strafrecht an.

Mit dem Datenbegriff lässt sich zwischen einer Informationseinheit, die selbst einen Sinn ausdrückt bzw. eine Funktion besitzt, und ihren Bausteinen nicht unterscheiden. In den meisten Computersystemen ist der kleinste Informationsbaustein das Bit, das entweder eine 0 oder eine 1 beinhaltet. Es kann eine selbständige Information beinhalten (z.B. das Geschlecht einer Person repräsentieren) oder sich (z.B. im Zusammenhang einer Bilddatei) erst gemeinsam mit Abertausenden weiteren Bits zu einer sinnvollen Information zusammenfügen. In beiden Fällen wird das Bit vom Datenbegriff erfasst.

Der Datenbegriff abstrahiert also auch von der Sinn stiftenden Einheit der Sache. Die Unterscheidung zwischen einem Sinn- bzw. Funktionszusammenhang und seinen isoliert sinnlosen Bruchstücken geht damit verloren. Der Verzicht auf diese Unterscheidung ist so, als würde man zwischen der Bedeutung eines Wortes in einem bestimmten Kontext und einem einzelnen Buchstaben nicht unterscheiden. Ein entsprechender Beleidigungstatbestand würde lauten: „Wer Buchstaben rechtswidrig verwendet, wird mit […] bestraft."

d) Identität

Alle Sachen (und Personen) unterliegen der Identitätsrelation. Nur deshalb kann man im Prozess angeben, welche Sache beschädigt bzw. zerstört wurde. Ferner kann dieselbe Sache weder mehrfach zerstört noch ihr dieselbe Funktion (ohne zwischenzeitliche Reparatur) mehrfach genommen werden.

Daten hingegen lassen sich kopieren, was zu einer „Identitätsspaltung" führt und zur Aufgabe des Identitätskonzepts zwingt: Das Löschen einer Kopie vernichtet die Daten, und doch sind dieselben Daten (andernorts) weiterhin unverändert vorhanden.[22] Entsprechend können auch endgültige Veränderungen von Daten anhand einer Kopie zu beheben, also bloß zeitweilig sein. Zerstörung, Beschädigung sowie dauerhafte und zeitweilige Entziehung sind bei Daten nicht zu unterscheiden.[23]

Eine Sache bleibt auch nach der Beschädigung „dieselbe Sache", die sie vorher war. Aufgehoben wird die Identität erst durch Zerstörung, Verarbeitung etc. Bei einer Veränderung von Daten hingegen werden immer alte Daten durch neue ersetzt. Unterschiedliche Daten als „dieselben Daten" zu betrachten, ist gänzlich willkürlich. Nur größeren Zusammenhängen mit Einheit und Funktionen (und Kontext) kann man eine auch unter Veränderungen gleich bleibende Identität zusprechen. So kann man sagen: „Ich habe in *diesem* Text ein Beispiel eingefügt." Man kann aber nicht statt eines Textzusammenhangs einzelne Zeichen betrachten und sagen: „Die eingefügten Schriftzeichen sind dieselben wie die, die vorher noch nicht dort waren."

[18] §§ 263a, 268 und 269 StGB enthalten keinen Verweis auf § 202a Abs. 2 StGB und verzichten so auch noch darauf, dass die Daten sich zumindest als Zustand einer Speicher-, Sende-, Empfangs- oder Übertragungseinheit manifestieren. So werden insb. Eingabeakte bereits isoliert (nämlich vor ihrer Repräsentation im Verarbeitungssystem) erfasst.

[19] Näher *Spannbrucker*, Convention on Cybercrime (ETS 185), Ein Vergleich mit dem deutschen Computerstrafrecht in materiell- und verfahrensrechtlicher Hinsicht, 2004, S. 34 ff. im Internet unter http://d-nb.info/973688068/34 (11.7.2012).

[20] Vgl. *Graf*, in: Joecks/Miebach (Hrsg.), Münchener Kommentar zum Strafgesetzbuch, Bd. 3, 2003, § 202a Rn. 8.

[21] Vgl. *Heghmanns*, Strafrecht für alle Semester, Besonderer Teil, 2009, Rn. 917.

[22] Was nach h.M. die Löschensvariante von § 303a Abs. 1 StGB erfüllt, vgl. *Meinhardt* (Fn. 3), S. 101; *Wieck-Noodt*, in: Joecks/Miebach (Hrsg.), Münchener Kommentar zum Strafgesetzbuch, Bd. 4, 2006, § 303a Rn. 12.

[23] Näher dazu unten bei Fn. 29.

Würde man hingegen zusammenhängende Daten mit einer Funktion (oft sind das z.B. Dateien) betrachten, könnte man auf eine Identitätsrelation zurückgreifen. Beim Umcodieren etwa werden die Daten grundlegend umgestaltet, und doch bleibt die in ihnen codierte Information u.U. völlig gleich. Auch Kopien kann man dann als identisch ansehen (zumindest wenn sie gleichermaßen verfügbar sind, sonst stimmt ihre Funktion praktisch nicht überein).

e) Vermeidbarkeit dieser Abstraktionen

Die Abstraktion von der Substanz ließe sich nur vermeiden, indem man eine Manifestation der Daten in einem physischen Datenträger verlangt. Man gewönne dadurch allerdings nicht viel. Verwechslungen der Manipulation von Daten mit Manipulationen am Datenträger und Verwechslungen der Rechte an Daten mit Rechten am Datenträger finden ohnehin regelmäßig statt und würden so noch gefördert. Die Abstraktion von der Substanz ist – vor allem da auch bei der Sachbeschädigung heute die Funktion der Sache im Vordergrund steht – unproblematisch und ohne weiteres sinnvoll.

Bei den übrigen Abstraktionen ist das anders. Auch ein sinnvoller Zusammenhang von Daten weist eine Einheit auf und besitzt in der Regel Funktionen, worauf sich wiederum eine Identitätsrelation stützen könnte. Deshalb wäre es möglich, den Datenbegriff anders zu bilden, als dies im Strafrecht heute geschieht, und ihn dem Begriff der Sache wesentlich stärker anzunähern. Die Abstraktion von Einheit, Funktion und Identität findet ihren Grund nicht in der Struktur des vom Tatbestand zu schützenden Objekts. Der einzige strukturelle Zusammenhang ist, dass mit der Abstraktion von der Einheit auch die Funktion verloren geht und ohne Rückgriff auf Funktionen keine gegenüber Veränderungen beständige Identitätsrelation besteht.

Mit den Abstraktionen von Einheit, Funktion und Identität wird versucht, den Schutzbereich der Norm zu erweitern und Beweisschwierigkeiten zu vermeiden. Ob das gelingt und sinnvoll ist, oder letztlich doch Fälle erfasst werden, die gar nicht erfasst werden sollen, oder schlicht unklar bleibt, was erfasst wird, gilt es daher weiter zu prüfen.

f) Vorteilhafte vs. nachteilige Beeinflussung

Bei Sachen liefern die Zerstörung, die dauerhafte Entziehung, die Beschädigung und die kurzzeitige Entziehung Graduationsstufen des Unrechts. Durch die Abstraktion von Einheit und Identität gehen diese dem Datenbegriff verloren.

Doch nicht nur die Graduierung geht verloren: Für das Unwert-Urteil der Sachbeschädigung nach § 303 Abs. 1 StGB ist es eine notwendige Voraussetzung, dass die Substanz bzw. Funktion einer Sache beeinträchtigt wurden.[24] Durch die Abstraktion von Substanz und Funktion geht deshalb die Grundlage des Unwert-Urteils verloren.

> *Beispiel*: Eine Textdatei ist im Zeichensatz eines nicht mehr verwendbaren Computersystems codiert. Der Täter überträgt sie in den Standard-Zeichensatz des Systems, das die Datei künftig verarbeiten soll.

Die Situation wird hier in praktischer Hinsicht (für alle, die die Daten verwenden wollen) nur verbessert. Dieser Einschätzung liegt aber eine inhaltliche Betrachtung der Daten und ihrer Funktion zugrunde. Mit dem Datenbegriff des StGB hingegen kann man in der Handlung, die die alten Daten überhaupt erst wieder praktisch verwendbar macht, nur die Veränderung dieser Daten erkennen. Ob eine Veränderung nachteilig, neutral oder vorteilhaft ist, ließe sich mit Bezug auf Funktionen feststellen; die aber werden gerade ausgeblendet.[25]

Jede Veränderung von Daten geschieht durch „überschreiben" der alten Daten. Weil man ohne Identitätsrelation nicht sagen kann, dass die neuen Daten trotz ihrer Änderung „dieselben" wären wie die alten Daten, stellt sich jede Veränderung der Daten als Löschen der alten Daten dar.

Auf der Grundlage dieses Datenbegriffs kann man also letztlich zwischen den verschiedenen Einwirkungen auf Daten gar keine Unterscheidungen treffen. Die Anknüpfungspunkte, die es ermöglichen würden, eine rein vorteilhafte Aufbereitung von der Vernichtung von Daten zu unterscheiden, fehlen.

3. Die Tathandlungen

a) Verändern, löschen und unbrauchbar machen

Das Fehlen der durch die Abstraktionen beseitigten Anknüpfungspunkte hat unmittelbare Konsequenzen für die Tathandlungen. Die Datenveränderung kann begangen werden, indem der Täter Daten löscht, unterdrückt, unbrauchbar macht oder verändert.

Daten zu löschen und sie zu verändern ist dasselbe. Aus mancherlei Perspektive mag das auf den ersten Blick erstaunen. So sind z.B. bei der Textverarbeitung das Überschreiben und das Löschen von Text nicht ohne weiteres dasselbe. Ein Computerspeicher aber ist in viele völlig gleichartige Einheiten (Bytes) aufgeteilt, die immer genau einen Wert beinhalten. Dieser lässt sich ändern, aber Speicherstellen ohne Inhalt gibt es nicht. (Das ist ähnlich wie mit der Farbe von Gegenständen: Alles hat immer eine Farbe; ersatzlos löschen kann man sie nicht, nur verändern.). Man löscht Daten, indem man die sie beinhaltenden Speicherstellen (oder Verweise auf diese Speicherstellen) überschreibt, also Daten verändert. Umgekehrt besteht jede Veränderung von Daten in einem Überschreiben der betreffenden Speicherstellen, also einem Löschen der dort zuvor stehenden Daten. Unterscheiden lässt

[24] Bei § 303 Abs. 2 StGB ist das etwas anders. Das steht den Überlegungen hier aber nicht entgegen, denn erstens war § 303 Abs. 2 StGB nicht Vorbild von § 303a StGB, sondern wurde erst viel später ins Gesetz aufgenommen. Zweitens ist § 303 Abs. 2 StGB selbst eine gesetzliche Analogie zu § 303 Abs. 1 StGB und ersetzt den sich aus der Funktion der Sache ergebenden Bewertungsmaßstab durch einen anderen (näher dazu *Schuhr*, JA 2009, 169 [172, 174]).

[25] Vgl. auch *Hilgendorf/Frank/Valerius*, Computer- und Internetstrafrecht, 2005, Rn. 194.

sich beides nur für eine Gesamtheit von Daten: Bleibt es trotz der Veränderung „dieselbe" Gesamtheit, liegt „bloß eine Veränderung" vor, geht die Gesamtheit bei der Veränderung unter, ist sie auch eine Löschung. Die Unterscheidung erfolgt also anhand der Identitätsrelation und bezieht sich auf ein viel komplexeres Konstrukt als Daten. Von diesem Konstrukt aber spricht der Tatbestand gar nicht.

Um Daten unbrauchbar zu machen, muss man ihren Inhalt beeinflussen, sie also verändern. Schulbeispiel dieser Begehungsvariante ist die Manipulation eines Programms durch Einfügen störender Befehle.[26] Im Einfügen liegt technisch indes immer eine Veränderung von Daten.[27] Umgekehrt macht jede Veränderung die dabei gelöschten Daten unbrauchbar. Von „Unbrauchbarkeit" kann man überhaupt nur mit Bezug auf eine Funktion sprechen, muss also wieder eine funktionale Gesamtheit von Daten voraussetzen und gerade nicht den weiten strafrechtlichen Datenbegriff.

Daten (im weiten strafrechtlichen Begriffsverständnis) zu löschen, sie unbrauchbar zu machen und sie zu verändern, ist also aus technischen und semantischen Gründen letztlich dasselbe.[28] Dass man in jedem Kommentar für diese „Begehungsvarianten" jeweils typische Fallgruppen nachlesen kann,[29] zeigt, dass bei der Auslegung der Tatbestandsmerkmale die Begrifflichkeit gewechselt und innerhalb derselben Anwendung der Norm teils ein weiter, teils ein enger Datenbegriff verwendet wird. Das ist widersinnig, aber im Ergebnis unschädlich, solange es nur dazu führt, dass das Verändern seine begriffliche Weite behält und Auffangvariante wird, während die übrigen Varianten ad hoc eingegrenzt werden.[30]

Bei der Sachbeschädigung ist das Zerstören die stärkste Form der Beschädigung. § 303 Abs. 1 StGB kennt also nur eine Begehungsform (das Beschädigen), hebt darin aber eine besonders intensive Schädigung des Rechtsguts (seine Zerstörung) hervor. Der Datenbegriff erlaubt bei § 303a Abs. 1 StGB keine entsprechende Graduierung. Ignoriert man hingegen seine Abstraktionen und verwendet ein echtes Analogon zu Sachen, kann man die Graduierung rekonstruieren: Bezüglich einer funktionalen Gesamtheit von Daten enthält die Begriffskette „verändern, unbrauchbar machen, löschen" eine Steigerung von neutralem bis besonders nachteiligem Handeln. Das Verändern ist dann eine Grundform der Tatbegehung.

b) Unterdrücken

Man kann die bei der Veränderung gelöschten Daten als durch das Löschen unterdrückt ansehen oder für das Unterdrücken verlangen, dass die Daten selbst unverändert bleiben, ihre Verwendung aber anderweitig verhindert wird. Jedenfalls kann die Unterdrückung von Daten nicht nur durch eine Veränderung der Daten geschehen. Diese Begehungsvariante soll (entweder ausschließlich oder zumindest auch) Fälle erfassen, in denen der Zugriff auf unverändert bleibende Daten zumindest für eine gewisse Dauer unterbunden wird, z.B. indem der Täter den Datenträger entwendet.[31] Das Unterdrücken von Daten tritt also als weitere Grundform der Tatbegehung neben das Verändern.

Das Unterdrücken hat auch keine Entsprechung bei der Sachbeschädigung. Daten ohne ihre Veränderung zu unterdrücken, beinhaltet gar keine Manipulation des Tatobjekts, sondern eine Form seiner Entziehung. In gewisser Hinsicht gleicht die Entziehung der Sache allerdings ihrer Beschädigung: Sie verhindert gleichfalls, dass der Berechtigte die Funktion der Sache (soweit diese beschädigt bzw. entzogen ist) nutzen kann. Auch die Sachentziehung ist nicht nur unschön, sondern eine z.B. nach § 823 Abs. 1 BGB zivilrechtliche Haftung auslösende unerlaubte Handlung. Sie ist aber gerade nicht in allgemeiner Form strafbar.[32] Es gibt also keinen klassischen Deliktstatbestand, zu dem die sonstige Unterdrückung von Daten analog wäre. Und es ist auch nicht ersichtlich, weshalb die Verfügbarkeit von Daten vom Gesetzgeber als schutzwürdiger angesehen wird als die Verfügbarkeit eigener Sachen.

c) Fehlender Unwert und fehlende Verhaltensnorm

Die Sachbeschädigung erfasst nur einen nachteiligen Umgang mit Sachen. Die Zerstörung vernichtet Einheit, Funktion und Identität der Sache. Die Beschädigung tut der Substanz bzw. der Funktion der Sache Abbruch. Gerade deshalb verletzt die Sachbeschädigung einen Wert.

[26] Statt vieler *Zaczyk* (Fn. 3), § 303a Rn. 9.

[27] Entweder müssen die nach der Einfügestelle folgenden Daten „nach hinten verschoben" werden, was durch rekursives Überschreiben – also Verändern – der Speicherstellen geschieht. Oder die Daten sind segmentiert, so dass die einzufügenden Daten als neues Segment „freie" Speicherstellen überschreiben und die Verweise, aus denen sich die Reihenfolge der Segmente ergibt (i.a. sog. Zeiger in Tabellen oder verketteten Listen), neu gefasst – also verändert – werden müssen. (Im Ergebnis kommt es dabei nicht darauf an, ob auch das Überschreiben der „freien" Speicherstellen als tatbestandliche Veränderung angesehen oder dies mangels Nutzungsinteresse abgelehnt wird – so z.B. *Schulze-Heiming*, Der strafrechtliche Schutz der Computerdaten gegen die Angriffsformen der Spionage, Sabotage und des Zeitdiebstahls, 1995, S. 176. Letzteres ist freilich inkonsequent, solange man an der Prämisse festhält, dass Daten keine Funktion zu haben brauchen, denn indirekt wird dabei auf eine Funktion abgestellt.).

[28] *Welp*, IuR 1988 Sonderheft, 434 (436); *Tolksdorf* (Fn. 3), § 303a Rn. 19.

[29] Statt vieler *Fischer*, Strafgesetzbuch und Nebengesetze, Kommentar, 59. Aufl. 2012, § 303a Rn. 9-12; *Zaczyk* (Fn. 3), § 303a Rn. 7-11.

[30] Die Überlappung der Tathandlungen hindert als solche jedenfalls nicht die Bestimmtheit des Tatbestandes (*Schlüchter*, Zweites Gesetz zur Bekämpfung der Wirtschaftskriminalität, 1987, S. 84).

[31] Vgl. *Zaczyk* (Fn. 3), § 303a Rn. 8 m.w.N.

[32] Der Diebstahl setzt nach § 242 StGB eine Wegnahme und Zueignungsabsicht voraus, die Unterschlagung nach § 246 StGB eine Zueignung, der unbefugte Gebrauch eines Fahrzeugs nach § 248b StGB ein bestimmtes Tatobjekt und seinen Gebrauch etc.

Die Formulierung der Tathandlungen des § 303a Abs. 1 StGB suggeriert, dass sie die gleiche Struktur aufweisen würden wie die der Sachbeschädigung und deren Unwert sich im Wege der Analogie auf die Tathandlungen der Datenveränderung übertrage. Mit den Tathandlungen des Veränderns und Unterdrückens von Daten werden indes neben nachteiligen Einwirkungen ebenso neutrale oder gar vorteilhafte erfasst: Ebenso wie man eine funktionale Gesamtheit von Daten durch Veränderung einzelner Daten ggf. verbessern kann, kann es auch vorteilhaft sein, den Zugriff auf störende oder überflüssige Daten zu unterbinden. Die Tathandlungen der Datenveränderung sind daher grundsätzlich wertneutral und beschreiben insbesondere keinen Unwert.[33] Insoweit ist die Analogie kardinal gescheitert. Das sei mit zwei Beispielen verdeutlicht:

> *Beispiel 1*: Moderne Ampelsysteme sind computergesteuert. Das ist nötig, weil der Verkehrsfluss sich nur dann über längere Strecken optimieren lässt, wenn man die verschiedenen Ampelanlagen eines größeren Bereichs koppelt und gemeinsam steuert. Manche Fußgängerampeln werden nur auf Knopfdruck grün. Dann speichert das System, ob der Knopf bereits gedrückt wurde. Wenn nun ein Fußgänger diesen Knopf drückt, löscht er die bisherigen Daten, nach denen der Knopf noch nicht gedrückt war, macht sie unbrauchbar und verändert sie dahingehend, dass der Knopf nun gedrückt ist. Darin liegt aber keinerlei Unwert.
>
> *Beispiel 2*: Unser Fußgänger geht weiter. Die Kreuzung, die er überquert, wird von einem modernen Videosystem überwacht. Dieses zeichnet sein Bild per Computer auf. Auf dem Datenträger, auf den die Aufzeichnung erfolgt, standen immer schon andere Daten. Schon wieder bewirkt er, dass sie in einer bestimmten Weise verändert werden, denn wenn er nicht über die Kreuzung ginge, würde zwar eine andere, aber eben nicht diese Veränderung erfolgen. Wiederum liegt in diesem Verhalten grundsätzlich kein Unwert.

Auch der Vorsatz des Handelnden ändert daran nichts. Wenn unser Fußgänger sich mit Computern auskennt, weiß er, dass er Daten verändert, und das ist völlig in Ordnung. Wer eine rechtlich neutrale oder gar erwünschte Handlung vorsätzlich vornimmt, schafft durch seinen Vorsatz kein Unrecht.

Die Beispiele enthalten nicht etwa Alltagssituationen, die zufälligerweise im unscharfen Rand des Deliktstatbestands liegen. Dann wären sie uninteressant, denn jede gesetzliche Bestimmung besitzt unvermeidlich einen solchen unscharfen Rand. In den geschilderten Situationen können sich jedoch Angriffe auf die betreffenden Computersysteme verbergen.

In *Beispiel 1* kann es so sein, dass sich die Programmfunktion, die die Fußgängerampel steuert, dadurch zum Absturz bringen lässt, dass man in einem bestimmten Rhythmus auf den Knopf der Ampel drückt. Die Fußgängerampel schaltet dann auf Grün und bleibt grün, die Autoampel wird rot und bleibt rot. Und unser Fußgänger bewirkt vorsätzlich genau das. Dadurch macht er sich einerseits nach Deliktstatbeständen strafbar, die die Verkehrssicherheit betreffen. Andererseits soll der Tatbestand der Datenveränderung ein solches Drücken des Knopfes als Manipulation eines Computersystems erfassen. In *Beispiel 2* kann man sich etwas Entsprechendes vorstellen, indem der Fußgänger mit dem Glas seiner Armbanduhr das Sonnenlicht auf die Kamera reflektiert.

Diese modifizierten Beispiele entsprechen einem gebräuchlichen Angriffsmuster, das darin besteht, sich Kenntnis von Programmfehlern zu verschaffen und sie mit speziellen, scheinbar regulären Eingabedaten auszunutzen. Entsprechende Angriffe, bei denen z.B. mit manipulierten Bild-Dateien über WWW-Browser sog. Trojaner auf Computer gespielt werden, gibt es immer wieder. Das soll § 303a Abs. 1 StGB gerade erfassen, und hier ist das Unrecht grds. nicht zu bezweifeln.

Das Tatobjekt Daten und die Tathandlungen des Veränderns bzw. sonstigen Unterdrückens der Daten liefern indes keinerlei Ansatz, um in den Beispielen zwischen dem alltäglichen Drücken an der Ampel bzw. Überqueren der Kreuzung und der kriminellen Manipulation der Computer zu unterscheiden. Das hat mit einer unscharfen Grenzziehung nichts zu tun; durch die dortige Bestimmung der Tathandlungen erfolgt gar keine Grenzziehung zwischen unrechtmäßigem und rechtmäßigem Verhalten.

Jede Einwirkung auf Computer – also jeder Umgang mit Computern, der nicht in einer rein passiven Wahrnehmung ihrer Anzeige oder sonstigen (weder vom Täter veranlassten noch sonst beeinflussten) Ausgabe besteht – erfolgt durch Veränderungen ihrer Daten.[34] Zu jedem noch so kleinen Bearbeitungsschritt eines Programms gehört die Manipulation des Inhalts mindestens eines Prozessorregisters oder einer Speicherstelle. Das Computerstrafrecht soll den Umgang mit Computern gerade schützen und fördern, aber keineswegs generell unter Strafe stellen. Das hätte auch sehr weitreichende Konsequenzen, denn die Liste der Alltagsbeispiele lässt sich fast beliebig fortsetzen: Viele Häuser haben heute eine computergesteuerte Lichtanlage; das Drücken auf den Lichtschalter wäre verboten. Jedes Handy ist ein Computer, und viele andere Telefone sind es auch; einen anderen Menschen anzurufen wäre oft verboten.

Der Umgang mit Computern und damit auch das Verändern von Daten ist rechtlich grundsätzlich erwünscht und oft sogar geboten. Der Tatbestand der Datenveränderung kann also kein Verbot des Veränderns von Daten beinhalten, auch wenn das auf den ersten Blick anders aussieht. Den bislang diskutierten Merkmalen – Tathandlungen und Tatobjekt – kann der Normunterworfene letztlich in keiner Situation entnehmen, was er tun darf und was nicht. Sie liefern keine Verhaltensnorm.

[33] Vgl. *Lenckner/Winkelbauer*, CR 1986, 824 (828); *Popp* (Fn. 3), § 303a Rn. 3 f.

[34] Vgl. auch *Schlüchter* (Fn. 30), S. 74; mit diesen Umstand vertiefender Rezension *Welp*, IuR 1987, 353 (354); *Tolksdorf* (Fn. 3), § 303a Rn. 5; *Gerhards*, Computerkriminalität und Sachbeschädigung, 1996, S. 35 f.

4. Verweisung auf andere Rechtsgebiete

a) „Fremd" und „rechtswidrig" als Tatbestandsmerkmale

Bei der Sachbeschädigung entsteht durch den Unwert, der in der Schädigung der Sache liegt, nur ein Teil des Unrechts der Tat. Die Sachbeschädigung schützt nicht Sachen, sondern Menschen, die sich die Funktion der Sache zu Nutze machen wollen und dürfen. Daher muss die Sache für den Täter der Sachbeschädigung „fremd" sein. Der Unwert der Sachbeschädigung ergibt sich erst aus einer Kombination zweier jeweils für sich negativer Bewertungen: Erstens muss die Sache beeinträchtigt werden. Zweitens muss dabei die sachenrechtliche Rechtsposition ihres Eigentümers verletzt werden.

Bei § 303 Abs. 1 StGB liefern beide Unrechtskonstituenten echte Beschränkungen des Tatbestands: Beschädigt der Eigentümer seine Sache selbst oder willigt er in die Beschädigung ein bzw. ist mit ihr einverstanden,[35] knüpft der Straftatbestand an den in der Beschädigung liegenden Unwert keine nachteiligen Folgen. Umgekehrt erfasst er aber auch bei weitem nicht alle Verletzungen der Rechtsposition des Eigentümers. Nur wenn sie in einer negativen Beeinflussung der Sache bestehen und sich in einem Substanz- oder Funktionsverlust manifestieren, wird der Tatbestand erfüllt.

§ 303a Abs. 1 StGB enthält kein Wort, das in der grammatikalischen Struktur des Satzes dem Merkmal „fremd" der Sachbeschädigung entspricht. Das einzige überhaupt noch verbleibende Wort des Tatbestandes ist „rechtswidrig". Würde man es – wie seine Entsprechung in § 303 Abs. 1 StGB – als überflüssigen Verweis auf das allgemeine Verbrechensmerkmal, dass kein Rechtfertigungsgrund erfüllt ist, verstehen, bliebe es bei einem Tatbestand, der jede Einwirkung auf Computer gleichermaßen erfasst und damit gar kein Unrecht zu typisieren vermag.

Will man zumindest versuchen, § 303a Abs. 1 StGB als Deliktstatbestand zu konstruieren, muss man „rechtswidrig" deshalb als Tatbestandsmerkmal ansehen.[36] Es ist das einzige deliktsbegründende Merkmal des ganzen Tatbestandes und muss im Vergleich zu § 303 Abs. 1 StGB sowohl die negative Beeinflussung des Tatobjekts als auch den Verstoß gegen seine rechtliche Zuordnung ersetzen und so die Verhaltensnorm nebst Unrecht der Tat bestimmen.

Es liefe auf dasselbe Ergebnis hinaus, wenn man „rechtswidrig" wie in § 303 Abs. 1 StGB als Merkmal verwerfen und statt seiner in § 303a Abs. 1 StGB ein ungeschriebenes Merkmal postulieren würde, dem man die genannte Funktion überträgt.[37] Das wäre durchaus konsequent, aber auch das Zugeständnis, dass die Norm hinsichtlich der vom Gesetzlichkeitsprinzip geforderten Bestimmtheit nichts zu bieten hat, denn das tatbestandstypische Unrecht würde dann ohne jeden Anknüpfungspunkt im Wortlaut der Norm hinzugedichtet. Eine einschränkende Auslegung von Tatbeständen auch mittels ungeschriebener Merkmale verletzt das Gesetzlichkeitsprinzip zwar nicht (sie geschieht durch den Rechtsanwender, für den das erweiterte Analogieverbot gilt, der dehnt den Tatbestand aber gerade nicht aus); ein Tatbestand, der überhaupt erst durch eine solche Auslegung Unrecht erhält, wäre aber nichts anderes als eine Ermächtigung zur Strafrechtssetzung durch den Rechtsanwender, also eine idealtypische Verletzung des Bestimmtheitsgrundsatzes durch den Gesetzgeber.

b) Verweisungstechniken

Es gibt grundsätzlich zwei Arten von anderweitig festgelegten Verhaltensnormen (und in ihrer Verletzung liegendes Unrecht), auf die ein Straftatbestand sich (auf jeweils unterschiedliche Weise) beziehen kann: Erstens kann er (insbes. als Blankett oder mittels normativem Tatbestandsmerkmal) auf rechtliche Normen verweisen, die zu einer anderen Regelungsmaterie gehören und einschlägige Verhaltensnormen beinhalten. Zweitens kann man jedes Verhalten eines relativ weit gefassten Typs für den Fall unter Strafe stellen, dass es nicht vom Einverständnis (bzw. der Einwilligung) eines Berechtigten gedeckt ist. Vordergründig ist das ein präventives Verbot mit Erlaubnisvorbehalt. Damit wird aber nur die Gesetzestechnik beschrieben. In der konkreten Handlungssituation trifft den Täter entweder das generelle Verbot oder bestimmte Verhaltensweisen wurden ihm (evtl. gar unter Bedingungen) freigestellt. Die an ihn gerichtete konkrete Verhaltensnorm kann er also nicht dem Gesetz entnehmen. Sie wird erst von der zur Einverständniserklärung befugten Person gesetzt und mitgeteilt. Dieser Person wird also in einem vom Deliktstatbestand festgelegten Rahmen die Kompetenz übertragen, den Umgang des anderen mit ihrem Rechtsgut durch eigene Verhaltensnormen für den Einzelfall zu regeln, und der Straftatbestand bewehrt diese privaten Einzelfallregelungen mit Sanktionen.

Beides sind gebräuchliche Regelungstechniken. Im ersten Fall macht die Verweisung die strafrechtliche Regelung akzessorisch zum jeweiligen Sachrecht, das die Verhaltensnormen beinhaltet. Wenn die Verhaltensregeln dort gesetzlich hinreichend bestimmt werden oder die Verweisung sich auf einen bestimmten Kern der Regelung beschränkt,[38] kann das ein sehr angemessenes Regelungsmodell sein: Die Verhaltensnormen stehen im sachlich passenden Kontext, und das Strafrecht sanktioniert gezielt bestimmte Verstöße.

[35] Auf die Frage, ob ein Einverständnis bereits die Fremdheit oder die Beschädigung ausschließt oder erst als Einwilligung die Tat rechtfertigt (dazu *Zaczyk* [Fn. 3], § 303 Rn. 21 m.w.N.), kommt es hier nicht an.

[36] *Lackner/Kühl*, Strafgesetzbuch, Kommentar, 27. Aufl. 2011, § 303a Rn. 4; *Popp* (Fn. 3), § 303a Rn. 3 f., 11; *Rengier*, Strafrecht, Besonderer Teil, Bd. 1, 14. Aufl. 2012, § 26 Rn. 7.

[37] Vgl. *Fischer* (Fn. 29), § 303a Rn. 4, 8, 13; *Maurach/Schroeder/Maiwald* (Fn. 3), § 36 Rn. 35; *Heghmanns* (Fn. 21), Rn. 918 m.w.N.; *Sondermann*, Computerkriminalität, 1989, S. 40 ff.; *Krutisch*, Strafbarkeit des unberechtigten Zugangs zu Computerdaten und -systemen, 2004, S. 145.

[38] Zu weite und konturarme Regelungen können im Wege der Normspaltung auf einen für das Strafrecht akzeptablen Kern reduziert werden, vgl. *Sieber*, in: Hoeren/Sieber (Hrsg.), Handbuch Multimedia-Recht, 29. Lfg., Stand: August 2011, Teil 19.1 Rn. 10.

Regelungen des zweiten Typs nehmen im aktuellen Strafrecht laufend zu. In besonderem Maße kennzeichnen sie das Sexualstrafrecht.[39] Doch auch z.B. chirurgische Heileingriffe werden strafrechtlich in dieser Form behandelt: Die mit der Operation zunächst bewirkte temporäre Verschlechterung des Gesundheitszustands des Patienten fassen die Rechtspraxis und große Teile der Lehre[40] als Körperverletzung auf, um sie den Regeln über die Einwilligung unterwerfen zu können. Ein an den Chirurgen gerichtetes Verbot des Operierens meint niemand ernst.[41] Es wäre auch widersinnig, eine medizinisch indizierte Operation zu verbieten, um die Gesundheit zu schützen. Die Konstruktion dient vielmehr dazu, den Patienten selbst über die Behandlung seines Körpers entscheiden zu lassen, also eine auf seinen Körper bezogene Verhaltensnorm für den Arzt im aktuellen Fall selbst setzen zu lassen.

Dieser zweite Regelungstyp ist unter Bestimmtheitsgesichtspunkten grundsätzlich problematisch, in manchen Bereichen (wie eben dem Sexualstrafrecht und dem Arztstrafrecht – auch wenn dort de lege ferenda ein selbstständiger Tatbestand der Einwilligungslösung vorzuziehen wäre) gleichwohl der einzig sachgerechte Regelungsmodus. Um die Bestimmtheitsprobleme im Rahmen zu halten, muss dabei (1.) feststehen, auf wessen Einwilligung bzw. Einverständnis es ankommt, müssen (2.) klare Regeln über die Wirksamkeit der Einwilligung bzw. des Einverständnisses bestehen und (3.) die Erklärungen weitgehend eindeutig interpretiert werden können.

Die beiden Regelungstypen (Akzessorietät vs. Einverständnismodell) schließen einander nicht aus. Das zeigt sich schon beim ärztlichen Heileingriff, dessen strafrechtliche Handhabung ein Beispiel für beide Regelungstypen abgibt: Zwar darf der Patient in weitem Umfang durch Einwilligung oder Verweigerung der Einwilligung selbst über die Zulässigkeit einer Behandlung entscheiden. Diese Kompetenz besteht aber nur dort, wo die Rechtsordnung die Zulässigkeit der Behandlung (und evtl. sogar die Pflicht des Arztes, zu behandeln) nicht selbst regelt (z.B. über eine mutmaßliche Einwilligung, hypothetische Einwilligung, Garantenpflichten oder Jedermannspflichten nach § 323c StGB[42]).

c) „Rechtswidrig" als Verweisung ins „Datenrecht"?

Das Merkmal „fremd" in § 303 StGB macht die Sachbeschädigung akzessorisch zum Sachenrecht (und zu Bestimmungen in anderen Teilen der Rechtsordnung, welche die Rechtsposition des Eigentümers ausgestalten). Die absolute Rechtsposition des Eigentümers wird aber (ganz § 903 BGB entsprechend) nicht absolut geschützt; vielmehr gehört es gerade zu dieser Position, dass er – wiederum innerhalb eines rechtlich vorgegebenen Rahmens – fremde Eingriffe erlauben darf. Die an den Täter gerichtete Verhaltensnorm ergibt sich also erst im Zusammenspiel von Sachenrecht und Einzelfallregelung des Berechtigten. Auch für die letztere ist das Sachenrecht von Bedeutung, denn es legt den Eigentümer als zur Einverständniserklärung berechtigte Person fest.

Ebenso, wie das Merkmal „fremd" ins Sachenrecht verweist, muss das Merkmal „rechtswidrig" auf andere Teile der Rechtsordnung verweisen, die für Daten entsprechende Regelungen beinhalten wie das Sachenrecht für Sachen. Diese Anforderung ergibt sich nicht nur daraus, dass die Datenveränderung zur Sachbeschädigung analog sein soll, sonst aber fast gar keine Ähnlichkeit zu ihr hätte. Es verbleibt gar keine andere Möglichkeit, um eine Verhaltensnorm in § 303a Abs. 1 StGB zu bringen. Man kann sie nur noch außerhalb des Strafrechts erhoffen, nach einem entsprechenden „Datenrecht" suchen und dann an dieses anknüpfen.

Wenn es ein ausgearbeitetes „Datenrecht" gäbe, das klärt, wer welche Veränderungen an Daten wann vornehmen darf bzw. nicht darf, oder zumindest festlegt, wer für den Einzelfall bestimmen darf, wem welche Veränderungen an Daten erlaubt sein sollen, würde sich immer noch die Frage stellen, ob man wirklich jede Verletzung dieser Regeln kriminalisieren muss. Bis zu dieser Frage gelangt man aber gar nicht. Es gibt schon kein „Datenrecht".[43]

Es gibt nur einzelne Ansätze zu einem solchen Rechtsgebiet, und diese Ansätze sind höchst heterogen. So gibt es ein Urheberrecht und ein Datenschutzrecht, mit weitreichenden Verboten, aber gerade zur Löschung von Daten auch Geboten. Und es gibt das Prinzip der Informationsfreiheit und diverse Sorgfalts- und Schutzpflichten, etwa im Bereich der Korruptionsbekämpfung, die den Verboten des Datenschutzes unmittelbar zuwiderlaufen. Vielfach ist das Verhältnis dieser auf dasselbe Verhalten bezogenen Gebote und Verbote ungeklärt. Eine gewisse Klärung der Rechte zur Beeinflussung von Daten erfolgt im Schuldrecht. An diese Klärung kann das Strafrecht aber nur selten anknüpfen, denn sie gilt nur im Verhältnis der Vertragsparteien zueinander. Wer ein Computersystem angreift, schließt darüber selten Verträge mit dem Betreiber oder anderen Personen, und es ist auch gar nicht der Sinn des Strafrechts, bloße Vertragsverletzungen zu sanktionieren.[44] Von einem Datenrecht, das die von § 303a StGB aufgeworfenen Fragen klärt, kann gegenwärtig keine Rede sein.[45]

[39] Vgl. z.B. *Renzikowski*, in: Joecks/Miebach (Hrsg.), Münchener Kommentar zum Strafgesetzbuch, Bd. 3, 2. Aufl. 2012, Vorbem. zu § 174 ff. Rn. 2 ff.

[40] Zum Streitstand *Knauer/Bose*, in: Spickhoff (Hrsg.), Medizinrecht, Kommentar, 2011, § 223 StGB Rn. 16 ff. m.w.N.

[41] Ein Arzt wird ggf. sogar nach § 323c StGB bzw. unechten Unterlassungsdelikten bestraft, wenn er sich in medizinisch dringenden Fällen nicht intensiv um eine Einwilligung des Patienten bemüht (BGH NJW 1983, 350).

[42] Es geht hier nur darum, dass über solche Konstruktionen Regelungen denkbar sind. Ob die hier jeweils angesprochenen Konstruktionen und insb. ihre Handhabung in der Rechtsprechung überzeugen, ist an dieser Stelle unerheblich.

[43] Vgl. *Popp* (Fn. 3), § 303a Rn. 3 f.

[44] Vgl. *Fischer* (Fn. 29), § 303a Rn. 6.

[45] Auf diesem rechtlichen Feld hat sich zwar vieles verändert, seit *Sieber*, ZStW 103 (1991), 779 (786 ff.), einen entsprechenden Befund formuliert hat. Ein einigermaßen konsistentes Daten- bzw. Informationsrecht gibt es aber – auch nur in dem begrenzten Umfang, in dem es als Basis strafrechtlicher Regelungen erforderlich wäre – weiterhin nicht.

Ob man statt an rechtliche Normen anzuknüpfen im Strafrecht ebenso auf leges artis zurückgreifen dürfte, muss hier nicht geklärt werden, denn es gibt nicht einmal unter Experten stabile Konventionen darüber, was erlaubt ist und was nicht. Insbesondere in RFCs (den „requests for comments", die maßgeblich technische Spezifikationen und intendierte Nutzungen beschreiben) geht es typischerweise darum, durch Konventionen technische Möglichkeiten zu schaffen, aber nicht deren Nutzung vom Missbrauch abzugrenzen. Sobald auch technische Laien involviert sind, kann von stabilen Konventionen erst recht keine Rede mehr sein.

§ 303a StGB als akzessorische Norm aufzufassen, wäre daher illusionär. Damit bleibt als letzte Möglichkeit, § 303a StGB in einem Einverständnismodell zu rekonstruieren. Dazu müssen die bislang vorhandenen Ansätze zu einem Datenrecht nur so weit reichen, dass sie die nötige Bestimmung der zur Einverständniserklärung befugten Person und ihrer Kompetenzen liefern.

d) Für ein Einverständnis maßgebliche Person?

Daten lassen sich nicht so eindeutig einem Inhaber zuordnen, wie das Sachenrecht Sachen einem Eigentümer zuordnet. Das liegt in ihrer Natur: Interesse besteht regelmäßig an ihrer Nutzung, die aber ganz anders als bei Sachen in keiner Weise ausschließlich sein muss, denn parallele Zugriffe bzw. das Anfertigen von Kopien sind technisch viel unproblematischer als bei Sachen. Unabhängig davon besteht ggf. ein selbständiges Interesse an der Geheimhaltung der Daten, am Ausschluss bestimmter Nutzungen oder Nutzer und u.U. gar ein Anspruch auf Löschung oder Änderung.[46] Solche Interessen liegen aber regelmäßig im Inhalt der Daten begründet, sind unabhängig von Zugriffsmöglichkeiten auf die Daten und stehen der Schutzrichtung des § 303a StGB (der den Erhalt und die Verfügbarkeit der Daten schützt) diametral entgegen.[47] Aus „datenrechtlicher" Perspektive gibt es also keinerlei Anlass, einer Person eine Inhaberstellung zuzuweisen.[48]

Hier zeigt sich, dass das Datenrecht keineswegs nur noch nicht so weit entwickelt ist, dass es die Inhaberschaft klären würde; vielmehr ist gar nicht damit zu rechnen, dass es sich jemals um die Bestimmung eines Inhabers bemühen wird. Wenn im Strafrecht überlegt wird, ob man als Inhaber den Eigentümer des Datenspeichers bzw. den Betreiber der Anlage,[49] denjenigen, „der die Daten in einem ‚Skripturakt' erzeugt, also ihre Speicherung selbst unmittelbar bewirkt hat",[50] den Auftraggeber der Speicherung[51] etc. ansehen sollte, verkennt das grundlegende Besonderheiten von Daten. Gesucht wird derjenige, der dem Eigentümer einer Sache am besten entspricht. Aus den angegebenen Gründen ist das aber eine Suche nach einem Phantom.

„Datenrechtlich" ist keine Inhaberschaft, sondern nur die Zuweisung jeweils spezieller Rechte und Pflichten sinnvoll. Diese sind regelmäßig nicht in einer Person und oft nicht einmal in einem für Einwilligungsfragen hinreichend überschaubaren Personenkreis konzentriert. Auch das Herausgreifen bestimmter Rechtsbeziehungen führt nicht weiter: Stellt man nur auf Nutzungsrechte[52] oder das Interesse an der Unversehrtheit der Daten[53] ab, ergibt sich eine insbesondere Datenschutzansprüchen zuwiderlaufende Schutzrichtung, sobald man aber auch im Inhalt der Daten begründete Rechte einbezieht, wird der Tatbestand überdehnt.

Die Bestimmung eines „Inhabers" der Daten kann nur in den besonders einfachen Ausnahmefällen gelingen,[54] in denen sich zufälligerweise alle betroffenen Interessen in einer Person bündeln, etwa eine Privatperson eigene private Daten auf einem eigenen Rechner ablegt und der grundsätzlich ohne Beziehung dazu stehende Täter diese Daten löscht. Die Bemühungen, „Fallgruppen" für die „Fremdheit der Daten" zu bilden und den Tatbestand so zu konturieren,[55] verfolgen deshalb keinen überzeugenden Ansatz. § 303a StGB ist primär als Wirtschaftsstrafrecht gedacht und müsste auch in wesentlich komplexeren Fallgestaltungen handhabbar bleiben. Die Frage nach der Inhaberschaft ist nicht nur bislang umstritten, sondern unentscheidbar und das Einwilligungsmodell strukturell ungeeignet, um die Komplexität der sedes materiae zu erfassen.

> *Beispiel 3*: Heute sieht ein realistisches Szenario z.B. so aus, dass ein Unternehmen (A) standardisierte Online-Shops für seine Kunden entgeltlich hostet (d.h. grds. auf eigenem Server zum Abruf durch Nutzer bereit hält) und deren Daten gegen Bezahlung teilweise auf Cloud Storage (über das Internet ansprechbaren Speicherplatz) eines anderen Anbieters (B) auslagert. Dessen Speichermedien

[46] Näher z.B. *Meinhardt* (Fn. 3), S. 152 ff.

[47] Vgl. *Wieck-Noodt* (Fn. 22), § 303a Rn. 4; *Kindhäuser*, Strafrecht, Besonderer Teil, Bd. 2, 6. Aufl. 2011, § 24 Rn. 10. Gleichwohl wurde in BT-Drs. 10/5058, S. 34 auch auf sie abgestellt.

[48] Dies und nicht die Komplexität der Rechtsbeziehungen ist hier der entscheidende Unterschied. Auch an Sachen können zahlreiche Rechte verschiedener Personen bestehen, die sich größtenteils aus dem Eigentum herleiten. Ein entsprechendes Rechtsinstitut, welches bei Daten im Zentrum entsprechender Rechtsgeflechte stehen würde, wäre wegen ihres besonderen Naturells aber nicht sinnvoll.

[49] Vgl. zu diesen (oft nicht einmal unterschiedenen) Varianten § 62 S. 2 des Explanatory Reports zur Cybercrime-Convention; *Stree/Hecker*, in: Schönke/Schröder, Strafgesetzbuch, Kommentar, 28. Aufl. 2010, § 303a Rn. 3 m.w.N.

[50] BayObLG JR 1994, 476 (477) m. Anm. *Hilgendorf*. Dabei stützt sich das Gericht auf *Welp*, IuR 1988, 443 (447 f.), der selbst bemerkt: „Für diese Annahme spricht – in Ermangelung aller normativen Vorgaben – nichts weiter als eine gewisse Plausibilität" (unter eingehender Erörterung entsprechend *Meinhardt* [Fn. 3], S. 119-166), und auch letztere erweist *Popp*, JuS 2011, 385 (388), als Täuschung.

[51] Vgl. auch dazu *Popp*, JuS 2011, 385 (388 f.).

[52] So etwa *Hoyer*, in: Rudolphi u.a. (Hrsg.), Systematischer Kommentar zum Strafgesetzbuch, 119. Lfg., Stand: September 2009, § 303a Rn. 5 f.

[53] *Weber* (Fn. 3), § 12 Rn. 48.

[54] Vgl. *Tolksdorf* (Fn. 3), § 303a Rn. 12-13.

[55] *Fischer* (Fn. 29), § 303a Rn. 5 ff.; ausf. *Marberth-Kubicki*, Computer- und Internetstrafrecht, 2. Aufl. 2010, Rn. 128-136.

sind als Kreditsicherheit übereignet (an C). Um Speicherplatz und damit Kosten zu sparen, möchte A nun große Dateien seiner Kunden komprimieren. Seine Kunden, die die Daten als Teil ihrer Onlineshops in das System des A (und damit zugleich das des B bzw. C) eingespielt haben, würden dabei keine Daten verlieren, denn die Kompression würde A nur mit einem verlustlos arbeitenden Algorithmus durchführen. Freilich wird das Speicherabbild der Datei (also Daten) verändert. Daran haben die Kunden nicht nur kein Interesse, es stört sie sogar, denn der Zugriff auf die Online-Shops könnte langsamer werden (weil die Dekompression jeweils Rechenleistung erfordert). Auch B, in dessen System die Daten liegen, und C haben Interesse daran, dass die Daten nicht komprimiert werden, weil sie ihre Einnahmen erhalten wollen (was wiederum nur mittelbaren Bezug zu den Daten hat).

Hier gibt es nicht *den* Betreiber bzw. Eigentümer des Computersystems und nicht *den* Inhaber der Daten. Jeder der Beteiligten hat diese Rollen in jeweils einer gewissen Hinsicht inne. Ein solchermaßen „mehrschichtiger" Aufbau eines Computersystems ist heute keine seltene Sondersituation, sondern in der Wirtschaft sehr üblich. So oder so ähnlich sind viele Onlineshops, Webmail-Angebote, soziale Netzwerke, Mailbox-Systeme, Lernplattformen etc. konstruiert.

In Fällen wie *Beispiel 3* Strafbarkeitsrisiken zu schaffen, wird weder der Situation gerecht, noch entspricht es der intendierten Schutzrichtung des § 303a StGB. Ob A sein System um eine Kompressions-Komponente erweitern darf oder nicht, muss in den zivilrechtlichen Vertragsbeziehungen geklärt werden, und auf Verstöße kann ggf. mit Sekundäransprüchen reagiert werden. § 303a StGB erfasst den Fall aber grundsätzlich, und das Merkmal „rechtswidrig" vermag ihn nicht eindeutig aus dem Tatbestand auszugrenzen.

Tatsächlich wird § 303a StGB von Gerichten auch bereits auf computerbezogene Vertragsverletzungen angewendet. Das Entfernen eines Net-Locks bzw. SIM-Locks – d.h. das Aufheben einer Programmsperre, die es verhindert, ein von Netzbetreibern an ihre Kunden subventioniert verkauftes Handy vertragswidrig in Netzen der Konkurrenz zu verwenden – wurde bereits nach § 303a Abs. 1 StGB abgeurteilt.[56] Das Handy und die betroffenen Datenträger standen längst im Eigentum des Käufers. Die Veränderung der Daten beseitigte nur eine Funktionseinschränkung des Computersystems im Handy. Die Verurteilung nach § 303a Abs. 1 StGB sanktioniert also die Verletzung einer vertraglichen und ggf. urheberrechtlichen Pflicht[57] des „Handybesitzers", die Funktionsbeeinträchtigung seines Eigentums und lizensierter Programme zu dulden. Das ist zur Sachbeschädigung nicht nur nicht mehr analog, sondern läuft direkt konträr, denn der (mit seinem eigenen Verhalten stets einverstandene) Eigentümer und „Inhaber" (inkl. seiner Helfer) wird bestraft.

Auf diese Weise werden die ausdifferenzierten gesetzgeberischen Entscheidungen über die Sanktionierung von Urheberrechtsverstößen durch Haftung, Bebußung oder – nur in besonderen Fällen – Bestrafung missachtet und Vertrags- und Strafrecht vermengt.[58] Das hat beträchtliche Konsequenzen. Beziehungen zwischen Unternehmen und ihren Kunden werden regelmäßig durch Daten abgebildet und gesteuert, die in einem Computersystem hinterlegt sind. Von ihnen hängt es ab, welche Leistungen der Kunde tatsächlich erhält. Ihre Änderung betrifft also regelmäßig berechtigte und meist sogar vertragsgegenständliche Interessen. Auf der Basis der SIM-Lock-Entscheidungen läuft jeder Mitarbeiter eines Unternehmens, wenn er Eintragungen in die Unternehmens-EDV tätigt, die den vertraglichen Ansprüchen eines Kunden nicht gerecht werden, – selbst wenn er dabei den internen Vorgaben entsprechend handelt – Gefahr, nach § 303a Abs. 1 StGB bestraft zu werden.

e) Inhalt möglicher Einverständniserklärungen?

aa) In den obigen *Beispielen 1* und *2* (der Ampel und der Videoüberwachung) scheint zunächst alles für eine Lösung im Einverständnismodell zu sprechen. Vertragliche und urheberrechtliche Beziehungen spielen in diesen Beispielen keine Rolle. Der Betreiber der Ampel bzw. der Kamera erscheint unproblematisch als „Inhaber" der Daten. Er hat sich durch den Betrieb der Geräte konkludent mit ihrer ordnungsgemäßen Beeinflussung durch Dritte (Drücken des Knopfes, Gehen vor der Kamera) einverstanden erklärt, nicht aber mit manipulativem Verhalten. In den Varianten dieser Fälle manipuliert der Täter aber gerade Systemfunktionen. Das Einverständnis scheint zumindest hier erlaubtes von unerlaubtem Verhalten abzugrenzen, also die nötige Verhaltensregel zu liefern.

Ein Einverständnis kann nach ganz herrschender Ansicht aber nicht mit beliebigen Einschränkungen versehen werden. Vielmehr muss sich zur Tatzeit anhand der einem fiktiven Beobachter verfügbaren Informationen beurteilen lassen, ob das Verhalten des Täters der Einschränkung unterfällt oder nicht. So kann ein Supermarktbetreiber, der sein Geschäft dem Publikum öffnet, Personen mit Diebstahlsabsichten nicht wirksam davon ausnehmen.[59] Die Einschränkung seines Einverständnisses würde nur an Tatsachen anknüpfen, die beim Betreten des Geschäfts (also in der Tatsituation) nicht erkennbar sind (nämlich innere Tatsachen, ggf. Sonderwissen und ggf. entfernte Umstände wie Vorbereitungshandlungen des Diebes). Das aber ist unzulässig; Diebstahlsabsichten machen das Betreten nicht zu einem Hausfriedensbruch.

Ebenso ist das in den Beispielsfällen. In *Beispiel 1* ist das Drücken des Knopfes vom Einverständnis gedeckt. Solange es nicht in den Knopf beschädigende Gewalt ausartet, darf man den Knopf auch rhythmisch mehrfach drücken. Dass der

[56] AG Nürtingen MMR 2011, 121; AG Göttingen MMR 2011, 626 m. abl. Anm. *Neubauer*. Abl. auch *Stree/Hecker* (Fn. 49), § 303a Rn. 3 m.w.N.

[57] I.d.S. auch *Wolff* (Fn. 4), § 303a Rn. 2, 10 ff.

[58] Diese Vermengung hat bislang v.a. in der Diskussion um die unbefugte Verwendung von Daten nach § 263a Abs. 1 StGB viel Aufmerksamkeit und Kritik erfahren. Vgl. dazu *Mühlbauer*, wistra 2003, 244 (247) m.w.N.

[59] Vgl. *Fahl*, in: Satzger/Schmitt/Widmaier (Hrsg.), Strafgesetzbuch, Kommentar, 2009, § 123 Rn. 7 m.w.N.

Täter in der „kriminellen“ Variante durch seinen Rhythmus das Programm zum Absturz bringt, ist äußerlich während der Handlung nicht zu erkennen (nicht einmal für Experten, denn bei dieser Art von Manipulation wird ja ein Programmierfehler ausgenutzt, der behoben würde, wenn er bekannt wäre), sondern erst an der späteren Folge. Ebenso ist es in *Beispiel 2* grundsätzlich akzeptiert, sich von Überwachungskameras filmen zu lassen. Dabei darf man auch Armbanduhren tragen und mit der Reflektion des Sonnenlichts spielen. Das Verhalten in der „kriminellen“ Variante ist wieder äußerlich nicht als Manipulation eines Computers zu erkennen.

Dass das Einverständnismodell auch in diesen scheinbar einfachen und klaren Fällen scheitert, hat nichts damit zu tun, dass die Computer in ihnen etwas verborgen sind. Das Einverständnismodell scheitert aus denselben Gründen, wenn ein Arbeitgeber einem Mitarbeiter den Umgang mit seinen Computern unter dem Vorbehalt erlaubt, dass dieser sie nicht manipuliert. Der Grund des Scheiterns besteht schlicht darin, dass in der Einschränkung, Manipulationen blieben verboten, keine Verhaltensregel ausgedrückt wird. Diese Einschränkung ist nämlich nichts anderes als der Vorbehalt, das Verhalten des anderen nachträglich in einer Gesamtschau beurteilen und dabei sogar die Kriterien dieser Beurteilung erst nachträglich entwickeln zu wollen.

Nach ganz gängigem strafrechtlichem Verständnis ist hier die Einschränkung unwirksam, während das Einverständnis zumindest insoweit wirksam bleibt, als es eine Bestrafung ausschließt (was einer z.B. zivilrechtliche Haftung begründenden Beurteilung als rechtswidrig nicht entgegensteht). Das Gesetzlichkeitsprinzip wird gewissermaßen innerhalb des Einverständnismodells verteidigt. Folge davon ist zunächst nur die akzeptable (und vom Gesetzlichkeitsprinzip gezielt in Kauf genommene) Konsequenz, dass strafwürdiges Unrecht unsträflich bleibt. Es lassen sich aber auch Fälle bilden, in denen ein sozial adäquat handelnder Täter Daten eines anderen äußerlich erkennbar gegen dessen Interessen verändert:

bb) So genügt für den Widerruf eines Fernabsatzgeschäfts nach §§ 312d Abs. 1 S. 1, 355 Abs. 1 S. 2 BGB eine Erklärung in Textform (§ 126b BGB), also auch eine Email.[60] Ginge es rein nach den Präferenzen des Verkäufers, wäre er mit dem Erhalt einer solchen Email meist nicht einverstanden. Das hätte die absurde Konsequenz, dass der Verbraucher sich bei seinem Widerruf wegen der Veränderung der Daten auf dem Computer des Verkäufers nach § 303a Abs. 1 StGB strafbar machen würde, denn jede Zusendung einer Email geht notwendig mit der Veränderung von Daten auch im Empfangssystem einher.

Es hilft nicht viel, hier §§ 312d Abs. 1 S. 1, 355 Abs. 1 S. 2 BGB als Rechtfertigung für die Zusendung der Email zu bemühen. Der Fall lässt sich mit anderen für den Empfänger unangenehmen Inhalten und auch anderen allgemein akzeptierten Formen der Veränderung von Daten auf vernetzten Computern beliebig variieren. Letztlich muss unabhängig von einem Einverständnis sichergestellt werden, dass sozialadäquates Verhalten nicht als Datenveränderung bestraft wird. Ob man dies über selbständige Normen erreicht oder die rein tatsächliche Eröffnung von Zugriffsmöglichkeiten als konkludente Einverständniserklärung in alle sozialadäquaten Zugriffe auslegt, bleibt sich im Ergebnis gleich: Man verlässt das Einverständnismodell und setzt eigene normative Wertungen an die Stelle einer Erklärung bzw. erkennbarer Präferenzen. Das geschieht im Zeitpunkt der nachträglichen strafrechtlichen Beurteilung des Falles. Die Tat wird nicht anhand zur Tatzeit feststehender Verhaltensregeln beurteilt, sondern nachträglich wertend betrachtet. Insoweit hat das Abstellen auf die Sozialadäquanz den gleichen Effekt wie das Abstellen auf die Manipulationsfreiheit. Es geschieht hier aber nicht mehr bei der Frage der Reichweite der Einverständniserklärung bzw. sonstiger Rechtfertigungen, so dass die Konturlosigkeit nicht mehr im Rahmen der Einverständnisdogmatik abgefangen werden kann. Vielmehr ist der Tatbestand unmittelbar selbst betroffen.

cc) Einverständnismodelle schützen Selbstbestimmungsrechte. Sie können nur dann zur Tatzeit konkrete Verhaltensnormen liefern, wenn die Entscheidungsmöglichkeiten und ihre Konsequenzen dem Berechtigten bekannt und ihm nicht gleichgültig sind. Schon daran fehlt es in den von § 303a StGB erfassten Situationen zumindest bei Computer-Laien aber regelmäßig.

Der „normale PC-Nutzer“ etwa ist bei der Installation eines neuen Programms sicherlich damit einverstanden, dass die Programmdateien auf „freie“ Festplattenbereiche kopiert werden. Zugleich ist er sicherlich nicht damit einverstanden, wenn Dateien des Betriebssystems oder anderer Anwendungsprogramme gezielt sabotiert werden. Bei sehr verbreiteten PC-Betriebssystemen ist es aber ein üblicher Teil der Installation von Anwendungsprogrammen, Bibliotheksdateien mit Programmfunktionen, die zum Betriebssystem gehören bzw. mit anderen Anwendungsprogrammen gemeinsam verwendet werden, gegen neuere Versionen dieser Dateien auszutauschen. Meist ist das nicht mit Nachteilen verbunden, kann aber (auch ohne Schädigungsabsicht) zu Störungen bis hin zur Unbrauchbarkeit der Betriebssysteminstallation führen. Verneint man hier ein Einverständnis des Nutzers mit dem risikobehafteten Ersetzen der älteren Bibliotheken, bedeutet das, dass professionelle Programmierer sich regelmäßig strafbar machen. Bejaht man ein Einverständnis, hat das in der tatsächlichen Vorstellung der meisten heutigen PC-Benutzer, die sich nicht für den Aufbau des Betriebssystems und der Anwendungsprogramme interessieren, kaum eine Grundlage.

f) Das crimen extraordinarium für den Umgang mit Daten

Auch ein Einverständnismodell scheitert also: Erstens ist in vielen praktisch bedeutsamen Fällen unklar, auf wessen Einverständnis es ankäme.[61] Das liegt nicht an einem Mangel bisheriger Klärungen, sondern in der Vielschichtigkeit der Interessen an Daten, die sich – anders als Sachen – nicht einfach einem Inhaber zuordnen lassen. Zweitens liegt es in der Natur vernetzter EDV-Systeme, dass zahlreiche Einwirkungen auch auf eindeutig „fremde“ Daten unabhängig vom Einverständnis des „Inhabers“ erlaubt sein müssen, ohne dass

[60] *Ellenberger*, in: Palandt, Bürgerliches Gesetzbuch, Kommentar, 71. Aufl. 2012, § 126b BGB Rn. 3.

[61] Vgl. *Popp* (Fn. 3), § 303a Rn. 3 f.

in der Vernetzung ein generelles Einverständnis mit allen Einwirkungen (das den „Inhaber“ schutzlos stellen würde) liegen kann. Die Abgrenzung der „sozialadäquaten“ Einwirkungen von verbotenen kann aber mangels ausgearbeiteter Regeln nicht zur Tatzeit, sondern erst im Nachhinein erfolgen. Drittens fehlt vielen Betroffenen das nötige Wissen, um im Rahmen eines Einverständnismodells kompetent handeln zu können, und dieses Wissen lässt sich auch nicht jeweils aktuell (z.B. abgesichert durch entsprechende Aufklärungspflichten) kurzfristig herstellen.

Wenn § 303a Abs. 1 StGB mittels des Einverständnismodells rekonstruiert wird, entbehrt das deshalb der dazu nötigen Grundlagen. In Wirklichkeit wird dabei nur kaschiert, dass der Rechtsanwender die Tat an seinen eigenen Wertungen misst statt an einer zur Tatzeit bestehenden Verhaltensnorm. § 303a Abs. 1 StGB wird dabei so gehandhabt, als stünde dort: „Wer mit Daten umgeht, kann bestraft werden, wenn das dem Richter nachträglich angemessen erscheint.“ Das aber ist nichts anderes als ein allein nach Ermessen des Gerichts festzusetzendes Delikt, das crimen extraordinarium[62] für den Umgang mit Computern. Genau das aber soll der Bestimmtheitsgrundsatz verhindern.

5. Das Scheitern der Analogie

Rechtliche Analogien bestehen in einer (auf Ähnlichkeit gegründeten) Anpassung von Tatbestandsvoraussetzungen und Wertmaßstäben, nicht aber in ihrer Beseitigung. Die Datenveränderung in Analogie zur Sachbeschädigung auszuformen ist im geltenden Recht deshalb gescheitert. Das wirft einerseits die Frage auf, ob die dargestellten Gründe dafür beseitigt und die Analogie dadurch doch noch hergestellt werden können. Andererseits wirft es die Frage nach den Konsequenzen dieses Scheiterns auf.

a) Korrekturmöglichkeiten über den Datenbegriff

Zunächst ist der Datenbegriff so weit abstrahiert, dass er kein Analogon zur Sache mehr ist. Ein engerer und damit tatbestandlich handhabbarer Datenbegriff wäre indes durchaus möglich. Als Merkmal, auf das sich dabei abstellen ließe, kommt die Funktion der Daten im Rahmen eines Computersystems in Betracht.[63] Zudem haben Daten oft auch einen die rein technische Betrachtung transzendierenden Sinn (Informationsgehalt), der sich nur dem Menschen, der den Datenverarbeitungsvorgang gestaltet oder sein Ergebnis wahrnimmt, erschließt.[64] Mit einem daran anknüpfenden Datenbegriff könnten immerhin Veränderungen, die die Funktion und den Sinn der Daten in ihrem konkreten Verwendungsbereich gar nicht betreffen – z.B. bloßes Umcodieren, das verlustlose Komprimieren in *Beispiel 3* etc. – und deshalb auch keine Einbußen irgendeines schützenswerten Gutes bewirken können, aus dem Tatbestand ausgeschieden werden. Das wäre ein erster Schritt, um vor allem Strafbarkeitsrisiken von professionell (und dabei lege artis) mit Computersystemen umgehenden Personen zu reduzieren.

Auch wenn die Funktion bzw. der Sinn der Daten betroffen ist, kann die Veränderung vorteilhaft sein. Das ist der Normalfall des Umgangs mit Computern. Er sollte von keinem Straftatbestand erfasst werden. Dass die Tathandlungen des § 303a StGB auch ihn erfassen, liegt am Bestreben, Beweiserleichterungen zu schaffen. Dass der Inhalt irgendwelcher Speicherstellen geändert wurde, lässt sich leichter nachweisen als die Schädigung von Funktion oder Sinn. Diese Beweiserleichterungen sind aber gar nicht erforderlich. In der Regel wäre wohl mit der Mitwirkung der Opfer zu rechnen. Wo eine solche Mitwirkung unterbleibt, ist ein strafrechtlicher Schutz entbehrlich, zumal nach § 303c StGB sogar ein Antragserfordernis besteht. Würde man zu einem konkreteren Datenbegriff übergehen, könnte man daher auch die Tathandlungen auf nachteilige Veränderungen beschränken.

Beides geschieht tatsächlich schon heute in den meisten Tatbeständen, die scheinbar den gleichen Datenbegriff verwenden wie § 303a StGB (oder sogar mangels Verweis auf § 202a Abs. 2 StGB einen tendenziell noch weiteren): § 238 Abs. 1 Nr. 3 StGB erfordert einen Personenbezug und die Verwendung der Daten für Bestellungen oder Kontaktaufnahme durch Dritte, stellt also konkrete Anforderungen an Sinn und Funktion der Daten. In § 263a StGB müssen die unrichtigen oder unvollständigen Daten den Sinn einer falschen Tatsachenbehauptung haben. Die unbefugte Verwendung von Daten muss in der Weise „täuschungsäquivalent“ sein, dass die Daten eine tatsächlich nicht bestehende Befugnis ausdrücken. Die Daten müssen in ihrer konkreten Verwendung also wieder einen eng vorgegebenen Sinn haben. Eine Funktion muss ihnen außerdem zukommen, denn sie müssen eine Vermögensdisposition und einen Vermögensschaden bewirken. § 269 Abs. 1 und 274 Abs. 1 Nr. 2 StGB setzen u.a. Beweiserheblichkeit, also ebenfalls einen näher bestimmten Sinn voraus. Indirekt setzt sogar § 303b Abs. 1 Nr. 2 StGB eine Funktion der Daten voraus, denn sonst könnten sie keine erhebliche Störung verursachen. Die Tatbestände werden jeweils nur durch eine Verletzung des genannten Sinns bzw. der betreffenden Funktion erfüllt. § 202a Abs. 1 StGB knüpft zwar nicht an die Funktion und den Sinn der Daten an (was auch dort zu einer bzgl. des Schutzzwecks problematischen Weite des Tatbestandes führt), fordert aber zumindest die Überwindung einer besonderen Zugangssicherung. Nur in § 202b StGB fehlen entsprechende Einschränkungen, und das wirft dort die gleichen Probleme auf wie in § 303a StGB.[65]

b) Unbestimmtheit mangels Verhaltensnorm

Den Datenbegriff und die Tathandlungen in der angegebenen Weise zu konturieren (so dass die Vorschrift nur mehr Veränderungen erfasst, die eine Funktion oder den Sinn beeinträchtigen), würde die Bestimmtheitsprobleme von § 303a StGB mildern, aber nicht lösen. Durch die Konturierung entstünde eine Analogie zur Beschädigung einer Sache. Doch ebenso wie bei weitem nicht jede Beschädigung einer Sache als straf-

[62] Vgl. dazu *Schreiber*, Gesetz und Richter, 1976, S. 29.

[63] Vgl. auch *Maurach/Schroeder/Maiwald* (Fn. 3), § 36 Rn. 36 m.w.N.

[64] Zu „semantischem“ vs. „syntaktischem“ Aspekt von Daten vgl. auch *Schmitz*, JA 1995, 478 (479).

[65] Zu den weiteren Problemen der Vorfelddelikte s.u. Fn. 81.

bares Unrecht erfasst wird, darf auch nicht jede nachteilige Veränderung von Daten als solches behandelt werden, denn weder Sachen noch Daten haben einen Selbstzweck oder eine eigene Würde. Eine Lösung des Bestimmtheitsproblems ergäbe sich daher erst, wenn sich auch für das Merkmal „fremd" der Sachbeschädigung eine Entsprechung entwickeln ließe.

Das vom Tatbestand der Sachbeschädigung in Bezug genommene Sachenrecht ist der über Jahrtausende wohl am besten ausgearbeitete Teil unserer Rechtsordnung überhaupt. Auch in den Gewohnheiten der Bevölkerung ist er tief verwurzelt. Das zeigt sich in einer höchst bemerkenswerten Eigenschaft von § 303 StGB: Die Sachbeschädigung führt gar nicht zu einer unmittelbaren Beeinträchtigung eines Rechtsgutsträgers. Der Freiheit des Eigentümers tut die Tat erst dann Abbruch, wenn er die Sache später tatsächlich verwenden möchte, wegen der Beschädigung bzw. Zerstörung aber nicht verwenden kann. Die Sachbeschädigung antizipiert diese Verletzung und beinhaltet in diesem Sinne ein Vorfelddelikt zur eigentlichen Schädigung. Das fällt heute gar nicht mehr auf, weil das Sachenrecht derart gut und stabil ausgearbeitet ist, dass uns die Unterscheidung zwischen Mein und Dein schon im Kindesalter in Fleisch und Blut übergeht und wir die Verletzung von Eigentum wie eine tatsächliche Beeinträchtigung des Eigentümers empfinden.

Das „Datenrecht" hingegen liefert heute Argumente, um zivilrechtliche Streitigkeiten im Nachhinein zu entscheiden. Das ist, wenn man in Rechnung stellt, wie jung das Rechtsgebiet ist, schon ziemlich viel. Es ist aber viel weniger als ein System vor der Tat feststehender Verhaltensnormen, und das bräuchte ein Straftatbestand der Datenveränderung, um darauf verweisen zu können.[66] Dieser „Mangel" kann auch nicht von den Strafgerichten durch konkretisierende Auslegung des § 303a StGB behoben werden.[67] Erstens wäre es mehr als eine Herkulesaufgabe, die nötige Systematisierung der Grundzüge des Datenrechts nebenbei zu erledigen. Zweitens könnten sie sich dabei nur Verhaltensnormen ausdenken, die aus dem Gesetz in keiner Weise zu ersehen wären. Drittens würde es dem gerade aus dem Strafrecht hinausgehenden Verweis zuwiderlaufen, wenn ausgerechnet die Strafgerichte den Inhalt der Pflichten klären würden.

Zwischen dem Sachenrecht und dem „Datenrecht" liegen Jahrtausende rechtlicher und sozialer Entwicklungen. Vielleicht könnte sich manches auch zügiger vollziehen. Das „Datenrecht" steht aber vor der besonderen Herausforderung, keinen „Inhaber" der Daten als „Eigentümerersatz" bestimmen und diesem die Entscheidungen über „seine" Daten übertragen zu können, sondern die maßgeblichen Verhaltensregeln in viel größerem Umfang selbst entwickeln zu müssen, als das im Sachenrecht erforderlich war. Diese Entwicklung darf keinesfalls einfach als bereits geschehen postuliert werden.

Deshalb ist es heute letztlich unmöglich, den aktuellen § 303a StGB in einer dem Gesetzlichkeitsprinzip entsprechenden Weise zu handhaben und muss insbesondere auch eine verfassungskonforme Auslegung scheitern. In dem großenteils gründlich vorbereiteten und durchgeführten Gesetzgebungsverfahren zum 2. Gesetz zur Bekämpfung der Wirtschaftskriminalität v. 15.5.1986 ist § 303a StGB spät, überstürzt und – gerade auch bzgl. der Frage, ob es der Strafbarkeit von Datenveränderungen überhaupt bedarf – entgegen dem wissenschaftlichen Rat v.a. von *Sieber* eingefügt worden.[68] Dabei hat man sich mit der vordergründig plausiblen, bei näherem Hinsehen aber in zentralen Punkten gar nicht durchgeführten Analogie zur Sachbeschädigung begnügt und übersehen, dass dem Tatbestand sogar die Verhaltensnorm fehlt. Ein Delikt ohne Verhaltensnorm, die nach allgemeinen Kriterien im Voraus klärt, welches Verhalten zulässig ist, und welches nicht, ist aber schlechterdings unbestimmt.[69] § 303a StGB sollte deshalb vom Bundesverfassungsgericht aufgehoben werden.[70]

6. Die Vorgaben der Cybercrime-Convention

Nach einer Aufhebung stellt sich nicht nur die Frage, ob die Vorschrift kriminalpolitisch überhaupt nötig ist.[71] Deutschland ist nach Art. 4 Abs. 1 der Cybercrime-Convention vielmehr verpflichtet, Datenveränderungen unter Strafe zu stellen, und die bislang auf § 303a Abs. 1 StGB bezogene Analyse und Kritik trifft ohne nennenswerte Abweichungen[72] auch auf jene Vorschrift zu.[73]

Art. 4 Abs. 1 der Cybercrime-Convention enthält sogar eine eigene Begehungsvariante der Verschlechterung („deterioration") von Computerdaten. In ihr tritt das Scheitern der Ana-

[66] Ob sich dazu wirklich ein eigenständiges Rechtsgebiet herausbilden muss oder nicht eher vielschichtige Rechtsprobleme innerhalb vorhandener Systematik bzw. unter Erweiterung traditioneller Rechtsgebiete zu lösen sind, ist eine ganz andere Frage. Mit guten Gründen in letzterem Sinne bereits *Haft*, NStZ 1987, 6 (10).

[67] A.A. *Fischer* (Fn. 29), § 303a Rn. 5 f.

[68] Vgl. BT-Drs. 10/5058, S. 34. Er hielt §§ 303a, 303b StGB für entbehrlich. Für den Fall, dass der Gesetzgeber sich für Gesetzgebung in dieser Richtung entscheiden sollte, riet er jedenfalls zu einer in § 303 StGB eingebetteten Lösung, die diesen vorsichtig erweitert (*Sieber*, Informationstechnologie und Strafrechtsreform, 1985, S. 61). Das war damals richtig und wäre es heute immer noch.

[69] Wie sehr das auch die Praxis irritiert, zeigt das Urteil des AG Böblingen WM 1990, 64 (65). Der Versuch einer Subsumtion wird nicht einmal ansatzweise unternommen. Stattdessen werden die für den Tatbestand relevanten Umstände bei der Strafzumessung strafschärfend berücksichtigt.

[70] Vgl. oben Fn. 3.

[71] Die Fachserie 10 Reihe 3 (Rechtspflege, Strafverfolgung) des Statistischen Bundesamts weckt Zweifel daran, denn sie weist für das Jahr 2010 deutschlandweit immerhin nur 67 Aburteilungen bei 44 Verurteilungen aus (S. 40 f.), und die Werte der Vorjahre waren ähnlich.

[72] Sie gründen in dem etwas anderen Datenbegriff, dessen Abweichungen sich in den hier bedeutsamen Punkten aber nicht auswirken.

[73] Insbesondere soll er ebenso der Sachbeschädigung nachgebildet sein. In § 61 des Explanatory Reports wird ausführlich eine Gleichsetzung der einzelnen Begehungsvarianten mit den Begehungsformen der Sachbeschädigung (sowie zusätzlich die Unterdrückensvariante) erörtert.

logie zur Sachbeschädigung offen zu Tage: Entspräche die Norm der Sachbeschädigung, würde jede Begehungsform eine Verschlechterung voraussetzen. Sie wäre also nicht eine Begehungsform unter anderen, sondern die Grundform. Tatsächlich aber ist die neutrale Veränderung („alteration") die Grundform zur Schädigung, Löschung und Verschlechterung („damaging, deletion, deterioration"), zu der – wie in der deutschen Regelung – die Unterdrückung selbständig hinzutritt.[74] Von einer Verschlechterung kann überhaupt nur in dem Spezialfall die Rede sein, dass Funktion und Sinn der Daten eine qualitative Bewertung der Veränderung zulassen.

Auch im Übrigen besitzt Art. 4 Abs. 1 der Cybercrime-Convention die gleiche Struktur wie § 303a Abs. 1 StGB. Insbesondere enthält er das gleiche Merkmal „rechtswidrig" („without right").

Ein wesentlicher Unterschied besteht aber: Die Cybercrime-Convention ist kein unmittelbar auf den Bürger anwendbares Strafrecht, sondern eine Verpflichtung der Vertragsstaaten, entsprechendes Strafrecht selbst zu erlassen. Dabei verbleiben den Staaten Spielräume zur Konkretisierung. Würde man vom Gebot einer möglichst wortgetreuen Umsetzung ausgehen, wäre jede nationale Entsprechung zu Art. 4 Abs. 1 der Cybercrime-Convention unvermeidlich unbestimmt, würde also gegen Art. 7 Abs. 1 der EMRK verstoßen. Die Konvention weiß sich aber selbst der EMRK verpflichtet; ihre Präambel und auch ihr zum Prozessrecht gehörender Art. 15 dokumentieren das ausdrücklich. Das spricht dafür, die Umsetzungsverpflichtungen jeweils als Pflicht zu einer Art. 7 EMRK genügenden Umsetzung aufzufassen, was die unvermeidlichen Eingrenzungen auch vom Standpunkt der Cybercrime-Convention rechtfertigt.

Richtigerweise wird man Art. 4 Abs. 1 der Cybercrime-Convention daher zunächst das Gebot zu entnehmen haben, auf nationaler Ebene eine ordentlich ausgearbeitete Analogie zur Sachbeschädigung zu erlassen. Die innerstaatliche Norm wäre dann enger als die Formulierung der Cybercrime-Convention, entspräche aber gerade ihrer Intention.

Das beseitigt indes nur einen Teil des Bestimmtheitsproblems, denn weiterhin wird eine Klärung der zugrundeliegenden „datenrechtlichen" Frage vorausgesetzt, welches Verändern bzw. Unterdrücken zulässig und welches unzulässig („without right") ist. Über ein hinreichend ausgearbeitetes Datenrecht verfügt heute aber kein Staat. Daran wird sich in absehbarer Zeit auch nichts ändern. Die Bezugnahme auf das „Datenrecht" in seinem jeweiligen Ausarbeitungszustand ist insoweit sinnvoll, als datenrechtlich erlaubtes Verhalten im Strafrecht nicht zu verbieten ist. Eine dem Bestimmtheitserfordernis aus Art. 7 Abs. 1 EMRK genügende Umsetzung muss den Tatbestand aber darüber hinaus weiter eingrenzen.

Es gibt derzeit keinen anderen Weg, als dieses Problem durch die Aufnahme weiterer strafrechtlicher Tatbestandsvoraussetzungen zu lösen. Mit deren Hilfe müssen ein Unwert umschrieben und ein Schutzzweck gekennzeichnet werden und daraus eine strafrechtliche Verhaltensnorm entstehen.[75]

7. Eine konventionskonforme Notlösung de lege ferenda

Die Konvention gibt dazu sogar ein ausgearbeitetes Mittel an die Hand: Nach Art. 4 Abs. 2 können Staaten nach entsprechendem Vorbehalt die Strafbarkeit an das Entstehen eines schweren Schadens knüpfen.[76] Durch eine solche Einschränkung wird eine akzeptable Bestimmtheit des Tatbestandes hergestellt: Die Norm verbietet und sanktioniert dann schädigende Datenveränderungen. Im Schaden liegt ein unrechtsbegründendes Merkmal; neutrale und vorteilhafte Handlungen lassen sich davon abgrenzen. Auf die Person des Geschädigten kann dann auch hinsichtlich einer eventuellen Einwilligung abgestellt werden. Diesen Weg geht z.B. Österreich in § 126a Abs. 1 öStGB.[77]

Zwar sehen weder Art. 19 WVRK[78] noch die Konvention selbst ausdrücklich eine Möglichkeit vor, die Erklärung dieses Vorbehalts nachzuholen. Unter Umständen ist dies auf völkergewohnheitsrechtlicher Grundlage aber bereits ohne Umwege möglich.[79] Jedenfalls steht den Staaten die Möglichkeit einer Kündigung der Cybercrime-Convention (dort Art. 47) verbunden mit einem Neubeitritt unter Anbringung des Vorbehalts (dazu Art. 42) offen. Wünschenswert wäre freilich eine einvernehmliche Anpassung von Art. 4 Abs. 1 der Cybercrime-Convention im Rahmen einer Überarbeitung, die zur Ergänzung und Aktualisierung auch anderer Stellen ohnehin bereits diskutiert wird.

Die Bemerkungen zur Cybercrime-Convention gelten für Art. 4 des Rahmenbeschlusses 2005/222/JI über Angriffe auf Informationssysteme[80] entsprechend. Ein Vorbehalt ist dazu zwar nicht zu erklären, die Vorschrift enthält aber von vornherein die Öffnungsklausel, dass „kein leichter Fall vorliegt".

Der Rückgriff auf ein wirtschaftliches Schadenserfordernis ist keine Ideallösung. Auch an Daten ohne monetären Wert kann ein strafrechtlich schützenswertes Interesse bestehen. Ein Schadenserfordernis wäre aber zumindest eine Zwischenlösung für die Zeit, bis eine bessere Begrifflichkeit und ein ausgereifteres Datenrecht zur Verfügung stehen. Ein tatbestandliches Schadenserfordernis hätte auch unmittelbare Vorteile für die Computersicherheit: Nicht zuletzt die Erfahrungen mit der Entwicklung des open source-Betriebssystems Linux haben gezeigt, dass ungewollte Manipulationen von

[74] S.o. III. 3. b).

[75] So aktuell ebenfalls *Sieber*, Internetstraftaten und Strafverfolgung im Internet, 69. DJT, Gutachten C, 2012, S. C43, C88 und C154 sowie *ders.* NJW-Beil. 2012, 86 (89). Wiederum sei darauf verwiesen, dass genau das auch in §§ 202a, 238, 263a, 269, 274 und 303b StGB geschieht.

[76] Erklärt haben diesen Vorbehalt bislang Aserbaidschan (15.3.2010), Litauen (10.5.2004) und die Slowakei (8.1.2008).

[77] Österreich gehört zwar zu den ersten Unterzeichnern der Konvention, hat sie aber bislang noch nicht ratifiziert.

[78] Wiener Übereinkommen über das Recht der Verträge v. 23.5 1969 (UNTS Vol. 1155, I-18232, S. 331 [336]; BGBl. II 1985, S. 926 [934]).

[79] Vgl. International Law Commission, Guide to Practice on Reservations to Treaties, 2011 (im Internet abrufbar unter: http://untreaty.un.org/ilc/texts/instruments/english/draft%20articles/1_8_2011.pdf [12.7.2012]; vorgesehen für Yearbook of the International Law Commission 2011 II/2), Richtlinien 2.3 bis 2.3.2.

[80] S.o. Fn. 12.

Computersystemen besonders gut vermieden werden können, wenn die Suche, Offenlegung und Behebung von Sicherheitslücken gefördert wird. Die Suche nach Sicherheitslücken grundsätzlich unter Strafe zu stellen, worauf der derzeitige § 303a Abs. 1 StGB weitgehend hinausläuft, ist deshalb kein effizienter Beitrag zur Computersicherheit, sondern mittel- und langfristig von Nachteil für sie. Der Unterschied zwischen sicherheitstechnisch oft gerade nützlicher Suche nach Sicherheitslücken und krimineller Manipulation des Systems kann daher mit einem Schadenserfordernis grundsätzlich plausibel markiert werden.[81]

Wo sich der Tatbestand anders nicht bestimmt fassen lässt, muss Strafrecht fragmentarisch sein. Einem solchen Fragment können zwar grundsätzlich weitere Fragmente zur Seite gestellt werden. So ließe sich z.B. erwägen, gesetzlich auch eine Fallgruppe vorzusehen, in der persönliche und wissenschaftliche (und damit über Inhalte näher bestimmte) Daten auch ohne wirtschaftlichen Schadenseintritt geschützt werden. Schon daraus ergäben sich aber wieder Probleme: Erstens ist ein solcher Schutz evtl. nur solange sinnvoll, wie diese Daten sich im Einflussbereich desjenigen befinden, der an ihnen ein Interesse hat. Sind sie hingegen in fremde Hände geraten, liefe ein Löschungsverbot gerade bei geheimen Daten seinem Interesse oft unmittelbar zuwider. Zweitens ist für persönliche und wissenschaftliche Daten oft zugleich das Datenschutzrecht einschlägig, das vom Grundsatz der Datenvermeidung und Löschpflichten geprägt ist. Wann ggf. auch Dritte befugt (oder gar gehalten) sind, diese Vorgaben umzusetzen, müsste ebenfalls geklärt werden. Hier zeigt sich deutlich, dass die Unbestimmtheit des Tatbestands der Datenveränderung nicht nur auf vagen Begriffen beruht. Ihr liegen vielmehr ungelöste echte Sachprobleme zugrunde, deren Lösung auch nicht kurzfristig und nicht von Fall zu Fall gefunden werden kann.

IV. Bestimmtheit durch Analogie

Bestimmtheitsgrundsatz und Analogieverbot sind im strafrechtlichen Gesetzlichkeitsprinzip so eng verwoben, dass Strafrechtler mit Analogien leicht Verstöße gegen den Bestimmtheitsgrundsatz assoziieren. Die ersten hier vorgetragen Überlegungen (oben II.) haben gezeigt, dass diese Assoziation für den Einsatz von Analogie als Regelungstechnik grundsätzlich unzutreffend ist. Möchte der Gesetzgeber mit einem Tatbestand strafrechtliches Neuland beschreiten, kann seine Formulierung in Analogie zu etabliertem Strafrecht geradezu geboten sein.

Analogieschlüsse sind aber Regeln unterworfen, die beachtet werden müssen. In Rechtsgebieten mit Analogieverbot gerät das leicht in Vergessenheit und führt dann zu Rechtssätzen, die nicht einmal in Rechtsgebieten mit Analogie akzeptabel wären. Durch die Anlehnung der Formulierung eines neuen Tatbestandes an eine etablierte Vorschrift entsteht nicht automatisch eine hinreichend bestimmte Verhaltensnorm. Die Überlegungen zur Datenveränderung (oben III.) haben das gezeigt. Bevor eine Analogie in Gesetzesform gegossen werden kann, müssen die zu ihr erforderlichen Ähnlichkeiten aber tatsächlich bestehen bzw. hergestellt werden. Sonst bleibt es beim untauglichen Analogieversuch, der fast unvermeidlich zu einer unterbestimmten und evtl. sogar auch im Wege sukzessiver Konkretisierung nicht mehr bestimmbaren Norm führt. Dann verstößt der Tatbestand gegen Art. 103 Abs. 2 GG und Art. 7 Abs. 1 EMRK. Die Frage, ob die Vorschrift in der Praxis offenkundig willkürlich angewendet wird, ist dabei sekundär. Unbestimmte Tatbestände sind gerade auch in den Händen redlicher, sich dem Legalitätsprinzip verpflichtet wissender Staatsanwälte und Richter eine Dauergefahr. Bei § 303a StGB ist das der Fall.

Das hinter § 303a StGB und Art. 4 Abs. 1 der Cybercrime-Convention stehende Programm der Anlehnung an die Sachbeschädigung ist und bleibt dabei richtig. Es muss am Datenrecht und auch am strafrechtlichen Datenbegriff gearbeitet werden, dann wird eine dem heutigen Tatbestand der Datenveränderung sehr ähnliche Vorschrift wahrscheinlich einmal (in nicht allzu naher Zukunft) der in diesem Bereich bestmögliche Straftatbestand sein.

Gerade mit Blick auf jüngere Gesetzesänderungen im Computerstrafrecht kann man diesen Gedanken fortentwickeln: Die Vorfelddelikte des § 202c StGB und der ihn aufgreifenden §§ 303a Abs. 3, 303b Abs. 5 StGB (jeweils auf Basis von Art. 6 der Cybercrime-Convention) werfen sowohl hinsichtlich der Bestimmtheit des dort erfassten Verhaltens als auch hinsichtlich der Verhältnismäßigkeit (Erforderlichkeit und Geeignetheit) der Normen etliche Probleme auf. Unter anderem drohen sie, das Aufspüren von Sicherheitslücken zu hemmen und so deren Behebung zu vereiteln. Sucht man nach Ähnlichkeiten zu diesen Vorschriften in den entsprechenden traditionellen Tatbeständen (§ 202 StGB bzgl. § 202c StGB und § 303 bzgl. §§ 303a und 303b StGB), wird man nichts finden. Von dem ohnehin vorfeldartigen[82] § 303 StGB und dessen Versuch ausgehend eine weitere Vorverlagerung der Strafbarkeit anzuordnen, wird – obwohl das weit ausgearbeitete Sachenrecht im Hintergrund steht – aus gutem Grund nicht erwogen. Dass (und weshalb) es zu den neuen Vorfelddelikten des Computerstrafrechts kein klassisches Analogon gibt, wäre aller Anlass gewesen, auch im Computerstrafrecht entweder ganz auf sie zu verzichten oder sie zumindest weit sorgfältiger auszuarbeiten und im Anwendungsbereich zu beschränken.[83]

Die Suche nach Analogien und ihre Ausarbeitung im Rahmen gesetzgeberischer Arbeit kann also nicht nur eine hinreichende Bestimmtheit der Formulierung von Tatbeständen ermöglichen, sondern auch zur sachgerechten Beschränkungen des Strafrechts beitragen.

---

[81] Nicht zuletzt würden dann auch das materielle Recht und die Strafverfolgungspraxis sowie Erfolgsaussichten von Rechtshilfeersuchen weniger weit auseinanderklaffen (vgl. dazu *Ernst*, NJW 2007, 2661 [2665 f.]).

[82] Dazu oben III. 5. b).

[83] Zu den entstandenen Problemen vgl. *Popp*, GA 2008, 375, sowie BVerfG JR 2010, 79 m. Anm. *Valerius* und zahlreichen w.N. Wie *Valerius* dort zutreffend betont, gibt die Entscheidung zwar Anlass zu der Hoffnung, dass die Praxis diese Tatbestände restriktiv handhaben wird, beseitigt die Bedenken aber nicht (*Valerius*, JR 2010, 84 ff.).

Einseitiges Strafanwendungsrecht und entgrenztes Internet?*

Von Akad. Rätin a.Z. Dr. **Liane Wörner**, LL.M. (UW-Madison), Gießen

The paper questions, whether the subordination of criminal law to national state systems can cope with the – by nature – un-restricted and un-limited internet and its possibilities to act international. Neither total observation of all kinds of websites and internet forum seems to be even possible nor can this be called an achievable aim in respect of societal democratic orders. Efforts to restrict „the internet" fail. A coordinated approach by national states reconfiguring their national criminal laws in respect of the challenges of internet-crimes may be a solution and result in the release of International contractual provisions. But, agreeing on what shall be punished will not solve any conflicts of jurisdiction, because the Internet is a „boundless ocean". International coordination will require reconsidering what to protect on the one side and to reconsider national jurisdictional rules of choice of forum on the other side. In the end a transnational approach on choice of forum addresses national states as well as (directly) state citizens. Transnational power on choice of forum therefore cannot be a one-way-street, but a democratic process resulting in provisions. This will have to result in reinterpreting rules of national jurisdictions away from a one-side-viewed national sovereignty to transnational solidarity and transnational citizens.

I. Einführung: Das entgrenzte Internet

Die Informationsplattform Internet ist aus unserem Leben nicht mehr wegzudenken. Wir verhalten uns zu ihr, mit *Callas*, „fast schon wie Fische zum Wasser: Wir merken nicht, dass es uns umgibt. Wir schwimmen einfach drin."[1] Faktisch sind die mehr als drei Milliarden Webseiten des world wide web (www) mit über 150.000 verschiedenen newsgroups und ca. 25.000 verschiedenen Chatkanälen im Internet Relay Chat (IRC) jedenfalls auf Basis der derzeitigen Netzstruktur zur Feststellung von Straftaten längst nicht mehr vollständig überwachbar,[2] noch wäre dies erstrebenswert. Der anhaltende Trend zur „globalen Verbreitung digitaler Informationen", ob per peer to peer oder mittels „Cloud Computing", jeweils anonymisiert und kryptiert, stellt die Ermittler vor immer neue Herausforderungen.[3] Die Nutzung des Internets zu kriminellen Zwecken entwickelt sich zu *dem* Kriminalitätsphänomen des 21. Jahrhunderts.[4]

1. Piraten und Hacker

Dabei erinnert die aktuelle Diskussion um das Internet an das Zeitalter romantisch verklärter Piraterie und Freibeuterei des 16. und frühen 17. Jh. n. Chr. Der Vergleich mag überraschen, doch er ist rasch erklärt: Die Piraten, so ambivalent, wie wir sie heute verstehen, kamen mit der Entdeckung der terra incognita, der neuen Welt Amerikas.[5] Schätze wollten geborgen, neue Kommunikations- und Handelswege gefunden und neues Terrain erschlossen werden. Angelockt vom Reichtum der großen Handelsschiffe gab mancher seine ehrbare Stellung auf, um in den ungesicherten Meeren als Pirat sein „Glück zu machen". Mit Entdeckung der Weite des noch nicht erschlossenen Raums begann das goldene Zeitalter der Piraterie. Doch auch die Staatsmächte Europas wollten sich am Reichtum beteiligten und verteilten „Kaperbriefe" – also Lizenzen für Piraten zum Bestehlen und Berauben ausländischer Handelsschiffe im staatlichen Auftrag.[6]

Die terra incognita von heute ist das world wide web. Mit seiner Freigabe an die Welt 1989[7] begann die Schatzsuche. Was von *Tim Berners-Lee* am Cern/Schweiz für den einfachen und schnellen Austausch von Forschungsergebnissen gedacht war, ist heute unsere Hauptkommunikationsplattform und

---

* Vortrag im Rahmen des AIDP-Symposiums „Cybercrime: Ein deutsch-türkischer Rechtsdialog" an der Bilgi-Universität Istanbul, Türkei (13.-15.10.2011). Der Vortragsstil wurde weitgehend beibehalten.

[1] *Callas*, Die Zeit v. 29.9.2011, S. 29 (aus dem Englischen übersetzt v. *Thomas Fischermann*).

[2] So die Zentralstelle für anlassunabhängige Recherchen in Datennetzen (ZaRD) beim Bundeskriminalamt (BKA), unter: http://bka.de/nn_205994/DE/ThemenABisZ/Deliktsbereiche/InternetKriminalitaet/InternetrechercheZaRD/zard__node.html?__nnn=true (12.7.2012).

[3] So auch die ZaRD auf ihrer Internetseite unter „Perspektiven". Zur Zunahme des cloud computing vgl. Bundesamt für Sicherheit in der Informationstechnik (BSI), Die Lage der IT-Sicherheit in Deutschland 2011, BSI-Lagebericht IT-Sicherheit 2011, 2011, S. 38 ff., auch im Internet abrufbar unter: http/www.bsi.bund.de/ContentBSI/Publikationen/Lageberichte/bsi-lageberichte.html (12.7.2012).

[4] S. nur BKA, Bundeslagebild Cybercrime 2010, 2010, S. 5 ff., insb. S. 7; Bundesministerium des Inneren, Polizeiliche Kriminalstatistik 2010, Stand: April 2011, S. 8: Erhebungen zum Tatmittel Internet erfolgen seit 2010 in allen Bundesländern über eine entsprechende Sonderkennung. Die Steigungsrate liegt allein von 2009 auf 2010 bei durchschnittlich 8,1 %. Vgl. auch *Hecker*, Europäisches Strafrecht, 3. Aufl. 2010, § 11 Rn. 97 f. Zur Entwicklung schon *Valerius*, Ermittlungen der Strafverfolgungsbehörden in den Kommunikationsdiensten des Internet, 2004, S. 20 f.; *Böckenförde*, Die Ermittlung im Netz, 2003, S. 1 ff., insb. S. 7 f., spricht von „Netzkriminalität".

[5] Seefahrer gab es freilich bereits zuvor, doch entspann sich der eigentliche Kampf um die Meere gerade mit der Entdeckung der „neuen Welt".

[6] Zur rechtlichen Einordnung ausführlich *Kretschmer*, Globalisierung und Strafrecht, Grundlagen transnationaler Strafbegründung: Recht – Geschichte – Ökonomie – Politik (noch unveröff.), A. I. 3.-5. (Manuskript S. 9-27 ff.).

[7] Ursprung des Internets ist das bereits 1966/69 vom amerikanischen Verteidigungsministerium eingerichtete ARPAnet (Advanced Research Projects Agency). Zur Geschichte des Internets vgl. *Blancke*, APuZ 30-31/2005, 24 (25); *Valerius* (Fn. 4), S. 1 ff., insb. S. 4, 9.; *Böckenförde* (Fn. 4), S. 3. Der erste Browser stand 1993 kostenfrei zur Verfügung.

bestimmt unsere Handelswege. Auch heute gibt manch einer eine „ehrbare“ Stellung auf, um als „Anonymous“ Sicherheitslücken in der Kommunikationsplattform Facebook aufzuspüren[8] oder mittels des Software-Trojaners Katusha die Handelswege vieler Millionen Bankkunden zu durchkreuzen.[9] Es ist das goldene Zeitalter der Hacker, wie man jene Online-(Daten-)Piraten zu nennen pflegt.[10] Facebook ruft nach Sicherheit und verteilt ebenso wie viele Staatsmächte „Hacker-briefe“.[11] Der amerikanisch-israelische Computerwurm stuxnet wird 2010 („staatlich verordnet“) in eine Urananreicherungsanlage im Iran „eingepflanzt“ und manipuliert dort den Steuerungschip der Zentrifugen und damit das Atombombenprogramm des Iran insgesamt.[12] Das Internet als „wichtigste Infrastruktur unserer Zeit“ scheint zur Gefahr für Wohlstand und Sicherheit zu mutieren und steht vor dem Neubau.[13] Unklar ist mithin, was es überhaupt gegen wen zu schützen gilt.[14]

2. Weltmeer und Datenmeer

Die Piraterie ist heute weltweit geächtetes und international verfolgtes Delikt. Das Seerechtsübereinkommen der Vereinten Nationen von 1982[15] verpflichtet die Staaten zur gemeinsamen Bekämpfung der Piraterie auf den Weltmeeren. Doch sind damit nicht alle Probleme der internationalen Piraterie gelöst. Der seit dem 17. Jahrhundert anerkannte, wenn auch in seinen Grenzbereichen nicht unumstrittene, Grundsatz der Freiheit der Weltmeere[16] beschränkt die staatliche Hoheitsausübung bis heute auf Schiffe unter eigener Flagge. Die 1927 in Istanbul begründete „Lotus-Regel“ stellt eine Vermutung für die staatliche Handlungsfreiheit aufgrund staatlicher Souveränität auf. Denn nachdem am 2.8.1926 das französische Postschiff Lotus auf hoher See mit der Boz-Kurt kollidiert war und dabei acht türkische Seeleute ihr Leben verloren, entschied der Ständige Internationale Gerichtshof (StIGH) zugunsten der türkischen Souveränität:[17]

„International law governs relations between independent States. The rules of law binding upon States therefore emanate from their own free will [...]. Restrictions upon the independence of States cannot therefore be presumed.“

Für staatlich zulässiges Handeln bedarf es danach keiner völkerrechtlichen Erlaubnisnorm. Es darf nur kein völkerrechtliches Verbot entgegenstehen.[18] Und der souveräne Staat kann nicht zur Handlung verpflichtet werden. Die hieraus resultierenden Probleme in der Bekämpfung der internationalen Piraterie zeigt (beispielhaft) die Entführung des von der deutschen Reederei verwalteten Tankers Longchamp im Januar 2009 vor der Küste Somalias. Die Staatsanwaltschaft in Hamburg ermittelte wegen Angriffs auf den Luft- und Seeverkehr (§ 316c dStGB). Doch die deutsche Zuständigkeit für das in Deutschland verwaltete, unter der Flagge der Bahamas mit indonesischem Kapitän und philippinischer Mannschaft zwischen Norwegen und Vietnam verkehrende und von somalischen Piraten überfallene Schiff war keineswegs klar. Die deutsche Marine erklärte sich schließlich nach Prüfung für unzuständig.[19] Einseitige Souveränitätskonzepte helfen hier nicht weiter.

---

[8] *Fischermann/Hamann*, Die Zeit v. 8.9.2011, S. 27.

[9] Dazu: *Gatzke*, Kriminalistik 2012, 75; Zeitungsbericht *Katusha*, Weser-Ems-Zeitung v. 1.11.2010 (business-on, http://www.business-on.de/druckansicht/14_80_15512.html [28.2.2012]). Die exemplarische Aufzählung ist nicht abschließend. Zu den „Daten-Piraten“ sind neben Einzelpersonen und Personenzusammenschlüssen ebenso auch Unternehmen, Unternehmensgruppen und Staaten zu zählen, soweit sie im Umgang mit ihnen zugänglichen oder ihnen überlassenen Daten in Individualrechte eingreifen oder diese beschränken.

[10] Auf die zu den Piraten von damals bestehende gleichlaufende Ambivalenz machen nun etwa auch *Robertz/Rüdiger*, (Kriminalistik 2012, 79) aufmerksam.

[11] Zum Facebook-Aufruf s.a. *Fischermann/Hamann*, Die Zeit v. 8.9.2011, S. 27. Zum jährlichen Facebook-Hacker Cup: http://www.facebook.com/video/video.php?v=10100106817149407 (12.7.2012).

[12] Vgl. dazu BSI (Fn. 3), S. 28 f. Es kursieren bereits neue stuxnet-ähnliche Schadprogramme wie Duqu (*Höll/Krüger/Martin-Jung*, Süddeutsche Zeitung v. 20.10.2011, S. 5).

[13] *Fischermann/Hamann*, Die Zeit v. 8.9.2011, S. 27 (im Titel); *dies.*, Zeitbombe Internet, 2011, S. 25 ff., insb. S. 28.

[14] Zu definitorischen Problemen des Begriffs „Computerkriminalität“ vgl. bereits *Hilgendorf*, JuS 1997, 323 („Datennetzkriminalität“); *Sieber*, Computerkriminalität und Strafrecht, 1977, S. 184, 188 („Sammelsurium“); *ders.*, Legal Aspects of Computer-Related Crime in the Information Society, 1998, S. 24 ff.; *ders.*, in: Sieber/Brüner/Satzger/von Heintschel-Heinegg (Hrsg.), Europäisches Strafrecht, 2011, Kap. 6 Rn. 1-6 zum weiten Bereich der Computer- und Internetkriminalität und den definitorischen Problemen.

[15] Seerechtsübereinkommen der Vereinten Nationen („United Nations Convention on the Law of the Sea“) v. 10.12.1982, auch in Deutschland in Kraft seit 16.11.1994 (BGBl. II 1994, S. 1798; BGBl. II 1995, S. 602); basierend auf dem Genfer Übereinkommen über die Hohe See v. 29.4.1958, in Kraft seit 30.9.1962, in Deutschland seit dem 25.8.1973 (BGBl. II 1972, S. 1089, 1091; BGBl. II 1975, S. 843).

[16] Völkervertraglich anerkannt erst mit Art. 2 des UN-Übereinkommens über die Hohe See v. 29.4.1958 (UNCLOS I) sowie in Art. 87 ff. des UN-Seerechtsübereinkommens v. 10.12.1982 (UNCLOS III). Zur geschichtlichen Entwicklung vgl. auch *Kretschmer* (Fn. 6), B. III. (Manuskript S. 270 f.).

[17] Vgl. StIGH, Urt. v. 7.9.1927 – PCIJ Ser. A No. 10 (S.S. Lotus [Frankreich v. Türkei]), im Internet abrufbar unter: http://www.worldcourts.com/pcij/eng/decisions/1927.09.07_lotus.htm (12.7.2012).

[18] Zur Interpretation kurz auch *Hobe*, Einführung in das Völkerrecht, 9. Aufl. 2008, S. 619 f.

[19] Vgl. Hamburger Abendblatt v. 30.1.2009, im Internet unter: http://www.abendblatt.de/wirtschaft/article596093/Deutsche-Marine-Wir-sind-fuer-die-Longchamp-nicht-zustaendig.html (12.7.2012). Zum Verfahrensausgang: Spiegel-online v. 28.3.2009, abrufbar unter: http://www.spiegel.de/panorama/justiz/somalia-entfuehrter-deutscher-gastanker-longchamp-wieder-frei-a-616040.html (12.7.2012).

Auch im aktuellen Datenmeer des www bestehen Jurisdiktionskonflikte wegen strafbarer Handlungen im Internet. Höchst fraglich ist es, ob sich ein „goldenes Zeitalter des Hackertums“ mit einer Invasion gegen das Internet beenden ließe[20] oder ob eher ein Umdenken und gegebenenfalls ein Neustrukturieren seiner Kommunikationsformen und Datenübertragungswege – seien es Facebook oder „library.nu“[21] – angezeigt sind. Eine rechtliche Begrenzung der terra incognita Internet tut gut und not. Man sollte aber nicht erwarten, dass mit Mitteln des Strafrechts über seine grundsätzlich friedenssichernde Funktion hinaus[22] mittels Datensicherheit ein kriminalitätsfreier Raum geschaffen würde. Denn das veränderte auch *im* und *über das* Internet die Wertegesellschaft in eine Sicherheitsgesellschaft. Fraglich ist nun einerseits, inwieweit eine rechtliche Begrenzung des Internet möglich erscheint (II.), wie einseitig – im Sinne von staatlichen Formen abhängig – das Strafanwendungsrecht (III.) ist und wie sich beide Komponenten miteinander verbinden lassen (III./IV.)

II. (Faktische) Begrenzungsversuche

Neben aktuell geplanten staatlichen Versuchen zur nationalstaatlich betriebenen Begrenzung des world wide web etwa durch das (deutsche) Nationale Cyber-Abwehrzentrum in Bonn[23] mit einer Softwareschutzhülle gegen Hacker[24] oder dem von EU-Justizkommissarin Viviane Reding gerade erarbeiteten EU-Datenschutzrahmengesetz[25] – *Jon Callas* prophezeit sogar die staatliche Übernahme der sozialen Internetnetzwerke (von google bis facebook)[26], – stand lange die an anderer Stelle angedachte Begrenzung des Internets durch die Weiterentwicklung von peer to peer-Systemen in „zuverlässige Netze“.[27]

Der peer to peer-Schutz ist jedenfalls für die Kriminalitätsbekämpfung wenig zielführend. Nach der Idee des peer to peer-accountable soll Zutritt nur dem gewährt werden, der sich als identifizierbar, vertrauenswürdig und zuverlässig erweist. Die Nutzer sollen untereinander verantwortlich sein und frei von staatlichem Zugriff entscheiden, in welchem System sie „leben“ möchten: in einem mit mehr Regulierung oder in einem, in dem ein jeder einen jeden belügt und betrügt. Mittels verlässlicher Reputationssysteme und Schutztools könne man beide unterscheiden.[28] Diese dezentrale „Internet-Governance“[29] entspricht einer informationellen Selbstbestimmung der Internetuser. Doch der Kriminelle wird sich kaum freiwillig in einem Netz von Betrügern und Lügnern tummeln, sondern gerade Zugang zu einem speziellen peer to peer-accountable suchen. Den an staatliche Hoheitsgrenzen auch noch gebundenen Ermittlungsorganen und Justizen fällt dann unter ungleich erschwerten Bedingungen die Durchsetzung des Opferschutzes zu. Die Balance zwischen informationeller Selbstbestimmung und Opferschutz im Internet erscheint kaum haltbar.[30] Den entwickelten cloud-Systemen haften insoweit die gleichen Probleme an.[31] Denn der vermeintlich höchste Datenschutz, etwa in einer besonders gesicherten „zuverlässigen cloud“, beinhaltet gerade den Zugriffsreiz. Zugleich erschwert die Vielzahl an Usern und an clouds die Sicherungsmöglichkeiten.[32]

Auch der Blick auf einen aktuellen Fall[33] zeigt, dass die faktische territorial-staatliche Begrenzung des Internets nicht funktioniert: Die Ermittler der EK-Katusha, benannt nach dem von den Tätern eingesetzten Trojaner, sprengten eine internationale Hacker-Bande in einem der umfangreichsten Ermittlungsverfahren gegen Verbreiter von Schadsoftware. In 39 Telekommunikationsüberwachungsmaßnahmen ermittelten sie ca. 670 sogenannte Finanzagenten in über 100 Botnetzen mit über 50 Servern, die für die acht Hauptverdächtigen – zwei Deutsche, ein Brite und fünf estnische Staatsbürger – tätig waren. In Deutschland wurden ca. 400.000 mit dem Katusha-Trojaner infizierte PCs festgestellt, weltweit ca. 2,5

[20] So der Vorschlag von *Fischermann/Hamann*, Die Zeit v. 8.9.2011, S. 27; *dies.* (Fn. 13), S. 33 ff., 234 ff.

[21] Das angeführte Bsp. „www.library.nu“ (12.7.2012) ist als Beispiel für ein lange Zeit funktionierendes Webportal gewählt, welches umfassend den Down- und teilweise Upload von belletristischer und vor allem auch wissenschaftlicher Literatur ermöglichte. Juristisch unbehelligt blieb es lange vor allem, weil hier national verschieden Betreiber, Webhost und Server*standort* zusammenwirkten und hieraus – wenn man so will – ein negativer Jurisdiktionskonflikt entstand. Seit Ende 2011 war die Seite gesperrt, ist inzwischen aber offiziell mit google und Amazon verbunden legal zugänglich. Nachfolger existieren bereits.

[22] Hierzu grundlegend auch *Kretschmer* (Fn. 6), B. I. sowie B. III. und C.IV. (Manuskript S. 186, S. 278 ff. und S. 458 ff.).

[23] Kurz NCAZ, gegründet am 23.2.2011.

[24] Vgl. *Fischermann/Hamann* (Fn. 13), S. 231 ff., 243 ff.; dazu *dies.*, Die Zeit v. 8.9.2011, S. 27 (S. 29).

[25] *Hammann/Tatje*, Die Zeit v. 29.9.2011, S. 28.

[26] *Callas*, Die Zeit v. 29.9.2011, S. 29. *Fischermann/Hamann* (Fn. 13), S. 240 ff. plädieren für eine Datendiät etwa mittels einer Zentralstelle für Lizenzen im Umgang mit persönlichen Daten (*dies.* [Fn. 13], S. 240), die die Verwendung persönlicher Daten für den Einzelnen nach dessen Wünschen konkret lizensiert.

[27] Deutlich *Dyson*, APuZ 30-31/2005, 3.

[28] *Dyson*, APuZ 30-31/2005, 3.

[29] *Dyson*, APuZ 30-31/2005, 3.

[30] So die ZaRD auf ihrer Internetseite unter „Perspektiven“.

[31] Der durch den 2008 neu eingeführten § 110 Abs. 3 StPO erlaubte Zugriff auf die Cloud-Daten führt insbesondere zu einer „Online-Durchsuchung light“; zu den Zugriffsmöglichkeiten ausführlich und krit. s. *Schlegel*, HRRS 2008, 23, und *Bär*, ZIS 2011, 53 (54 f.), vor allem auch zu den praktischen Problemen des transnationalen Zugriffs; zu Recht kritisiert *Bär*, a.a.O., die Vorschriften der Cyber Crime Convention als insoweit unzureichend.

[32] *Fischermann/Hamann* (Fn. 13), S. 243 schlagen deshalb vor, mittels internationaler Bestimmungen festzulegen, dass die gespeicherten Cloud-Daten auf Superspeichern dort lagern sollen, wo die Menschen leben, um deren Daten es geht. Allerdings lassen sich auch Lebensmittelpunkte heute nicht mehr einfach bestimmen.

[33] Die Hauptverhandlungen, zuletzt gegen die fünf estnischen Beschuldigten, liefen am 30.9.2011 und endeten mit einem Vergleich.

Mio. Mittels des Trojaners wurden die Onlinebankgeschäfte der betroffenen Kunden so manipuliert, dass erst nach der Eingabe aller Daten durch die Kunden einschließlich der Transaktionsnummern der Bank (TAN) eine Umleitung der Überweisung unter Änderung des Überweisungsbetrags auf ein anderes Konto erfolgte. Den deutschen Ermittlern gelang es in enger Zusammenarbeit mit den estnischen und den britischen Behörden, einen Schaden in Höhe von 1,2 Mio. Euro abzuwenden.[34] Weder die international zusammengesetzte Tätergruppe noch die ebenso international betroffenen Kunden, noch die nunmehr ebenfalls international zusammenwirkenden Ermittler lassen sich faktisch noch in nationalstaatliche territorial erfassbare Grenzen „pressen".

Beschränkungen sind damit allenfalls bezogen auf den Datenfluss und seine Sicherungen denkbar. Im Übrigen ist das Internet entgrenzt. Publikationen im Internet sind grundsätzlich ebenso weltweit zugänglich wie weltweit Datenzugriffe möglich sind.[35] Rechtliche – auch strafrechtliche und im Besonderen strafanwendungsrechtliche – Regelungen müssen hierauf reagieren.

III. Einseitiges Strafanwendungsrecht oder Internationales Internetstrafrecht für alle?

Internationale Verfahren wie Katusha fordern die nationale Straftatverfolgung der Zukunft heraus.[36] Dabei gilt es einerseits zu klären, was im Internet überhaupt verfolgt werden kann und darf und welche Maßnahmen hierfür ergriffen werden dürfen.[37] Neben jene zu klärenden, teils auch faktischen Fragen, tritt unmittelbar eine weitere: Welches Strafrecht soll gelten?

1. „Das Rechtsnetz" – Auf hoher See der Rechte

Art. 22 der Cybercrime Convention des Europarats (2001)[38] knüpft für die festzulegende Gerichtsbarkeit an die völkerrechtlich anerkannten Anknüpfungspunkte, insbesondere der Territorialität, des Flaggengrundsatzes und der aktiven Personalität, an. Eine dezidierte Darstellung aller Strafanknüpfungspunkte ist hier freilich nicht zu leisten und auch nicht gewollt.[39] Vielmehr steht ihre Anwendbarkeit für das Internet in Frage und damit die Grundsatzfrage, ob das www Sonderregulierungen erfordert und inwieweit sich völkerrechtlich anerkannte Prinzipien nutzen lassen.

Insoweit kann zunächst festgehalten werden, dass die Statusüberprüfung des „CyberCrime@IPA Projektes" mit der Türkei eine grundsätzliche Übereinstimmung der türkischen Strafanwendungsvorschriften der Art. 8-13 türkStGB mit den Anforderungen der Cybercrime Convention feststellt.[40] Doch die Strafanwendungsfrage beim transnationalen und internationalen Datenmissbrauch bei facebook, mittels stuxnet oder Katusha löst das nicht. Während Art. 23-34 der Cybercrime Convention die Zusammenarbeit bei den Ermittlungen, Rechtshilfe und Auslieferung betreffen, bleibt die „Ausübung der Strafgerichtsbarkeit durch eine Vertragspartei nach ihrem innerstaatlichen Recht" nach Art. 22 Abs. 4 Cybercrime Convention ausdrücklich vorbehalten.

Das ist nicht unproblematisch, wie der Blick ins deutsche Strafanwendungsrecht zeigt. Denn das deutsche Strafrecht ist für seine extensive Auslegung weit bekannt.[41] An ihm soll offenbar „die Welt genesen", kritisierte *Hilgendorf* schon 1997 die Strafverfolgung im Internet.[42] Weil sich aber im territorial entgrenzten Internet weder der Datenzugriff noch die Datenmanipulation an staatliche Grenzen halten, entsteht im Hinblick auf die Zuweisung der nationalstaatlichen Gerichtsbarkeit nahezu zwangsläufig eine Jurisdiktionskonkurrenz. Auf-

[34] Genauer Schaden: 1.202.362,00 €. Ein Schaden in Höhe von 438.180,00 € ist gleichwohl entstanden und konnte nicht mehr verhindert werden. Die nachweislichen von den Tätern manipulierten Überweisungen belaufen sich auf einen Gesamtbetrag in Höhe von 1.640.542,00 €; zu öffentlich zugänglichen Verfahrensinformationen vgl. *Gatzke*, Kriminalistik 2012, 75; Zeitungsbericht *Katusha*, Weser-Ems-Zeitung v. 1.11.2010 (Fn. 9).

[35] So auch schon *Hilgendorf*, ZStW 113 (2001), 650 (651). *Valerius* (Fn. 4), S. 141, spricht vom globalen Dorf und seinen Bürgern als „Netizen" (net citizens).

[36] Ebenso schon *Hilgendorf*, ZStW 113 (2001), 650 (651).

[37] Ausführlich bereits *Böckenförde* (Fn. 4) spricht vom eigenen „Ermittlungsraum", S. 9, 167 ff.; *Valerius* (Fn. 4), S. 21 ff., insb. S. 26 ff. Zu den auftretenden faktischen wie rechtlichen Problemen vgl. auch die Beiträge im Rahmen dieses Projekts in dieser Ausgabe von *Groß*, ZIS 2012, 466, und *Rettenmaier/Palm*, ZIS 2012, 469.

[38] Übereinkommen über Computerkriminalität v. 23.11.2001. Die deutsche Fassung ist im Internet abrufbar unter: http://conventions.coe.int/treaty/ger/treaties/html/185.htm (12.7.2012).

[39] Zu den Anknüpfungspunkten vgl. etwa *Ambos*, Internationales Strafrecht, 3. Aufl. 2011, §§ 1-4, insb. § 4 mit Übersicht in Rn. 23; *Satzger*, Internationales und Europäisches Strafrecht, 5. Aufl. 2011, § 5; *Hecker* (Fn. 4), § 2 Rn. 12 ff.; *Eser*, in: Schönke/Schröder, Strafgesetzbuch, Kommentar, 28. Aufl. 2010, Vor §§ 3-9 Rn. 11 ff.; *Werle/Jeßberger* in: Laufhütte/Rissing-van Saan/Tiedemann (Hrsg.), Strafgesetzbuch, Leipziger Kommentar, Bd. 1, 12. Aufl. 2007, § 3 Rn. 24 ff.; *L. Wörner/M. Wörner*, in: Sinn (Hrsg.), Jurisdiktionskonflikte bei grenzüberschreitend organisierter Kriminalität, 2012, S. 203 (S. 227 ff.).

[40] www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/CountryProfiles/cyber_cp_Turkey_2011_January.pdf (12.7.2012). Project on Regional Cooperation in Criminal Justice: Strengthening capacities in the fight against cybercrime, s. jp.coe.int/CEAD/JP/Default.asp?TransID=204 (12.7.2012).

[41] Schon *Eser*, in: Leipold (Hrsg.), Rechtsfragen des Internet und der Informationsgesellschaft aus deutscher und japanischer Sicht, Symposium der rechtswissenschaftlichen Fakultäten der Albert-Ludwigs-Universität Freiburg und der Städtischen Universität Osaka, 2002, S. 303 (S. 321 ff.).

[42] *Hilgendorf*, NJW 1997, 1873 (1874); zur vielfach aufgenommenen These vgl. auch: *Jofer*, Strafverfolgung im Internet, 1999, passim; *Roggan*, KJ 2001, 337.

grund der weithin anerkannten Ubiquitätsthese[43] werden für den in einem Staat an einem Computer handelnden Hacker schon dann mehrere Gerichtsbarkeiten zuständig, wenn diese Handlung in anderen Staaten einen Erfolg herbeiführt, sei es der Verlust, der Missbrauch oder die Manipulation von Daten. Der in einer Beschränkung auf die staatliche Territorialität gedachte Strafanknüpfungspunkt führt so unter Gleichbehandlung aller Handlungs- und Erfolgsorte einer Internetstraftat zu einer „globalen Strafrechtskonkurrenz".[44] Der Territorialitätsschutz verwandelt sich mit Beachtung des Internet-Erfolgsorts im deutschen – wie im Übrigen auch im türkischen – Strafrecht in einen passiven Personalschutz für alle Internetuser.[45]

Aus deutscher Perspektive ließe sich jene globale Konkurrenz jedenfalls für die sog. Inhaltsdelikte[46] zwar weitgehend reduzieren. Wird nämlich für die Strafbarkeit schon an den zu verbreitenden Kommunikations- bzw. Dateninhalt angeknüpft, wie im Fall des Verbreitens pornographischer Dateien (§§ 184 ff. dStGB) oder von volksverhetzenden Äußerungen (§ 130 dStGB), kann nur auf den Handlungsort abgestellt werden, wenn sich die Strafbarkeit in Form bereits abstrakter Gefährdung in der Handlung erschöpft.[47] Auf den Eintritt eines Erfolgs, den Eintritt einer auch nur konkreten Gefährdung, kommt es dann für die Strafbarkeit nicht an, § 9 Abs. 1 Var. 3 dStGB ist nicht einschlägig. Globale Strafrechtskonkurrenz im Internet ließe sich so also sehr einfach durch Vorverlagerung auf eine „Internetstrafbarkeit" schon bei abstrakter Gefährdung jeglicher krimineller Kommunikation verhindern. Denn dann käme es mangels erforderlichen Deliktserfolgs nur auf die Handlung an. Doch das wäre nicht nur rechtsstaatlich bedenklich, es erscheint auch im Ergebnis wohl nicht wünschenswert, wie die Diskussion um den Fall Toeben und die Verbreitung der sog. „Ausschwitzlüge" im Internet zeigt.[48]

Es gilt vielmehr einerseits zwischen bloß abstrakten Gefährdungsdelikten und Eignungsdelikten, die jedenfalls eine Eignung zu eine potentiellen Gefährdung durch die Handlung erfordern (auch: potentielle Gefährdungsdelikte), strikt zu trennen: Für erstere ist schon ihre Zulässigkeit überhaupt fraglich,[49] für zweitere kann § 9 Abs. 1 Var. 3 dStGB über die Eignung zur potentiellen Gefahr tatsächlich anwendbar werden.[50] Andererseits – und das ist hier entscheidend – besteht aber eben gerade kein grenzüberschreitender Konsens für Äußerungsdelikte, sondern die Strafbarkeit wird in den nationalen Rechtskulturen unterschiedlich beurteilt. Dem anglo-amerikanischen Rechtskreis ist die mit Äußerungsdelikten verbundene Einschränkung des free speech-Grundsatzes, wie im Fall Toeben, sogar eher befremdlich.[51] So wird hier letztlich einseitig souverän über die extensive Auslegung der Vorschriften des deutschen Strafanwendungsrechts die deutsche Strafbarkeit für Fälle eröffnet, in denen der Täter an der Computertastatur in seinem Heimatland handelt, unabhängig davon, wie diese Handlung dort strafrechtlich bewertet wird. Unproblematisch ist dies eben nur, wenn wie im Fall der Verbreitung von Kinderpornographie die Strafwürdigkeit solcher Handlungen international anerkannt ist.[52] Im Übrigen ist zunächst zu klären, was es im Internet gegen wen zu schützen gilt. Und dass die Lösung über restriktive oder extensive Auslegungen der Strafanwendungsvorschriften, etwa des § 9 Abs. 1 Var. 3 dStGB, für strafbare Handlungen im und über das Internet nicht trägt, zeigt schon der Blick auf die Äußerungsdelikte etwa der Beleidigung: Für die strafbare Beleidigung (§ 185 dStGB), wegen des Zugangserfordernisses ein Erfolgsdelikt, gilt, dass auch bei der über das Internet in Deutschland wahrnehmbaren Beleidigung eines amerikanischen Kommilitonen durch einen kalifornischen Studenten das deutsche Strafrecht eröffnet werden müsste.[53]

Daneben wird das deutsche Strafrecht im Falle gegebener aktiver Personalität oder in stellvertretender Strafrechtspflege

[43] Vgl. nur die Landesberichte in der rechtsvergleichenden Studie von *Sinn* (Hrsg., Fn. 39), passim. Die Ubiquitätsthese gilt auch im türkischen Strafrecht nach Art. 8 Abs. 1 türkStGB.

[44] Deutlich schon *Eser* (Fn. 41), S. 303 (S. 321, 324), der deshalb für ein Abstellen nur auf den Handlungsort plädiert (S. 325).

[45] Vgl. ähnlich schon *Eser* (Fn. 41), S. 303 (S. 324); *Sieber*, NJW 1999, 2065 (2066).

[46] Bei sog. *Inhalts*delikten besteht der kriminelle Charakter schon im *Inhalt* der Kommunikation selbst, auf das zur Verbreitung verwendete Medium kommt es nicht an. Das dürfte sogar die überwiegende Zahl im Internet begangener Delikte betreffen, *Hilgendorf/Frank/Valerius*, Computer- und Internetstrafrecht, 2005, Rn. 231.

[47] Ebenso deutlich *Hilgendorf/Frank/Valerius* (Fn. 46), Rn. 231, 234; vgl. auch *Rotsch*, ZIS 2010, 168 (170, 171).

[48] Vgl. BGHSt 46, 212 = NJW 2001, 624 = ZUM-RD 2001, 103 = MMR 2001, 228 m. Anm. *Clauß*, MMR 2001, 232, und Anm. *Hörnle*, NStZ 2001, 309, sowie auch *Vassilaki*, CR 2001, 260; *Heghmanns*, JA 2001, 276; *Jeßberger*, JR 2001, 429; *Lagodny*, JZ 2001, 1194; *Kudlich*, StV 2001, 395; *Hilgendorf/Frank/Valerius* (Fn. 46), Rn. 232.

[49] Krit. etwa *Baroke*, in: Sinn/Gropp/Nagy (Hrsg.), Grenzen der Vorverlagerung in einem Tatstrafrecht, 2011, S. 247 (S. 264 ff., 275 f. m.w.N.).

[50] So der BGH in BGHSt 46, 212; zust. *Clauß*, MMR 2001, 228 (232 f.). Die Anwendbarkeit von § 9 Abs. 1 dStGB über reine Erfolgsdelikte hinaus bejahen auch *B. Heinrich*, GA 1999, 72; *Sieber*, NJW 1999, 2065 (2067 ff.). Insgesamt lehnen dies ab: *Hilgendorf*, NJW 1997, 1873 (1875 f.); *Hilgendorf/Frank/Valerius* (Fn. 46), Rn. 232; *Cornils*, JZ 1999, 394 (395 f. m.w.N.). Grds. krit. jüngst *Rotsch*, in: Graf/Jäger/Wittig (Hrsg.), Wirtschafts- und Steuerstrafrecht, Kommentar, 2011, § 9 Rn. 19.

[51] Vgl. etwa *Whitman*, Yale Law Journal 109 (2000), 1279, worauf zu Recht auch *Hörnle*, NStZ 2011, 309 hinweist. Vgl. auch *Sieber*, NJW 1999, 2065.

[52] Ebenso deutlich *Hörnle*, NStZ 2011, 309.

[53] *Hilgendorf*, NJW 1997, 1873 (1876). Freilich kommt den deutschen Strafverfolgungsbehörden hier § 153c dStPO, insbesondere Abs. 1 Nr. 2 zu Hilfe (vgl. *L. Wörner/M. Wörner* [Fn. 39], S. 203 [S. 224] m.w.N.).

(§ 7 dStGB) zuständig,[54] wenn die Tat auch am Tatort – für das Internet wäre es besser zu formulieren: an irgendeinem der Tatorte – strafbar ist. Für das aktive Personalitätsprinzip geht die türkische Regelung in Art. 11 türkStGB darüber wohl noch hinaus und fordert keine identische Tatortnorm. Das gilt auch im deutschen Strafrecht, wenn von der Internetstraftat eines der besonders geschützten nationalen (§ 5 dStGB) oder internationalen (§ 6 dStGB) Rechtsgüter betroffen ist. Straffrei bleibt mithin nur, wem es gelingt, keines der wesentlichen Rechtsgüter zu verletzen und wer ohne Handlungs- und Erfolgsort in Deutschland eine straffreie Insel entdeckt, um eine dort straffreie Handlung so zu begehen, dass sie sich nicht als identische Tatortnorm auswirkt.

Die Zielrichtung dieser „Strafanwendungsregeln" ist klar. Ausgehend von der Grundannahme staatlicher Souveränität sollen sie die Verfolgbarkeit jedweder in den staatlichen Grenzen auftretender oder festgestellter Kriminalität sicherstellen. Sie stammen aus einer Zeit, in der das Reisen noch nicht Teil des Alltags, das Überwinden von Grenzen noch mit erheblichem Aufwand verbunden war. Während etwa *Eser* 2002 in seiner Typisierung der Internetstraftaten noch von solchen sprach, die mittels des Internets nur schneller begangen werden, und solchen, die tatsächlich nur im entgrenzten Internet möglich sind,[55] lautet die Frage 2012 bereits, welche Bedeutung der staatlichen Hoheitsgrenze im weltweiten Wirtschafts- und Handelsverkehr überhaupt noch beigemessen werden kann.[56] Die nationalen Strafanwendungsregeln sind mit ihrem staatssouveränen Ansatz nicht auf diese globale Herausforderung vorbereitet, weder im Internet noch auf hoher See.

2. Überlegungen zur Nautik des Rechts

Um *Callas*' „schwimmende Fische"[57] einzufangen, können wir nur Netze auswerfen. Auch hierzu gibt es bereits hinreichend Vorschläge.

Eine globale weltweite Zuständigkeit eines Staates liegt dabei weder im staatlichen Interesse noch ist sie staatlicherseits zu bewältigen,[58] Strafanwendungsvorschriften in diesem Sinne begrenzen die materielle Strafgewalt[59] und prozessuale Verfolgungsvorschriften geben zusätzlich Opportunitätsmöglichkeiten zum Absehen von der Verfolgung. Es dient vielmehr dem Selbstschutz des Staates, wenn er in seinem Hoheitsgebiet umfassend die eigene Strafgewalt ausübt.[60] Das Meer lässt sich nicht von einer Stelle aus befischen.

Umgekehrt lässt sich auch die vorhandene „gemeinsame Essenz" des Strafbaren nicht als „Weltstrafrecht deklamieren", sondern könnte allenfalls die „Grundlage für eine noch zu verfassende Strafrechtsordnung" bieten.[61] Allein es fehlt am gemeinsamen Gesetzgeber. Unklar ist also, wie ein solches Fischernetz gespannt werden sollte. Globalisiertes Strafrecht setzt vielmehr voraus, dass sich auf globaler Ebene eine Gemeinschaft gebildet hat, die unvollkommen, vielschichtig und vielfältig sein mag, die aber zumindest segmentär das Attribut verdient, globalisiert zu sein.[62]

Von deutscher Seite wird etwa drittens vorgeschlagen, die Anwendbarkeit der nationalen Strafrechte auf Internetstraftaten mittels restriktiver Auslegung gerade des Erfolgsbegriffs weitgehend zu beschränken[63] und entweder nur auf den Handlungsort abzustellen[64] *oder* nur einen mittels Push-Technologie auf deutsche Webseiten und Server bzw. in Deutschland zugänglichen Dateninhalt als Erfolg gelten zu lassen.[65] Und doch zielt der Ansatz, unter extensiver Auslegung mit jeder Zugriffsmöglichkeit auf strafrechtsrelevante, missbrauchte oder manipulierte Datenbestände im Internet auch einen Erfolgsort und die Strafanwendung zu bejahen,[66] (je-

[54] Vgl. *Eser* (Fn. 41), S. 303 (S. 307, krit. S. 325 f.); *Weigend*, in: Hohloch (Hrsg.), Recht und Internet, 2001, S. 85 (S. 87); *Sieber*, NJW 1999, 2065.

[55] *Eser* (Fn. 41), S. 303 ff.

[56] Auch *Hilgendorf/Frank/Valerius* (Fn. 46), Rn. 213, halten nationale Grenzen für „nahelos bedeutungslos" und betonen zusätzliche Aspekte der Globalität und der Verantwortlichkeit der Diensteanbieter.

[57] *Callas*, Die Zeit v. 29.9.2011, S. 29.

[58] *Kretschmer* (Fn. 6), spricht vom „Gebot der politischen Klugheit", B. III. (Manuskript S. 267).

[59] Ebenso *Böse*, in: Kindhäuser/Neumann/Paeffgen (Hrsg.), Nomos Kommentar, Strafgesetzbuch, Bd. 1, 3. Aufl. 2010, Vor § 3 Rn. 5.

[60] Vgl. ausführlich *Oehler*, Internationales Strafrecht, 2. Aufl. 1983, Rn. 125, 153.

[61] *Kretschmer* (Fn. 6), B. III. (Manuskript S. 265). Krit. für die Entwicklung eines Europäischen Strafrechts mit einem Europäischen Strafgesetzbuch auch *Rosenau*, ZIS 2008, 9 (16 ff.).

[62] Vgl. *Kretschmer* (Fn. 6), B. I. (Manuskript S. 186.). Zu den Gefahren der Entterritorialisierung von Strafgewalt auch *F. Meyer*, in: Beck/Burchard/Fateh-Moghadam (Hrsg.), Strafrechtsvergleichung als Problem und Lösung, 2011, S. 87 (S. 93 ff.).

[63] Vgl. *Hilgendorf*, NJW 1997, 1873 (insb. 1876 m.w.N.); *Kienle*, Internationales Strafrecht und Straftaten im Internet, 1998, S. 68, 173 ff., so dass auch bei klassischen Erfolgsdelikten und bei konkreten Gefährdungsdelikten ein durch eine Handlung im Ausland in Deutschland verursachter Erfolg nur dann strafbar sei, wenn die Handlung auch im Ausland unter Strafe stehe unter Berufung auf eine analoge Anwendung von § 7 StGB.

[64] So etwa der Vorschlag von *Eser* (Fn. 41), S. 303 (S. 325).

[65] Ausführlich zur einschränkenden Anwendbarkeit des deutschen Strafrechts nur bei Push-Inhalten insb. *Sieber*, NJW 1999, 2065 (2066, 2069). Vgl. ähnlich auch *Cornils*, JZ 1999, 394 (395 f., 397), die auch eine Neudefinition des Handlungsbegriffs nach Kriterien der Steuerung und Kontrolle vorschlägt.

[66] Vgl. so *B. Heinrich*, GA 1999, 72 (83 f.); *Martin*, Strafbarkeit grenzüberschreitender Umweltbeeinträchtigungen, 1989, S. 79 ff., 118 ff.; *Eser* (Fn. 41), S. 303 (S. 309); aber auch BGHSt 42, 235 (242) = NJW 1997, 138 und schon BGH NStZ 1990, 36 (37): Deutsches Strafrecht soll über § 9 Abs. 1 Var. 3 dStGB gelten, „sofern es im Inland zu der Schädigung von Rechtsgütern oder zu Gefährdungen kommt, deren Vermeidung Zweck der jeweiligen Strafvorschrift ist", somit über die Begriffsbildung des allgemeinen Strafrechts hinaus.

denfalls) in die richtige Richtung. Nur das verhindert das Entstehen zu großer Hohlräume in den Fischernetzen. Es soll eben nicht möglich sein, sich eine straffreie Insel zu suchen, um von dort einen Server auf einer anderen straffreien Insel, wo die Serverprovider nicht haftbar gemacht werden können, mit illegalen Daten zu versorgen, die dann weltweit unter Verstoß gegen Urheberrechte abrufbar sind (das Beispiel www.library.nu). Allein das darf nicht dazu führen, dass Jurisdiktionskonkurrenzen zu Lasten nur eines Staates ausgehen.[67] Dem käme dann mit der Verfolgungsmöglichkeit womöglich auch die Verfolgungspflicht zu.

Der Restriktionsansatz muss folglich ein anderer sein. Weit wesentlicher wird das gegenseitige Helfen (Rechtshilfe) bei der Verfolgung und Aburteilung von Straftaten. Das Prinzip der stellvertretenden Strafrechtspflege könnte so (wieder) an Bedeutung gewinnen.[68] Doch die Vorzeichen haben sich geändert. Als eine Art Vorreiter eröffnet § 22 Abs. 5 der Cybercrime Convention 2001, dass die Staaten im Falle der Jurisdiktionskonkurrenz gemeinsam durch Konsultation die Gerichtsbarkeit bestimmen sollen. Was hier beschrieben ist, ist keine Souveränitätsentscheidung, sondern ein staatliches Miteinander in Solidarität. Damit aber wird gerade das Kompetenzverteilungsprinzip, dass *Oehler* bereits in seinem Buch zum Internationalen Strafrecht v. 1983 vorgestellt hat,[69] zum Prinzip der Prinzipe.[70] In der Folge kann das einseitig staatliche Strafanwendungsrecht zum konsultativ vereinbarten internationalen Strafrecht werden. Das zu fordernde Umdenken betrifft sowohl das Verhältnis der jeweils nationalen Strafrechte zueinander als auch die Auslegung der nationalen Strafanwendungsprinzipien im Verhältnis von Bürger und Staat.[71]

So bleiben die nationalen Strafrechte national begrenzt, die völkerrechtlich anerkannten und im Einzelnen in den nationalen Strafrechten geregelten Strafanwendungsprinzipien bleiben anwendbar. Nur ordnen sie sich neu ein. Das bedeutet keine Hierarchie der Strafanwendungsprinzipien.[72] Es bedeutet aber, dass sie umzudenken sind in Begrenzungsrichtlinien zur Anwendbarkeit nationalen Strafrechts.[73] Denn „die Voraussetzungen zur Anwendung des Strafrechts auch auf extraterritoriale Sachverhalte im Pluralismus von Gesellschaften und zunehmender Globalisierung [haben] sich gewandelt".[74] Das betrifft das Verhältnis zwischen den Staaten ebenso wie gegenüber den Beschuldigten und Opfern. Denn letztere wählen mehr und mehr frei, in welchem System sie leben und wessen Regeln sie akzeptieren wollen (und zwar auch real und nicht nur im Internet). Das im Strafrecht in Deutschland noch vorherrschende Rechtsgüterschutzprinzip gelangt damit (erneut) an seine Grenzen. Es müsste letztlich die internationale Verfolgung aller staatlich geschützten Rechtsgüter fordern.[75] Um seiner Funktion zur Wahrung der Friedensordnung noch gerecht werden zu können, ist der Strafgesetzgeber heute mehr denn je auf die Mitwirkung der zu verpflichtenden Staatsbürger angewiesen. Es entsteht eine Solidargemeinschaft. Damit in dieser die Rechte des Beschuldigten und mit ihnen die Rechtsstaatlichkeit des materiellen Strafrechts nicht unter Beschuss geraten, bedarf es im zunehmenden Internationalisierungsprozess klarer Regelungen, die für den Beschuldigten vorhersehbar das materielle Recht bestimmen und ihn nicht zum Gegenstand mehrerer Strafrechte und Strafprozesse werden lassen. Nur dann bilden etwa die europäischen Grundgedanken einer Freizügigkeit der EU-Bürger sowie einer gegenseitigen Anerkennung weiter die Basis freiheitlich demokratischer Entwicklungen.[76]

Plädiert sei hier also für ein gemeinsames Fischernetzwerk, bei dem man freilich aufpassen muss, dass man nicht überfischt!

IV. Fazit

Was bedeutet dies in aller gebotenen Kürze: Piraten gab es immer und wird es weiter geben. Ebenso wird es sich mit den Hackern verhalten. Beide schwimmen in einem Meer an Freiheiten, dass eben auch kriminelle Möglichkeiten eröffnet. Das Internet ist entgrenzt und allenfalls im Hinblick auf die Datenverfügbarkeit, nicht aber territorial eingrenzbar. Das Strafrecht ist jedenfalls in seiner nationalen Ausformung territorial begrenzt. Beides passt nicht zusammen. Unklar ist dabei nicht nur, was es in concreto zu schützen gilt, sondern auch durch wen. Beide Sachfragen bedürfen der internationalen Verständigung, gerade weil sich der Datenverkehr und Informationsaustausch im Internet nicht an staatlichen Grenzen anhalten lässt.

Zur Lösung kommen genau drei Dinge in Frage: Entweder man begrenzt (1) das Internet unter Ausschluss bestimmter user und unter vollständiger user-Kontrolle, baut es also letztlich neu oder man entgrenzt (2) das Strafrecht bzw. die Strafrechte im Sinne eines Internetstrafrechts für alle Internetuser eines world wide web-Staates. Im ersten Fall wird letztlich der user entmündigt und seines derzeit faktischen Hauptkommunikationsmittels beraubt. Er wäre völlig überwacht. Der zweite Fall kommt einer Staatsentmündigung gleich. Schon welches Weltorgan hierüber zu befinden hätte, ist fraglich.

In einem hier angedachten dritten Ansatz wird das Kompetenzverteilungsprinzip zum Prinzip der Prinzipe unter einer neuen Ausrichtung der einseitigen Strafanwendungsrechte

[67] Dies wäre aber wohl derzeit nach extensiver Auslegung des Erfolgsbegriffs im deutschen Strafrecht tatsächlich der Fall, so auch *Sieber*, NJW 1999, 2065 (2067). Vgl. etwa *B. Heinrich*, GA 1999, 72 (76, 82); Einstellungsverfügung des Generalbundesanwalts MMR 1998, 93 (Obiter Dictum).

[68] Ebenso *Kretschmer* (Fn. 6), B. III. (Manuskript S. 262).

[69] Vgl. *Oehler* (Fn. 60), Rn. 134 ff., 682 ff.

[70] Deutlich insoweit *L. Wörner/M. Wörner* (Fn. 39), S. 203 (S. 255).

[71] Dass solches Umdenken auch im nationalen Strafrecht angezeigt ist, zeigen die Ausführungen von *Zabel*, JZ 2011, 617 zur „Governance" im Strafrecht.

[72] Dagegen ausführlich *L. Wörner/M. Wörner* (Fn. 39), S. 203 (S. 227 ff.).

[73] S.o.; ähnlich *Kretschmer* (Fn. 6), B. III. (Manuskript S. 264).

[74] *L. Wörner/M. Wörner* (Fn. 39), S. 203 (S. 255).

[75] Ausdrücklich schon *L. Wörner/M. Wörner* (Fn. 39), S. 203 (S. 235, 255).

[76] *L. Wörner/M. Wörner* (Fn. 39), S. 203 (S. 255).

nicht auf Basis eines rein staatlichen Souveränitätsgedankens, sondern auf Basis eines Solidaritätsgedankens gegenüber den eigenen Staatsbürgern und gegenüber den anderen Staaten. „We need traffic rules", heißt es bei *Ladeur*.[77] So soll etwa die Zuständigkeit für Gerichte in den USA betreffend Tätigkeiten im Internet nach US-amerikanischem Recht dann gegeben sein, wenn der Beschuldigte durch seine Handlung nicht nur geringfügige Auswirkungen (minimum contacts) auf den Staat, welcher die Zuständigkeit der Strafverfolgung für sich in Anspruch nimmt, herbeiführt.[78] Der im Bereich der Rechtshilfe bereits geforderten Solidarität bedarf es im Hinblick auf territorial entgrenzte transnationale und internationale Kriminalitätsbereiche auch für die Strafanwendungsrechte und auch in der Verständigung über die transnational zu schützenden Rechtsgüter selbst. Das sollte auf Dauer zu einem Umdenken weg von staatlich einseitig gedachter Souveränität führen. An Lotus anschließend könnte das die Nachricht von 2011 aus Istanbul sein.

[77] *Ladeur*, German Law Journal 2009, 1201 (1214): „ […] for the internet and the information society, not the protection of any data of a nomadic individualism which fights against any restriction of its autonomy. […] Hybridization and the proliferation of linkages through networks are two of the characteristics of the internet. Instruments for the protection of the variety of the internet and the limitation of state power in the network of networks should make use of these paradigmatic phenomena."

[78] Hervorgehend aus dem Verfahren „Pres-Kap v. System One Direct" (District Court of Appeal of Florida, Third District, Urt. v. 12.4.1994 – No. 93-1440), der ersten Entscheidung, in welcher sich US-Gerichte mit Zuständigkeitskonflikten im Internet beschäftigen mussten. Vgl. dazu *Primig*, Internationales Strafrecht und das Internet, 2002, S. 4 f. (unter: http://rechtsprobleme.at/doks/primig-1-internationales_strafrecht.pdf [12.7.2012]); *Kuner*, CR 1996, 454. Im Internet ist diese Entscheidung einsehbar unter: http://www.loundy.com/CASES/Pres-Kap_v_System_One.html (12.7.2012). S. zu den verschiedenen Bestimmungen des U.S.C. (United States Code) z.B.: http://uscode.house.gov/search/criteria.shtml (12.7.2012). Aus der Entscheidung: „It is settled law that an individual's contract with an out-of-state party alone can (not) automatically establish sufficient minimum contacts in the other party's home forum to support an assertion of in personam jurisdiction against the out-of-state defendant, even where, as here, the foreign defendant allegedly breaches that contract by failing to make the required payments in Florida."

Steuerstrafrecht als Cybercrime!

Zwischenruf aus der Praxis

Von Rechtsanwalt Dr. **Bernd Groß**, LL.M., Frankfurt a.M.

Nur ganz wenige Wirtschaftsstraftaten haben heute nichts mit Computern zu tun. Während man bis Ende der neunziger Jahre Straftaten im Zusammenhang mit dem Internet mit Kinderpornographie in Verbindung setzte, ist in den letzten Jahren das Internet von Kriminellen meist dazu gebraucht worden, illegal Gelder zu verdienen.[1] *Was genau unter Cybercrime zu verstehen ist, lässt sich nur sehr schwer exakt definieren. Allgemein werden dem Cybercrime alle Straftaten zugeordnet, bei denen die EDV Tatmittel und/oder Tatobjekt ist. Oft werden das Internet und Computer im Zusammenhang mit Betrugsfällen (Abofallen, Phishing, Skimming etc.) wahrgenommen, also mit Taten, bei denen es ein ganz konkretes Opfer gibt.*

Ein aktuelles Beispiel aus der Praxis zeigt, dass man allein mit Computern, Fachwissen und krimineller Energie ausgerüstet dem deutschen Steuerzahler hunderte Millionen Euro „stehlen" kann und hierbei – unter Ausnutzung der Schwierigkeiten internationaler Rechtshilfe – weitgehend ungestört bleibt.

I. Das Prinzip

Im Jahr 2005 wurde innerhalb der Europäischen Union zum Schutz der Umwelt der Handel mit CO2-Zertifikaten eingeführt.[2] Vereinfach dargestellt funktioniert der Handel so, dass jeder Industrienation eine feste Menge an Zertifikaten zugeteilt wird. Soweit diese Zertifikate nicht benötigt werden, kann damit (zunächst zwischen Staaten) Handel getrieben werden. Die Europäische Union hat darüber hinaus den Emissionshandel auf Unternehmensebene eingeführt. Unternehmen werden zu einem Stichtag bestimmte Verschmutzungsrechte eingeräumt, wobei die Zuteilung jedes Jahr abnimmt. Verbraucht ein Unternehmen die ihm zugeteilten Rechte nicht, so kann es diese an andere Unternehmen veräußern, die einen höheren Bedarf haben. Somit entsteht ein Handel, der zum einen über Börsen (wie beispielsweise die EEX in Leipzig), zum anderen zwischen Unternehmen direkt (Over the Counter „OTC-Handel") stattfindet.

Bei den Emissionszertifikaten handelt es sich um eine lediglich virtuell existierende Nummernkette. Um am Handel mit Zertifikaten teilnehmen zu können, bedarf es der Anmeldung bei einem Emissionshandelsregister. In Deutschland werden diese Konten bei der Deutschen Emissionshandelsstelle (DEHSt) geführt. Die Anmeldeformalitäten konnten jedenfalls in der Vergangenheit sehr einfach elektronisch erledigt werden. Die Zertifikate werden dann zwischen den Vertragspartnern von Register zu Register übertragen, indem festgelegte Passwörter eingegeben werden, die die Übertragung in etwa vergleichbar mit dem Online-Banking legitimieren. Der Zugang zu dem Emissionshandelsregister konnte von jedem Internetanschluss aus weltweit erfolgen. Eine Übertragung der Emissionszertifikate außerhalb des Registers ist nicht möglich, so dass die Transaktionen nur online stattfinden können.

Die Emissionszertifikate unterliegen der Umsatzsteuer und erst im Sommer 2010 wurde das sog. „Reverse-Charge-Verfahren"[3] eingeführt, das Umsatzsteuerkettenbetrug unmöglich macht. Umsatzsteuervoranmeldungen werden im Übrigen elektronisch – d.h. über das Internet – abgegeben.

Bereits seit einigen Jahren haben Kriminelle erkannt, dass das System der Umsatzsteuer in Europa in hohem Maße anfällig für Betrug ist. Durch sog. „Umsatzsteuerkarusselle" entsteht beispielsweise dem deutschen Steuerzahler ein jährlicher Schaden in Milliardenhöhe. Das System ist dabei verblüffend einfach: Eine (gerade gegründete oder bislang inaktive) Gesellschaft importiert eine beliebige Ware aus einem anderen EU-Land. Diese Gesellschaft erhält die Ware ohne Umsatzsteuer. Sie verkauft die Ware zu einem günstigen Preis[4] plus Umsatzsteuer (19 %) an eine weitere Gesellschaft (Buffer), die die Ware ihrerseits mit Umsatzsteuer an eine dritte Gesellschaft (Distributor) veräußert. Die letzte Gesellschaft in der Kette veräußert die Ware ins Ausland zurück und erhält vom Finanzamt die Vorsteuer erstattet. Der Buffer erhält ebenfalls die abgeführte Vorsteuer zurück. Weil er selbst jedoch etwas mehr Steuer vom Distributor erhält als er bezahlt, entsteht beim Buffer eine Zahllast.

Je professioneller die Ketten organisiert sind, desto mehr Buffer werden eingesetzt. Die erste Gesellschaft erhält die Umsatzsteuer von ihrem direkten Handelspartner, sie gibt jedoch keine Steuererklärung ab. Vielmehr wird die Vorsteuer ins Ausland transferiert und die Hintermänner verschwinden, weshalb die erste Gesellschaft auch „missing trader" genannt wird. Weil es sich bei den „missing tradern" zumeist um Gesellschaften handelt, die von der monatlichen Abgabe von Umsatzsteuererklärungen befreit sind, fällt das Ganze oft lange Zeit nicht auf.[5]

Der Distributor ist – jedenfalls bei groß angelegten Ketten – zumeist eine renommierte Gesellschaft, deren Verantwortliche entweder benutzt werden, ohne selbst an der Kette be-

[1] Vgl. *Vassilaki*, MMR 2006, 212.

[2] Grundlage bildet das Kyoto-Protokoll von 1997, das am 16.2.2005 in Kraft trat. Der Emissionshandel in der EU begann am 1.1.2005.

[3] Vgl. § 13b Abs. 2 Nr. 6 UStG. Beim Reverse-Charge-Verfahren wird die Verpflichtung zur Zahlung der Umsatzsteuer auf den Leistungsempfänger verlagert. Der Vorteil besteht darin, dass Vorsteuerbeträge in erheblichem Umfang nicht mehr durch das Finanzamt ausgezahlt werden, sondern nur noch verrechnet werden.

[4] Der günstige Preis ist das Haupterkennungsmerkmal einer Umsatzsteuerhinterziehungskette (vgl. § 25d Abs. 2 UStG). Es gilt der Grundsatz: „If a deal is too good to be true, it is probably not true."

[5] Neuerdings werden bei Hinterziehungsketten auch Gesellschaften als Importeur eingesetzt, die ihre Steuererklärungen korrekt abgeben, zum Zeitpunkt der Zahlungsverpflichtung allerdings – wie von Anfang an geplant – insolvent sind.

teiligt zu sein, oder aber ihrerseits an den enormen Gewinnen durch „Kick-backs“ oder gar durch Einschaltung eigener Handelsfirmen beteiligt werden. Der große Vorteil beim Einsatz einer renommierten Gesellschaft ist, dass diese zum einen die Ware und die Umsatzsteuer finanzieren kann, zum anderen von den Steuerbehörden zunächst kein Verdacht geschöpft wird.

Alle Gesellschaften in der Kette sind zumeist hervorragend organisiert, um keinen Verdacht aufkommen zu lassen. Sie verfügen bei groß angelegten Hinterziehungsketten über einen professionellen Auftritt, es werden renommierte Steuerberater beauftragt, die Buchhaltung und Rechnungslegung wird mit großem Aufwand betrieben und es werden umfassende sog. „KYC-Prozesse“[6] für die Lieferanten durchgeführt, damit das Finanzamt möglichst lange keinen Verdacht schöpft.

Bei professionellen Hinterziehungsketten mit herkömmlichen Waren werden die Waren tatsächlich von einer Gesellschaft zur nächsten verbracht, damit wiederum formal der Eindruck entsteht, alles laufe korrekt ab. Hierdurch entsteht ein erheblicher logistischer und finanzieller Aufwand, weil die Waren ins Ausland verbracht werden müssen. Zusätzlich muss beachtet werden, dass dieselben Waren nicht mehrmals in einer Kette verwendet werden, weil Warendoppelungen häufig als sicheres Zeichen für Umsatzsteuerbetrug gelten. Jahrelang galt der Handel mit Telefonen, Computerteilen und andere elektronische Waren, die im Verhältnis zum Gewicht (und somit zu den Lager und Transportkosten) relativ teuer sind, als besonders anfällig für derartige Betrügereien.[7]

Wohl zunächst in Frankreich und England kam die Idee auf, dass ein Umsatzsteuerkarussell sich auch mit Emissionszertifikaten betreiben lässt, weil diese umsatzsteuerpflichtig sind. Die Vorteile liegen auf der Hand: Zunächst braucht ein Emissionshändler keine aufwendigen Büroräume und Lagerhallen. Auch die Gefahr, dass die gehandelte Ware drastisch an Wert verliert, bevor sie tatsächlich veräußert wird, ist nicht gegeben. Der entscheidende Vorteil ist aber, dass die Zertifikate lediglich als virtuelle Nummern in Emissionshandelsregistern angeboten werden. Es bedarf folglich nur eines Computers, eines Zugangs zum Emissionshandelsregister und eines Online-Banking-Systems, um einen derartigen Steuerbetrug zu begehen. Hinzu kommt noch eine weitere Besonderheit, die für den Umsatzsteuerbetrug geradezu ideal ist. Ursprünglich werden die Emissionszertifikate in Blöcken mit fortlaufenden Nummern vergeben. Bei einer Übertragung in ein anderes Register hat der Übertragende allerdings keinen Einfluss auf die Auswahl der Nummern. Somit werden bei jeder Transaktion die Nummern neu gestückelt und gemischt, so dass es nach kurzer Zeit faktisch unmöglich ist, die Nummern zu verfolgen, um Doppelungen festzustellen.

II. Die Umsetzung

Nachdem in England das Reverse-Charge-Verfahren eingeführt wurde, wurden ab Mitte 2009 in Deutschland Gesellschaften gegründet, die als Gesellschaftszweck den Handel mit Emissionszertifikaten hatten. Für die Gesellschaften wurden in Deutschland Bankverbindungen und Emissionshandelsregister eingerichtet. Weil es bereits Gerüchte über Steuerhinterziehung in diesem Bereich gab, waren nur wenige Banken bereit, für die Gesellschaften überhaupt Konten einzurichten.

Der Markt für (echte) Endabnehmer ist beim Emissionshandel beschränkt, weshalb sich anfangs kaum Distributoren fanden, die die Waren erwerben wollten. In diesem Zusammenhang muss im Übrigen darauf hingewiesen werden, dass es ein weit verbreiteter Fehlglaube ist, dass Umsatzsteuerkettenbetrug am Ende der Kette den Export voraussetzt. Das System funktioniert genauso, wenn am Ende der Kette ein deutscher Endverbraucher steht. Vermutlich wäre es im Zusammenhang mit den Emissionszertifikaten mangels Endverbrauchern und Exporteuren nie zu einem der größten Umsatzsteuerhinterziehungsfälle in Deutschland gekommen, wenn nicht eine Abteilung einer großen Bank in Frankfurt am Main in den Handel mit Emissionszertifikaten eingestiegen wäre.

Die Bank ging im Spätsommer 2009 mit sechs der gerade neu gegründeten Gesellschaften Handelsbeziehungen ein und nahm diesen Gesellschaften bereits nach wenigen Wochen insgesamt Emissionszertifikate im Wert von mehreren Millionen Euro täglich ab.[8] Die Bank veräußerte die Zertifikate ihrerseits an eine ihrer Tochtergesellschaften in England, so dass sie die gezahlten Steuern vom Finanzamt Frankfurt am Main zurückerstattet erhielt. Die Lieferanten wurden seitens der Bank dann bereits nach einem Tag bezahlt, wobei die Bank elektronische Gutschriften erstellte, um sicherzustellen, dass die Dokumentation für die Buchhaltung und Steuer korrekt ist. Die Tochtergesellschaft der Bank veräußerte die Zertifikate sodann an die Organisatoren des Betruges. Über den Umweg Dubai kamen die Zertifikate wieder nach Frankfurt am Main zurück. Alle Transaktionen konnten in Sekunden erfolgen, weil alles über das Internet geschah.

Wie einfach es das Internet Betrügern macht, ihr Handeln zu verschleiern, zeigt der tatsächliche Ablauf der Geschäfte. Die Abstimmung der Geschäfte zwischen den Gesellschaften lief offiziell über Telefon oder E-Mail, wobei den Beteiligten stets bewusst war, diese Kommunikation könnte von Ermittlungsbehörden abgehört werden. Tatsächlich kommunizierten die Mitglieder der Kette aber über Internetdienste wie Skype oder MSN. Während also in den „offiziellen“ Gesprächen der Eindruck erweckt wurde, als fänden zwischen den Gesellschaften reale Verhandlungen statt, wurden die illegalen Absprachen „online“ über Messenger-Systeme getroffen.

Bei vielen Gesellschaften wurden dann auch die Zahlungsvorgänge und die Übertragung der Zertifikate nicht aus Deutschland vorgenommen. Vielmehr nutzen die Hintermänner die Möglichkeit des weltweiten Zugriffs auf die Online-Systeme, um derartige Transaktionen selbst durchzuführen.

[6] KYC = Know your customer.

[7] Zu den steuerlichen und strafrechtlichen Aspekten des Umsatzsteuerkarussells *Gehm*, NJW 2012, 1257.

[8] Insgesamt entstand in der Zeit von September 2009 bis April 2010 allein mit den genannten sechs Gesellschaften ein Steuerschaden von mehr als 300 Mio. Euro.

Ein weiteres „Cybercrime"-Merkmal bestand dann in der Sicherung der Gelder: Nachdem die Bank ihren Lieferanten bezahlt hatte, wurden die Beträge an den Vorlieferanten per Online-Überweisung auf ein deutsches Konto transferiert. Von dort wurden die Gelder unmittelbar ins Ausland überwiesen, wobei hier sog. „Plattform-Banken" genutzt wurden. Vereinfacht dargestellt, handelt es sich hier scheinbar um Banken. Tatsächlich sind dies lediglich Gesellschaften, die ein Konto bei einer realen Bank im Ausland haben. Diese Gesellschaften, die meist das Wort „Bank" im Namen führen, verfügen aber jedenfalls virtuell über ein hoch professionelles eigenes Konten- und ein eigenes Online-Banking-System. Es sieht somit alles danach aus, als habe man es mit einer realen Bank zu tun. Hierdurch wird das Nachverfolgen der Gelder zwischen den Gesellschaften für die Ermittlungsbehörden massiv erschwert, weil die Gelder tatsächlich bereits längst wieder abgeflossen sind, während virtuell der Eindruck entsteht, sie würden innerhalb der „Plattform-Bank" transferiert.

III. Die Aufklärung

Nachdem die Ermittlungsbehörden das Treiben fast sechs Monate beobachtet hatten, wurden im April 2010 zunächst die Geschäftsführer der sechs Buffer-Gesellschaften festgenommen und hunderte von Gesellschaften durchsucht. Weil sich die Ermittlungsbehörden – wie von den Tätern geplant – auf die herkömmlichen Kommunikationsmittel konzentriert hatten, waren die Ermittlungsergebnisse zunächst im Verhältnis zum Aufwand relativ dürftig, was auch daran gelegen haben mag, dass einige der Täter – wie sich im Prozess herausstellte – Kenntnis von der bevorstehenden Durchsuchung hatten.

Allerdings gelang es der Generalstaatsanwaltschaft Frankfurt am Main mit Hilfe des Bundeskriminalamtes unter großem Aufwand Stück für Stück, die elektronischen Spuren zu verfolgen. So wurde ermittelt, dass eine Vielzahl der beteiligten Gesellschaften ihre hochprofessionellen Webseiten bei einem Programmierer in Pakistan hatte erstellen lassen. Auch konnte nach einiger Zeit nachgewiesen werden, dass der Zugriff auf die Registerkonten vielfach aus Dubai erfolgt war. Der Durchbruch gelang allerdings, als die Ermittler in der Lage waren, auf sichergestellten Rechnern die dort abgelegten Chat-Konversationen (Skype-Protokolle etc.) wiederherzustellen. Nachdem dies gelungen war, folgten alsbald die ersten Geständnisse und die Aufklärung konnte – immerhin bezüglich der in Deutschland agierenden Buffer-Gesellschaften – zügig voranschreiten.

Die hinterzogenen Steuern konnten gleichwohl zum größten Teil bis heute nicht sichergestellt, die Hintermänner, die die Anklage in Dubai vermutet, nicht zur Rechenschaft gezogen werden.

Allerdings war in diesem Fall nicht der Fiskus das endgültige Opfer, sondern vielmehr die Frankfurter Bank. Weil einige wenige Mitarbeiter jedenfalls fahrlässig in die Hinterziehungskette eingebunden waren, wird der Bank nunmehr nach § 25d UStG der Vorsteuerabzug versagt, was im Ergebnis dazu führt, dass die Bank die Rechnung übernehmen muss.

IV. Cybercrime im Cybercrime

Es muss einem geradezu als ironische Wendung der Geschichte vorkommen, wenn man noch auf folgende Begebenheit zurückblickt: Im März 2010 hatte das ganze System ein derartiges Ausmaß angenommen, dass auch herkömmliche Cyber-Kriminelle auf den Plan gerufen wurden. Diesen gelang es, sich durch „Phishing"-Attacken die Zugangsdaten von einigen Gesellschaften zu den Handelsregisterkonten zu erschleichen und auf diese Weise Emissionszertifikate im Gegenwert von mehreren Millionen Euro zu stehlen. Offenkundig sind nicht einmal Cyber-Kriminelle vor Cybercrime sicher.

V. Fazit

Das Internet bietet gerade im Bereich der Vermögensstraftaten gut ausgebildeten Tätern unglaubliche Möglichkeiten, weshalb es zwingend erforderlich ist, dass die Ermittlungsbehörden mit dem technologischen Fortschritt mithalten.

Gerade im Bereich der Umsatzsteuerhinterziehung ist die Hemmschwelle bei rein virtuellen Taten sehr niedrig, weil letztlich niemand genötigt und auch keine individuelle Person geschädigt wird. Aus diesem Grund sind in groß angelegte Umsatzsteuerhinterziehungen bislang häufig seriöse Kaufleute, Bankmitarbeiter, Steuerberater oder gar Anwälte eingebunden.

Auch um Gesellschaften, wie die im Beispiel erwähnte Bank, vor derartigen Betrügereien zu schützen, wäre es ratsam, bei der Umsatzsteuer generell das Reverse-Charge-Verfahren einzuführen. Solange dies nicht geschieht, müssen neben den Ermittlungsbehörden auch die Gesellschaften selbst – insbesondere beim Handel mit Gütern, die virtuell vertrieben werden – stets genau hinterfragen, ob sie selbst Teil einer solchen Betrugskette sein könnten. Es bedarf keiner hellseherischen Fähigkeiten, um zu erkennen, dass die Emissionszertifikate nur der Anfang von Steuerhinterziehungstaten mit virtuellen Gütern waren.

Bei der Abwägung zwischen Eingriffsrechten des Staates und den Freiheitsrechten der Internetnutzer sind auch die Belange aller redlichen Nutzer zu berücksichtigen, die durch sich immer mehr verbreitende kriminelle Nutzungsmöglichkeiten des Internets Schaden erleiden.

Vorratsdatenspeicherung: Bestandsaufnahme und Ausblick

Von Rechtsanwalt **Felix Rettenmaier**, Frankfurt a.M., Rechtsreferendarin **Lisa Palm**, Mainz

I. Einleitung

Im Bereich des Cybercrime, d.h. im Bereich von Straftaten, bei denen der Computer als Tatmittel oder Tatgegenstand einer strafbaren Handlung eingesetzt wird, stellt die Beweissicherung eines der größten Probleme der Strafverfolgung dar. Delikte wie Computerbetrug, Softwarepiraterie und das Ausspähen von Daten (z.B. einer PIN), aber auch eine Vielzahl von Delikten aus anderen Bereichen des Strafrechts, sind häufig nur dann verfolgbar, wenn elektronische Daten, insbesondere Telekommunikationsverbindungsdaten (Telefon, Fax, E-Mail, SMS etc.), gesichert und zu Beweiszwecken verwendet werden können. Die Speicherung dieser Telekommunikationsverbindungsdaten, die sog. „Vorratsdatenspeicherung", sollte eine solche Sicherung ermöglichen. Für die rechtliche Betrachtung ist dabei zwischen Bestandsdaten nach § 3 Nr. 3 TKG, die als Daten eines Teilnehmers für die Begründung, Änderung oder Beendigung eines Vertragsverhältnisses erhoben werden – insbesondere Name, Kundenanschrift und Internetprotokolladresse (im Folgenden: „IP-Adresse") –, sowie den sensibleren Verkehrsdaten nach § 3 Nr. 30 TKG, die mit jedem Telekommunikationsvorgang erhoben, verarbeitet oder genutzt werden, zu unterscheiden.

II. Rechtliche Grundlagen

1. RL 2006/24/EG

Die Vorratsdatenspeicherung ist eine Reaktion der EU auf die Terroranschläge von New York, Madrid und London. Als Konsequenz regte die EU mit der Richtlinie RL 2006/24/EG an, alle Telekommunikationsverbindungsdaten der Europäer zu speichern, um diese den Ermittlungsbehörden zur Verfügung zu stellen.[1] Die Erhebung sollte anlassunabhängig (d.h. ohne Tatverdacht) erfolgen und die Daten sollten den Ermittlungsbehörden auf Abruf zur Verfügung stehen. Vorgesehen war eine möglichst flächendeckende präventive Speicherung aller für die Strafverfolgung oder Gefahrprävention nützlichen Daten. Infolgedessen verpflichtete die Richtlinie die Telekommunikationsanbieter, die von ihnen erfassten Daten mindestens sechs Monate und höchstens zwei Jahre zu speichern, um diese für die Verfolgung von schweren Straftaten bereitzustellen. Nach Maßgabe der Richtlinie oblag es den Mitgliedstaaten dafür Sorge zu tragen, dass die gespeicherten Daten insbesondere „unter vollständiger Achtung der Grundrechte" des jeweils Betroffenen an die zuständigen Behörden weitergegeben werden.

Vom ersten Entwurf der Richtlinie bis zu ihrer Verabschiedung im Parlament vergingen nur drei Monate. Die Richtlinie enthält keine näheren Regelungen zur Verwendung der Daten. Die Maßnahmen zum Datenschutz werden überwiegend den Mitgliedstaaten überlassen. Eine gerichtliche Überprüfung der Richtlinie am Maßstab der Charta der Grundrechte der Europäischen Union ist bislang nicht erfolgt.

[1] ABl. EU Nr. L 105 v. 13. 4.2006, S. 54.

2. §§ 113a, 113b TKG und § 100g Abs. 1 S. 1 StPO – eingeführt durch das Gesetz zur Neuregelung der Telekommunikationsüberwachung v. 21.12.2007

Seit 2008 wurden in der Folge in Deutschland auf der Grundlage des Telekommunikationsgesetzes Verbindungsdaten aus der Telefon-, E-Mail- und Internetnutzung sowie Handy-Standortdaten für sechs Monate gespeichert. Diese Daten waren für die Strafverfolgungsbehörden sowohl zur Strafverfolgung (repressiv) als auch zu Zwecken der Gefahrenabwehr (präventiv) abrufbar.

3. BVerfG, Urt. v. 2.3.2010 – 1 BvR 256/08, 1 BvR 263/08, 1 BvR 586/08

Das Bundesverfassungsgericht hat mit seinem Urteil[2] zur Vorratsdatenspeicherung die §§ 113a und 113b des TKG und auch § 100g Abs. 1 S. 1 StPO, soweit danach Verkehrsdaten i.S.d. § 96 Abs. 1 TKG, die nach § 113a TKG (Nummer, Kennung des Anschlusses, personenbezogene Berechtigungskennung, Beginn und Ende, Datum und Uhrzeit der Verbindung) erhoben wurden, wegen Verstoßes gegen Art. 10 Abs. 1 GG (Brief-, Post und Fernmeldegeheimnis) – entgegen einer zuvor ergangenen einstweiligen Anordnung – für nichtig erklärt.

Zur Begründung führte das BVerfG u.a. aus, dass durch die Datenspeicherung bei den Bürgern ein bedrohliches Gefühl des „Beobachtetseins" hervorgerufen werde. Das Gesetz stelle zudem nicht sicher, dass nur schwerwiegende Straftaten Anlass für eine Datenerhebung begründen dürfen. Ferner sei es unverhältnismäßig, Daten ohne Wissen des Betroffenen und ohne richterliche Anordnung abzurufen. Darüber hinaus werde der Verhältnismäßigkeitsgrundsatz verletzt.[3]

Aus Sicht des BVerfG ist der Ansatz der Vorratsdatenspeicherung jedoch nicht schlichtweg unvereinbar mit den Vorgaben des Grundgesetzes. Allerdings handle es sich um einen besonders schweren Eingriff mit einer Streubreite, wie ihn die Rechtsordnung bisher nicht kenne.[4] Das BVerfG hat die Vorschrift des § 100g StPO in seinem Urteil jedoch nicht vollumfänglich beanstandet.

Vielmehr hat es u.a. vorgegeben, dass eine Speicherung der Daten nicht direkt durch den Staat erfolgen dürfe. Die Speicherung für die Dauer von sechs Monaten müsse zudem die zeitliche Obergrenze darstellen[5] und die anlasslose Spei-

[2] BVerfG, Urt. v. 2.3.2010 – 1 BvR 256/08 u. a. = NJW 2010, 833 = EuZW 2010, 280; Auswertung im Lichte der „Solange-Rechtsprechung" von *Bäcker*, EuR 2011, 103; umfassende Bespr. bspw. bei *Schramm/Wegener*, MMR 2011, 9.

[3] BVerfG NJW 2010, 833 (848 f.).

[4] BVerfG NJW 2010, 833 (834).

[5] Dazu krit. *Forgó/Krügel*, K&R 2010, 217 (219): Das Gericht weicht damit den im Volkszählungsurteil manifestierten Grundsatz auf, dass der Einzelne gegen die unbegrenzte Erhebung seiner persönlichen Daten geschützt sei, indem es eine „vorsorgliche, anlasslose Datenspeicherung" als mit dem

cherung müsse – als erklärte Ausnahme – mit einem Begründungs- und Ausgestaltungsaufwand verbunden sein, da die Vorratsspeicherung von personenbezogenen Daten zu lediglich unbestimmten oder noch nicht bestimmbaren Zwecken[6] verboten sei. Insbesondere sollten die Daten nicht anlasslos, sondern ausschließlich zur Verfolgung schwerer Straftaten genutzt werden können. Im Rahmen der Strafverfolgung müsse demnach ein durch bestimmte Tatsachen begründeter Verdacht einer schweren Straftat vorliegen. Dabei sei es Aufgabe des Gesetzgebers, abschließend festzulegen, zur Verfolgung welcher Taten ein Datenabruf möglich sein soll.[7] Darüber hinaus sei in den fraglichen Gesetzen weder dem Datenschutz noch der Datensicherheit ausreichend Rechnung getragen worden.[8] Der Datenabruf dürfe nur bei einer hinreichend konkreten Gefahr für ein bedeutsames Rechtsgut erfolgen.[9] Eine Übermittlung und Nutzung der gespeicherten Daten sei zudem grundsätzlich unter einen Richtervorbehalt zu stellen.[10] Weniger strenge Anforderungen stellte das BVerfG an die (mittelbare) Verwendung vorsorglich gespeicherter Daten in Form von behördlichen Auskunftsansprüchen hinsichtlich bereits bekannter IP-Adressen, da hierdurch keine Persönlichkeits- und Bewegungsprofile verwirklicht werden könnten.[11]

Im Ergebnis stellte das BVerfG fest, dass die Bundesrepublik Deutschland über eine verfassungsrechtliche Identität[12] verfüge, nach der die Freiheitswahrnehmung der Bürgerinnen und Bürger nicht vollständig erfasst und registriert werden darf. Die (teilweise) verfassungsrechtliche Unbedenklichkeit folgt somit aus dem Ausnahmecharakter der Regelung.[13]

Dem Beschluss zur Vorratsdatenspeicherung von Telekommunikations-Verkehrsdaten[14] ist darüber hinaus zumindest zu entnehmen, dass der neu eingefügte § 110 Abs. 3 StPO[15], der die Sicherung und Durchsicht von Daten erlaubt, die sich auf externen Speichermedien befinden, auf die der Betroffene Zugriff hat, bei einer ordnungsgemäßen Verfahrensausgestaltung als verfassungskonform anzusehen ist.[16] Auch hier spielt das Kriterium der Anlassbezogenheit eine übergeordnete Rolle. Die Daten dürfen demnach gesichert werden; sind allerdings unmittelbar zu löschen, sobald sie für die Strafverfolgung nicht mehr erforderlich sind.[17]

III. Auswirkungen der Entscheidung des BVerfG

In der Praxis der Strafverteidigung stellt sich im Zusammenhang mit der bislang vorgenommenen Vorratsdatenspeicherung insbesondere das Problem, ob – und wenn ja, in welchem Umfang – diese Daten von den Ermittlungsbehörden zu Lasten des Betroffenen verwendet werden dürfen. Zur Beurteilung dieser Fragen ist zwischen einer Datenerhebung vor und nach der (abschließenden) Entscheidung des BVerfG zu unterscheiden.

1. Datenerhebungen vor der BVerfGE

Das BVerfG gab dem Eilantrag auf Außer-Kraft-Setzung der angegriffenen §§ 113a und 113b TKG im März 2008 mithilfe einer einstweiligen Verfügung teilweise statt.[18] Die Verwendung gespeicherter Daten wurde aufgrund drohender schwerwiegender und irreparabler Schäden auf schwere Straftaten im Sinne des § 100a Abs. 2 StPO begrenzt. Die Pflicht zur Datenspeicherung blieb bestehen.

Nach der späteren Nichtigkeitserklärung wurde die Verwertung von Datenerhebungen vor der Hauptsacheentscheidung des BVerfG bezweifelt. Ohne jegliche gesetzliche Ermächtigungsgrundlage gewonnene Beweismittel dürften in einem rechtsstaatlichen Verfahren nicht verwertbar sein. Dies müsse auch gelten, wenn die Rechtsgrundlage nachträglich entfalle. Dass das BVerfG eine zukünftige Regelung zur Beweiserhebung für verfassungsrechtlich zulässig halte, könne hieran nichts ändern. Die erhobenen Daten hätten unverzüglich nach der Feststellung der Nichtigkeit der Vorschriften gelöscht werden müssen.[19] Für alle Fälle, die nicht von der einstweiligen Anordnung des BVerfG umfasst waren, sollte in Ansehung der Schwere des Rechtsverstoßes von einem fernwirkenden Verwertungsverbot ausgegangen werden.[20]

Nach Auffassung des OLG München[21] und des BGH[22] sind die Daten – auch nach Feststellung der (teilweisen) Nichtigkeit der gesetzlichen Grundlagen der Vorratsdatenspeicherung – verwertbar. Die Erhebung sei nach der zum Zeitpunkt der Erhebung geltenden Rechtslage zulässig gewesen, da sie den Anforderungen entsprach, die das BVerfG in

Telekommunikationsgeheimnis prinzipiell vereinbar qualifiziert.

[6] BVerfG NJW 2010, 833 (841 in Rn. 231).

[7] Dazu eingehend *Schramm/Wegener*, MMR 2011, 9 (11).

[8] BVerfG NJW 2010, 833 (840 in Rn. 221-225).

[9] BVerfG NJW 2010, 833 (849).

[10] BVerfG NJW 2010, 833 (843 in Rn. 247).

[11] BVerfG NJW 2010, 833 (844 in Rn. 254 f.).

[12] BVerfG, Beschl. v. 28.10.2008 – 1 BvR 256/08, eine direkt gegen die Vorschrift gerichtete Verfassungsbeschwerde wurde mangels Rechtswegerschöpfung insoweit als unzulässig verworfen, BVerfG NVwZ 2009, 103.

[13] Näher dazu *Roßnagel*, NJW 2010, 1238 (1240).

[14] BVerfG, Beschl. v. 16.6.2009 – 2 BvR 902/06 = NJW 2009, 2431.

[15] Aufgehoben mit Wirkung v. 1.9.2004 durch Gesetz v. 24.8. 2004 (BGBl. I 2004, S. 2198); Abs. 3 eingef. mit Wirkung v. 1.1.2008 durch Gesetz v. 21.12.2007 (BGBl. I 2007, S. 3198), entsprechend der Forderung des Art. 19 Abs. 2 des Übereinkommens des Europarats über Computerkriminalität.

[16] Vgl. *Klein*, NJW 2009, 2996 (2999).

[17] *Nack*, in: Hannich (Hrsg.), Karlsruher Kommentar zur Strafprozessordnung, 6. Aufl. 2008, § 110 Rn. 8.

[18] BVerfG, Beschl. v. 11.3.2008 – 1 BvR 256/08 = NVwZ 2008, 543.

[19] Anm. OLG München NJW-Spezial 2010, 601; Anm. BGH NJW-Spezial 2011, 216.

[20] *Volkmer*, NStZ 2010, 318 (320).

[21] OLG München MMR 2010, 793 = BeckRS 2010, 19914.

[22] BGHSt 56, 138 = NJW 2011, 1377; BGH NJW 2011, 1827; OLG München MMR 2010, 793 = BeckRS 2010, 19914.

seiner einstweiligen Verfügung aufgestellt hatte. Durch die Hauptsacheentscheidung sei die Rechtsgrundlage für die Maßnahme auch nicht rückwirkend entfallen. Die Verfassungsrichter hatten insoweit zwar angeordnet, dass im Rahmen laufender Auskunftsersuchen der Behörden erhobene Daten zu löschen seien. Hinsichtlich bereits übermittelter Daten seien jedoch auch für noch nicht rechtskräftig abgeschlossene Verfahren keine Restriktionen angeordnet worden. Ein rückwirkendes Beweisverwertungsverbot sei deshalb vom BVerfG nicht gewollt gewesen. Insoweit stellte der BGH fest, dass Telekommunikationsdaten, die vor dem 2.3. 2010 auf der Grundlage der einstweiligen Anordnung des BVerfG rechtmäßig gewonnen und an die ersuchenden Behörden übermittelt wurden, in einem Strafverfahren zu Beweiszwecken verwertet werden dürfen.

Zwar begründet eine anlasslose Speicherung aller Telekommunikationsdaten und folglich auch deren Verwertung einen schwerwiegenden Grundrechtseingriff.[23] Beweiserhebung und -verwertung greifen hier indes nicht in den absolut geschützten Kernbereich privater Lebensgestaltung ein. Der Eingriff in das Telekommunikationsgeheimnis kann durch die damit verfolgten Zwecke (Effektivierung der Strafverfolgung, der Gefahrenabwehr und der Erfüllung der Aufgaben der Nachrichtendienste) gerechtfertigt sein. Art. 10 Abs. 1 GG verbietet nicht jede vorsorgliche Erhebung und Speicherung von Daten überhaupt, sondern schützt vor einer unverhältnismäßigen Gestaltung solcher Datensammlungen und hierbei insbesondere vor einer entgrenzenden Zwecksetzung.[24]

Im vorliegenden Fall erfolgte die Datenerhebung und -verwertung in einem Ermittlungs- bzw. Strafverfahren und war auf den Verdacht einer Straftat nach § 244a StGB gestützt, die als schwer zu qualifizieren ist. Auch beschränkte sich der Eingriff auf Standortdaten eines benutzten Mobiltelefons und den Umstand, dass gewisse Telefonate geführt wurden, obwohl sogar eine Telekommunikationsüberwachung mit Aufzeichnung der Gesprächsinhalte auf der Grundlage von § 100a Abs. 2 Nr. 1 lit. j StPO zulässig gewesen wäre. Schließlich sei bei einer Gesamtabwägung auch zu berücksichtigen, dass eine Tataufklärung und ein Tatnachweis ohne die bereits erhobenen Daten – deren Erhebung zum Zeitpunkt ihrer Speicherung und Übermittlung von einer einstweiligen Anordnung des Bundesverfassungsgerichts als fortwirkende Legitimationsgrundlage gedeckt war – nicht oder zumindest nur wesentlich erschwert möglich gewesen wären. Die Nichtigkeitserklärung wirkt zwar ex tunc, dies betrifft indessen nicht die ebenfalls in Gesetzeskraft erwachsene einstweilige Anordnung. Ein Löschungsgebot wurde durch das BVerfG nicht statuiert.

2. Ermittlung der IP-Adresse nach bisherigem deutschem Datenschutzrecht

Das OLG Hamburg[25] stellte in einer anderen Entscheidung im Zusammenhang mit einer bereits erfolgten Urheberrechtsverletzung fest, dass das Ermitteln der IP-Adressen nach deutschem Datenschutzrecht nicht rechtswidrig sei. Es komme insofern kein Beweisverwertungsverbot in Betracht, zumal bei den ermittelten IP-Adressen ein Personenbezug mit normalen Mitteln ohne weitere Zusatzinformationen nicht hergestellt werden könne. Der Personenbezug werde erst durch die seitens der Staatsanwaltschaft nach § 161 Abs. 1 S. 1 und § 163 StPO angeforderte oder gemäß § 101 Abs. 9 UrhG gerichtlich angeordnete Auskunft des Providers ermöglicht.[26]

3. Diskussionsentwurf des Bundesministeriums der Justiz (Stand: 7.6.2011)

Das Bundesministerium der Justiz leitete aus dem Urteil des BVerfG zunächst die grundsätzliche Pflicht der Bundesregierung ab, sich für die Freiheitsrechte der Bürger auf europäischer Ebene einzusetzen.[27] Trotz der durch das BVerfG vorgegebenen Beschränkungen soll den wesentlichen Interessen der Strafverfolgung im Rahmen einer Abwägung von Sicherheitsbelangen und Grundrechten noch Rechnung getragen werden können. Vor diesem Hintergrund sollte sowohl die StPO als das TKG wie folgt geändert werden:

a) § 100j StPO-E

Der neue § 100j StPO (Sicherungsanordnung) sieht eine Anordnungsbefugnis für eine anlassbezogene Speicherungspflicht vor. Diese ist mit einem Erforderlichkeitsvorbehalt versehen und ist auf das notwendige Maß begrenzt. Die Sicherungsanordnung muss damit für die Erforschung des Sachverhalts – oder die Ermittlung des Aufenthaltsortes eines Beschuldigten – erforderlich sein. Von der Anordnung ist weiterhin gemäß § 100j Abs. 1 S. 2 StPO-E abzusehen, wenn die Voraussetzung des § 100g StPO (Straftaten von erheblicher Bedeutung) nicht vorliegen würden. Eine Begrenzung des Grundrechtseingriffs wird insbesondere dadurch erreicht, dass nur ein Rückgriff auf die bei den Telekommunikationsunternehmen ohnehin bereits vorhandenen gesicherten („eingefrorenen", sog. Quick-Freeze, in den USA üblich) und durch das Telekommunikationsunternehmen erhobenen Daten genommen werden kann. Die vorhandenen Daten werden also erst in dem Moment eingefroren, in dem die Verdachtslage den Anforderungen der Eingriffsnorm entspricht, sodass auf diese im Verfahren zurückgegriffen werden kann.

Die Speicherung der Daten erfolgt nach der Anordnung auf eine begrenzte Zeit. Mit Ablauf der Sicherungsfrist (höchstens ein Monat, § 100j Abs. 2 StPO-E) sind die erhobenen Daten unverzüglich zu löschen, § 100j Abs. 5 StPO-E, soweit keine Fortdauer der Maßnahme für maximal einen weiteren Monat angeordnet wird. In der Regel schließt sich an die Sicherungsanordnung eine Auskunftserteilung zur Verwendung der erhoben Daten im Ermittlungsverfahren nach § 100g StPO an. §100j StPO-E lässt es insoweit zunächst genügen, dass die – auch von der Polizei oder der Staatsan-

[23] BVerfG NJW 2010, 833 (838 f. in Rn. 212).
[24] BVerfG NJW 2010, 833 (838 in Rn. 206 f.).
[25] OLG Hamburg MMR 2011, 281 = GRUR-Prax 2010, 536.
[26] OLG Hamburg MMR 2011, 281 (282).
[27] Entwurf des „Gesetzes zur Sicherung vorhandener Verkehrsdaten und Gewährleistung von Bestandsdatenauskünften im Internet", RDV 2011, 202.

waltschaft in eigener Kompetenz zu treffende – Anordnung für die Erforschung des Sachverhaltes oder die Ermittlung des Aufenthaltsortes eines Beschuldigten erforderlich ist. Den Strafverfolgungsbehörden werden die gespeicherten Daten schließlich durch Zugriff gemäß § 100g StPO unter Richtervorbehalt und dem Vorbehalt einer Straftat von erheblicher Bedeutung für einen begrenzten Zeitraum zur Verfügung gestellt.

Dagegen wird teilweise vertreten, dass nicht nur ein „Quick-Freeze"-Verfahren einen verhältnismäßigen Eingriff in das Recht auf informationelle Selbstbestimmung und des Fernmeldegeheimnisses der Nutzer darstellt, sondern das Interesse an einer effektiven Terrorismusbekämpfung und sonstiger Kriminalität darüber hinausgehende Maßnahmen rechtfertigt.[28] Für die Wiedereinführung der bis zum Urteil des BVerfG bestehenden Rechtslage sollen vor allem zwei Gründe der Gefahrenabwehr sprechen: dass die moderne Telekommunikation zum einen eine ungeahnte Möglichkeit einer widerstandsfreien Bündelung von Wissen, Handlungsbereitschaft und krimineller Energie über Zeit und Raum hinweg verschafft und zum anderen, dass eine Speicherung von Spuren die Entstehung eines teilweise „rechtsfreien Raums" verhindert.[29]

b) § 100k StPO-E

Gemäß § 100k StPO-E (Auskunftspflicht) soll im Internetzugangsbereich eine eng befristete Speicherung von Verkehrsdaten zu dem Zweck erfolgen, Bestandsdatenauskünfte insbesondere zur Bekämpfung der Kinderpornografie zu den Strafverfolgungsbehörden bereits bekannten IP-Adressen zu ermöglichen, ohne die Verkehrsdaten selbst an die Strafverfolgungsbehörden herauszugeben. Anhand dieser Daten wird nicht ersichtlich, wer wen wann angerufen oder wem eine E-Mail geschrieben hat oder an welchem Standort sich der Nutzer wann befand, sondern nur zu welcher Zeit der Betroffene welcher IP-Adresse als Verantwortlicher zuzuordnen ist.

Für die nach Maßgabe des § 111 TKG erhobenen Bestandsdaten des Telekommunikationsunternehmens besteht eine Speicherungspflicht auch, soweit die Daten nicht für betriebliche Zwecke erforderlich sind, § 111 Abs. 1 S. 1 TKG. Strafverfolgungsbehörden dürfen die Herausgabe dieser Bestandsdaten bislang nach der Ermittlungsgeneralklausel (§§ 161 Abs. 1 S. 1, 163 StPO i.V.m. § 113 Abs. 1 TKG) unter der Voraussetzung verlangen, dass die Erhebung der Bestandsdaten für die Verfolgung einer verfahrensgegenständlichen Straftat erforderlich ist. Einer gerichtlichen oder staatsanwaltschaftlichen Anordnung bedurfte es dabei nicht.

Beachtenswert ist, dass das BVerfG diese Regelung zur Erhebung von Bestandsdaten grundsätzlich nicht beanstandet. Es hat jedoch angemerkt, dass auf der Ebene der Eingriffsschwelle sicherzustellen ist, dass eine Auskunft nur auf Grund eines „hinreichenden Anfangsverdachts oder einer konkreten Gefahr auf einzelfallbezogener Tatsachenbasis" erfolgen darf. Auch hier erfolgt für die Auskunftserteilung kein Zugriff der Strafverfolgungsbehörden auf die Verkehrsdaten.

c) § 113a TKG-E

§ 113a TKG (Datenspeicherung) sieht eine zeitlich eng befristete Speicherung von bei der Nutzung von Internetzugangsdiensten anfallenden Daten vor, ohne dass ein Zugriff der Strafverfolgungsbehörden auf Verkehrsdaten zulässig ist. Datensicherheit und Datenqualität der anlasslos gespeicherten Daten müssen nach Maßgabe des BVerfG verbessert werden. Die Speicherungsdauer wurde daraufhin auf sieben Tage beschränkt, für deren Ingangsetzung das Ende der Internetnutzung, d.h. der Entzug der zugewiesenen IP-Adresse, maßgeblich ist. Der Inhalt der Kommunikation darf hingegen nicht gespeichert werden.

Bis heute ist es aufgrund der von tiefen Meinungsverschiedenheiten geprägten Diskussion noch zu keiner Neuregelung gekommen.

IV. Aktuelle Entwicklungen

1. Bericht der EU-Kommission über die Bewertung der Richtlinie

Im April 2011 legte die EU-Kommission einen Bericht über die Bewertung der Vorratsdatenspeicherungsrichtlinie (2006/24/EG) vor.[30] Dort wurde Bilanz über die Anwendung der Richtlinie gezogen – nicht ohne erneut die Bedeutung der Telekommunikationsdatenspeicherung als wichtiges Instrument zum Schutz vor schweren Straftaten zu betonen. Dabei wurde nicht übersehen, dass damit eine beträchtliche Einschränkung des Rechts auf Privatsphäre einhergeht.[31] Die Datensicherheit stelle ein hohes Risiko dar. Deshalb entschloss sich die EU-Kommission auch zu einer umfassenden Revision des EU-Datenschutzrechts.[32] In diesem Zusammenhang erwägt die EU-Kommission die Aufnahme des vom BVerfG geschaffenen Grundrechts der Vertraulichkeit und Integrität informationstechnischer Systeme, dessen Schutzbereich bei Massendatenbezug eröffnet ist, in das Gesamtkonzept des Datenschutzes der Europäischen Union.[33]

[28] Auf der Innenministerkonferenz vom 21.-22.6.2011 zeigte sich eine gewisse Tendenz zu Gunsten der Vorratsdatenspeicherung und die ebenfalls umstrittene Verlängerung der Anti-Terror-Gesetze; die Verlängerung wurde nachfolgend vom Bundestag im Wege einer Kompromisslösung beschlossen (vgl. im Einzelnen Presseinformation des BMI v. 29.6.2011, zu Schutzlücken: http://www.bmi.bund.de/SharedDocs/FAQs/DE/Themen/Sicherheit/SicherheitAllgemein/7.html?nn=2075656 (9.6.2012).

[29] So *Möstl*, ZRP 2011, 225 (227 ff.) mit eigenem Regelungsvorschlag mit kumulativem „Quick-Freeze"-Verfahren und Mindestspeicherung.

[30] ABl. EU Nr. L 105 v. 13. 4.2006, S. 54, eingehend *Gola/Klug*, NJW 2011, 2484.

[31] Zum Bericht *Möstl*, ZRP 2011, 225 (227).

[32] Mitteilung KOM 2010, 609; eingehend *Gola/Klug*, NJW 2011, 2484 (2490).

[33] Mitteilung KOM 2010, 609, S. 6.

2. Vertragsverletzungsverfahren

Die EU-Kommission hat die Bundesregierung bereits Mitte Juni 2011 gemäß Art. 258 AEUV zu einer Stellungnahme im Rahmen eines Vertragsverletzungsverfahren aufgefordert, da die Frist für die Umsetzung der Richtlinie 2006/24/EG bereits im April 2011 ablief. Die Bundesrepublik Deutschland weigert sich jedoch weiterhin, anlasslos Daten über sechs Monate zu speichern. Mit diesem Verhalten, so die EU-Kommission, behindere der Gesetzgeber die deutschen Ermittlungsbehörden bei der Aufklärung schwerer Verbrechen. Aus deutscher Sicht bleibt der Konflikt mit der Charta der Grundrechte und den Datenschutzrechten bestehen. Zudem wird teilweise bezweifelt, dass die Richtlinie 2006/24/EG den Anforderungen des europäischen Primärrechts genügt. Fraglich ist die binnenmarktrechtliche Kompetenz nach dem jetzigen Art. 114 AEUV sowie die Vereinbarkeit mit den europäischen Grundrechten.[34] Die Zweifel bezüglich der Vereinbarkeit mit der Grundrechtecharta der europäischen Union werden im Übrigen von der Justizministerin geteilt.[35]

Auch wenn diese Zweifel berechtigt sind, ändert dies jedoch nichts an der Umsetzungspflicht der Bundesrepublik, da sich Mitgliedstaaten nicht auf die Rechtswidrigkeit der umzusetzenden Richtlinie berufen können.[36] Seitens der EU wurde mit Rücksicht auf die bestehende Problematik bereits versichert, dass keine rückwirkenden Strafzahlungen verhängt werden. Ausschließlich ein Zwangsgeld könne erhoben werden. Nach der Entscheidung über das Vertragsverletzungsverfahren könnte Deutschland somit ohne weiteres zügig ein Gesetz entsprechend den europäischen Vorgaben verabschieden und der Schaden bliebe verhältnismäßig gering.

V. Stellungnahme

1. Aus Sicht der Strafverteidigung ist zunächst darauf hinzuweisen, dass den Verkehrsdaten eine erhebliche Aussagekraft im Hinblick auf ihren Verursacher zukommt. Auf die grundgesetzlich in besonderem Maße zu schützende Intimsphäre des Betroffenen lassen sich – auch mit den in Rede stehenden legislativen Änderungen – hinreichende inhaltliche Rückschlüsse ziehen. Adressaten, Daten, Uhrzeit und Ort von Telefongesprächen erlauben insbesondere nach längerer Beobachtung und in ihrer Kombination detaillierte Aussagen zu gesellschaftlichen oder politischen Zugehörigkeiten, persönlichen Vorlieben, Neigungen und Schwächen. Hierüber lassen sich aussagekräftige Persönlichkeits- und Bewegungsprofile erstellen. Soweit der Richter am Bundesverfassungsgericht *Schluckebier* in seinem Sondervotum darauf verweist, dass die Vorratsdatenspeicherung Ausfluss der staatlichen Schutzpflicht gegenüber den Bürgern sei, geeignete Maßnahmen zu ergreifen, um die Rechtsgutsverletzung zu verhindern oder sie aufzuklären, überzeugt dies nicht in Gänze. Vielmehr muss es die Aufgabe des Gesetzgebers sein, diesen – unbestreitbar bestehenden – Schutzpflichten nachzukommen, ohne dass die Grundrechte des Einzelnen mehr als zwingend notwendig tangiert werden. Die von *Schluckebier* insoweit vertretene Auffassung, dass die Speicherung der zu erhebenden Daten durch „nichtstaatliche" Stellen den Einschüchterungseffekt beim Bürger entfallen lasse,[37] kann nach diesseitiger Auffassung nicht gefolgt werden. Zum einen erfolgt die Erhebung und Speicherung der Daten im Auftrag des Staates, zum anderen haben die in der Vergangenheit in gehäuftem Maße auftretenden „Datenpannen" und „Datenskandale" gezeigt, dass die Sicherheit von Daten keinesfalls selbstverständlich ist. Folgt man zudem der polizeilichen Kriminalstatistik des Bundeskriminalamtes hat die sechsmonatige Protokollierung aller Internetverbindungen im Jahr 2009 weder von der Begehung von Straftaten abgeschreckt, noch den Anteil der aufgeklärten Straftaten erhöht. Die präventiven und repressiven Ziele der Vorratsdatenspeicherung wurden daher – zumindest bis jetzt – verfehlt. Ein ausgewogenes – grundrechtsschonendes – Verhältnis von Zweck und Mittel scheint insoweit fraglich. Geht man überdies davon aus, dass sich der überwiegende Teil von Straftaten auch ohne die Sicherung und Auswertung von Telekommunikations*verkehrsdaten* aufklären lässt,[38] besteht für eine weitergehende Regelung keine Notwendigkeit.

2. Zusammenfassend lässt sich festhalten, dass die Vorratsdatenspeicherung – ungeachtet in welcher Form – als grundrechtsrelevante Maßnahme einen sensiblen Umgang erfordert. Dem Datenschutz und der Datensicherheit muss daher in einer dem betroffenen Grundrecht angemessenen Weise Rechnung getragen werden. Angesichts der Ergebnisse der polizeilichen Kriminalstatistik wird man außerdem den Mehrwert einer solchen Ermittlungshandlung ständig beobachten und daraufhin die Gewichtung von Eingriffsgut und Schutzgut dauerhaft neu hinterfragen müssen. Ergibt sich dabei, dass die staatliche Schutzpflicht durch eine Datenerhebung und Speicherung als grundrechtsrelevante Maßnahme nicht verbessert werden kann, ist eine Rechtfertigung zur Durchführung der Maßnahmen ausgeschlossen. Es sind daher – über das Grundsatzurteil des Bundesverfassungsgerichts hinaus – konkrete praktische Vorgaben des Parlaments für die Ermittler zu fordern. Diese müssen konkret, nachvollziehbar, ergebnisorientiert und von geringstmöglicher Grundrechtsrelevanz sein. Anderenfalls schadet die „Vorratsdatenspeicherung" dem Rechtsstaat.

[34] Vgl. *Gitter/Schnabel*, MMR 2007, 411 (412 ff.); *Westphal*, EuR 2006, 706 (711 ff.).

[35] http://www.bmj.de/SharedDocs/Interviews/DE/Printmedien/20120611_NJW_VDS_auf_dem_Pruefstand.html (7.9.2012); hierzu s. auch *Derksen*, WD 11-3000-18/11.

[36] EuGH MMR 2010, 783; *Möstl*, ZRP 2011, 225 (227).

[37] *Schluckebier*, NJW 2010, 852.

[38] Vgl. Verband der deutschen Internetwirtschaft Eco, http://www.golem.de/1010/78537.html (6.6.2012).

Der „Grundsatz der Verfügbarkeit“ von Daten zwischen Staat und Unternehmen*

Von Wiss. Mitarbeiter **Dominik Brodowski**, LL.M. (UPenn), München

Der europastrafrechtliche Grundsatz der Verfügbarkeit von Daten betrachtet die Möglichkeiten der Mitgliedstaaten der Europäischen Union, auf Daten zuzugreifen, die von einem anderen Mitgliedstaat für hoheitliche Zwecke vorgehalten werden. Das gleiche Rechtsprinzip ist jedoch bereits auf nationaler Ebene, insbesondere im Verhältnis zwischen Staat und Unternehmen zu diskutieren: Inwieweit sind Daten, die Bürger an Unternehmen oder sonstige Dritte preisgegeben haben, für Strafverfolgungszwecke verfügbar? Eine Analyse der strafprozessualen Eingriffsgrundlagen und der zu beachtenden Ausnahmevorschriften – etwa für Berufsgeheimnisträger – zeigt, dass insoweit ein Grundsatz der Verfügbarkeit bereits weitestgehend verwirklicht ist. Aus der Hand gegebene Daten stehen nahezu schrankenlos für Strafverfolgungszwecke zur Verfügung.

The principle of availability enshrined in European Criminal Law means that databases operated by the authorities in one state should be freely accessible to the authorities of other member states. The same principle deserves to be discussed within each criminal justice system, in the relation to data stored by private entities: How freely is data stored by private entities available in criminal investigations? In Germany, data entrusted to third parties is in nearly all cases available to the authorities. Therefore, such a principle of availability has already fully been materialized in German criminal procedure.

I. Die Bedeutung von Datenbeständen für die Strafverfolgung

Der außerordentlich hohe Börsen- bzw. Marktwert von Unternehmen wie Facebook oder Google beruht auf den immensen Beständen an persönlichen Daten, die diese Unternehmen angesammelt haben. Dass diese Datenbestände aber nicht nur in wirtschaftlicher Hinsicht, sondern auch für die Strafverfolgung von Bedeutung sind, sei zunächst anhand dreier Fallbeispiele exemplifiziert.

> *Beispiel 1*: Auf Bitten der Staatsanwaltschaft Halle durchsuchten im Sommer 2006 deutsche Banken alle Zahlungen mit Kreditkarten darauf, ob Kunden einen bestimmten Betrag auf ein verdächtiges Konto in Thailand überwiesen hatten. Mit einer solchen Überweisung konnte nämlich auf kinderpornographische Schriften zugegriffen werden. Die Banken ermittelten 322 Personen; etliche wurden später wegen des Besitzes kinderpornographischer Schriften verurteilt.[1]

> *Beispiel 2*: Der Ermittlungsrichter am AG Mannheim ordnete in einem Ermittlungsverfahren wegen Untreue die Beschlagnahme aller E-Mails an, die noch in einem bestimmten Postfach bei einem Internetprovider lagen und die aus dem Zeitraum August 2008 bis Dezember 2009 stammten. Der kooperative Internetprovider stellte der Polizei nun einen umfassenden Gastzugang zur Verfügung. Die Polizei betrachtete alle Nachrichten – auch solche aus dem Jahr 2010 – und konnte dem Verdächtigen so einen völlig anders gelagerten Betrug nachweisen.[2]

> (Hypothetisches) *Beispiel 3*: In Berlin filmt eine Überwachungskamera eine Person dabei, wie sie ein Auto in Brand setzt. Auf Bitten der Polizei gleicht Facebook das Foto mit sämtlichen auf Facebook gespeicherten Fotos mit einer automatischen Gesichtserkennung ab und benennt den Täter.

All diesen Beispielen ist gemein, dass Unternehmen nicht allein über eigene Daten verfügen, sondern Daten verdächtiger, aber auch unbeteiligter Dritter heranziehen und den Strafverfolgungsbehörden aushändigen. Inwieweit ist ein solches Verhalten der Unternehmen geboten, inwieweit ist es verboten?

II. Die Prinzipien der Zweckbindung und der Verfügbarkeit von Daten

Bevor auf diese konkreten Beispiele und die jeweiligen Eingriffsgrundlagen eingegangen werden kann, gilt es, den Bogen zu spannen zur *Verfügbarkeit* von Daten für Strafverfolgungsbehörden. Dieser Begriff hat seine Wurzeln in der Europäisierung des Strafrechts: Dem Grundsatz der Verfügbarkeit von Daten zufolge sollen Daten, die in einem Mitgliedstaat der EU bereits vorrätig sind, ohne größere formelle oder materielle Hindernisse auch in anderen Mitgliedstaaten für andere polizeiliche und strafprozessuale Zwecke zur Verfügung stehen.[3] Das gilt etwa für Fingerabdruckdaten, die in Deutschland vom Bundeskriminalamt vorgehalten werden.

Der europastrafrechtliche Grundsatz der Verfügbarkeit betrachtet somit das Verhältnis zwischen mehreren *Staaten* und thematisiert primär Zugriffe auf Daten, die von *staatlicher Seite* erhoben und gespeichert werden. Bezüglich solcher staatlich vorgehaltenen Daten ist wegen des gegenläufigen Prinzips der Zweckbindung von Daten aber bereits bei inner-

---

* Das Manuskript beruht auf einem Vortrag des *Verf.* auf dem Symposium der deutschen und türkischen Landesgruppe der AIDP „Cybercrime: Ein deutsch-türkischer Rechtsdialog“ an der Bilgi Universität, Istanbul. Der Vortragsstil wurde beibehalten.

[1] Vgl. BVerfGK 15, 71 m. Anm. *Brodowski*, JR 2010, 546; *Schaefer*, NJW-Spezial 2009, 280; *Schnabel*, CR 2009, 384.

[2] Vgl. LG Mannheim, StV 2011, 352 m. Anm. *Albrecht*, jurisPR-ITR 19/2011 Anm. 5.

[3] Vgl. *Böse*, Der Grundsatz der Verfügbarkeit von Informationen in der strafrechtlichen Zusammenarbeit der Europäischen Union, 2007; *Meyer*, NStZ 2008, 188; *Papayannis*, ZEuS 2008, 219; *Zöller*, ZIS 2011, 64, sowie den Rahmenbeschluss 2006/960/JI des Rates v. 18.12.2006 über die Vereinfachung des Austauschs von Informationen und Erkenntnissen zwischen den Strafverfolgungsbehörden der Mitgliedstaaten der Europäischen Union, ABl. EU 2006 Nr. L 386, S. 89.

staatlichen Datenabfragen eine Vielzahl von Grenzen für Ermittlungsmaßnahmen zu beachten.[4]

In diesem auch verfassungsrechtlich überformten Spannungsfeld zwischen Verfügbarkeit und Zweckbindung staatlich erhobener Daten besteht viel Anlass zur Diskussion. Die zunehmende Verlagerung hoheitlichen Handelns auf Private – man denke allein daran, dass Post- und Telekommunikationsdienste noch vor wenigen Jahren hoheitlich organisiert waren – zwingt aber dazu, dieselbe Fragestellung auch für das Verhältnis zwischen Staaten und Unternehmen aufzuwerfen. Inwieweit ist eine Zweckbindung bei von Unternehmen erhobenen Daten zu beachten, inwieweit sind von Unternehmen erhobene Daten für die Strafverfolgungsbehörden verfügbar?[5]

III. Eingriffsgrundlagen

Nach deutschem und europäischem Verfassungsverständnis erfordern Zugriffe der Ermittlungsbehörden auf personenbezogene Daten eine gesetzliche Eingriffsgrundlage.[6] Die in Deutschland normierten Eingriffsgrundlagen seien im Folgenden daraufhin untersucht, ob innerstaatlich ein Grundsatz der Verfügbarkeit von Daten bereits verwirklicht ist.

1. Zeuge

Das klassische Beweismittel schlechthin – der Zeuge – scheidet dabei von vornherein aus: Er ist nämlich ein persönliches Beweismittel, der über seine persönliche Wahrnehmung bekunden soll.[7] Die allermeisten Daten, an welchen die Ermittlungsbehörden Interesse haben, werden von Mitarbeitern der Unternehmen jedoch nicht persönlich wahrgenommen, sondern nur automatisch von den Rechnern des Unternehmens verarbeitet. Zwar könnten Unternehmensangehörige die entsprechenden Informationen abfragen, und sich damit zu Zeugen „machen“, doch zu solchen eigenen Nachforschungen ist eine Privatperson oder ein Privatunternehmen nicht verpflichtet.[8]

2. Freiwillige Auskunft

Eine andere Frage ist allerdings, ob ein Zeuge oder ein Unternehmen eigene Nachforschungen tätigen darf – und ob die Staatsanwaltschaft darum bitten darf. Grundsätzlich ist ein solches kooperatives Zusammenwirken von Zeugen, Unternehmen und der Staatsanwaltschaft gestattet und sogar geboten – und in der Praxis auch oft zu verzeichnen. Die Grenze findet die Kooperation jedoch dann, wenn sie zur Kollusion wird, also zu nicht von der Rechtsordnung akzeptierten Nachteilen für Dritte führt.

a) Das ist zunächst dann der Fall, wenn sich die Zeugen oder die Mitarbeiter des Unternehmens *strafbar* machen würden: So dürfen sie etwa keine Auskunft geben über Telekommunikationsvorgänge, denn dann drohte ihnen eine Bestrafung nach § 206 Abs. 1 StGB.[9]

b) Aufgrund der Gesetzesbindung der Exekutive (Art. 20 Abs. 3 GG) ist es den Strafverfolgungsbehörden ebenfalls nicht gestattet, um *ordnungsrechtlich verbotenes* Verhalten zu bitten. Oftmals sind aber freiwillige Recherchen datenschutzrechtlich verboten. Maßstab hierfür ist § 28 Abs. 2 Nr. 2 lit. b BDSG, demzufolge die Datennutzung und -weitergabe zulässig ist, soweit dies zur Strafverfolgung erforderlich ist „und kein Grund zu der Annahme besteht, dass der Betroffene ein schutzwürdiges Interesse an dem Ausschluss der Übermittlung oder Nutzung hat“. Rechtsprechung und Literatur verstehen letzteres aber nicht als starre Ausschlussklausel, sondern nehmen eine Interessenabwägung zwischen dem Strafverfolgungsinteresse des Staates einerseits und dem Recht auf informationelle Selbstbestimmung des einzelnen andererseits vor.[10]

Bei dieser Abwägung sind erstens die „schutzwürdigen Interessen“ grundsätzlich weit auszulegen und erfassen daher auch „wirtschaftliche oder berufliche Nachteile“.[11] Zweitens sind die besonderen Wertungen des Grundrechts auf Vertrau-

[4] Exemplarisch seien herausgegriffen die Limitierung der Verwertbarkeit von Zufallsfunden (etwa gem. § 477 Abs. 2 S. 2 StPO), das Erfordernis einer Aussagegenehmigung gem. § 96 StPO, das Steuergeheimnis (§ 30 AO) sowie die Unzulässigkeit der Verwertung von Daten aus dem Autobahnmauterfassungssystem für strafprozessuale Zwecke (§§ 4, 7, 9 Bundesfernstraßenmautgesetz, s. zur insoweit identischen Vorläufervorschrift des Autobahnmautgesetzes LG Magdeburg, NJW 2006, 1073 m. Anm. *Fraenkel/Hammer*, DuD 2006, 497).

[5] Während beim europastrafrechtlichen Prinzip die *wechselseitige* Verfügbarkeit im Vordergrund steht, dominiert im Verhältnis zwischen Staaten und Unternehmen der *einseitige* Zugriff des Staates auf von Unternehmen gespeicherte Daten. Auf diese Konstellation soll sich daher auch die folgende Darstellung beschränken.

[6] Aus verfassungsrechtlicher Sicht vgl. BVerfGE 65, 1 (43); 67, 100 (143); 84, 239 (279); 103, 21 (33); 115, 320 (341); BVerfGK 15, 71 (76 f.), sowie aus europäischer Sicht vgl. nur Art. 8 Abs. 2 Charta der Grundrechte der Europäischen Union (GRC), ABl. EU 2010 Nr. C 83, S. 389. Zur Auffassung der Kommission, als gesetzliche Grundlage reiche die Zuständigkeit der Strafverfolgungsbehörden zur Strafverfolgung, s. jedoch unten bei und mit Fn. 36.

[7] S. nur *Senge*, in: Hannich (Hrsg.), Karlsruher Kommentar zur Strafprozessordnung, 6. Aufl. 2008, Vor § 48 Rn. 1; *Eisenberg*, Beweisrecht der StPO, 7. Aufl. 2011, Rn. 1000.

[8] Aus prozessualer Sicht s. *Eisenberg* (Fn. 7), Rn. 1199 f.; *Ignor/Bertheau*, in: Erb u.a. (Hrsg.), Löwe/Rosenberg, Die Strafprozeßordnung und das Gerichtsverfassungsgesetz, Bd. 2, 26. Aufl. 2008, § 69 Rn. 9 m.w.N.; *Krehl*, NStZ 1991, 416 f.; *Petri*, StV 2007, 266, aus materiell-rechtlicher Sicht s. nur *Lenckner/Bosch*, in: Schönke/Schröder, Strafgesetzbuch, Kommentar, 28. Aufl. 2010, § 161 Rn. 3 m.w.N.

[9] Mangels verbindlicher Anordnung besteht auch keine Rechtfertigung für ein solches Verhalten, ja es wäre sogar eine Umgehung der gesetzlich bestimmten, spezielleren Eingriffsgrundlagen der §§ 100a, 100b StPO.

[10] *Gola/Schomerus*, Bundesdatenschutzgesetz, Kommentar, 10. Aufl. 2010, § 28 Rn. 46 m.w.N.

[11] *Gola/Schomerus* (Fn. 10), § 28 Rn. 26.

lichkeit und Integrität informationstechnischer Systeme[12] zu beachten: In heutiger Zeit verlassen sich viele auf eine (vermeintlich?) sichere Datenspeicherung im Internet, etwa bei der Archivierung von E-Mails. Staatliche Akteure dürfen nun die Wertungen dieses Grundrechts nicht dadurch konterkarieren, dass sie die Preisgabe vertraulich abgespeicherter Informationen durch Dritte fördern. Drittens ist ein mehrpoliges Grundrechtsverhältnis zu berücksichtigen: Neben den Grundrechten des Beschuldigten und denjenigen des Unternehmens sind hier auch die Grundrechtspositionen aller anderen Kunden von Bedeutung. Denn auch deren Daten werden regelmäßig durchsucht, so etwa bei der Suche nach verdächtigen Überweisungen auf ein bestimmtes Konto. Geschieht dabei ein Fehler – und dies kann leicht geschehen –, so werden auch die Daten unbescholtener Kunden übermittelt.[13]

c) Was folgt daraus? Unternehmen ist es datenschutzrechtlich verwehrt, quasi in vorauseilendem Gehorsam freiwillig umfangreiche Hilfe zur Strafverfolgung zu leisten, wenn sie dabei auf umfassende und besonders schützenswerte Datenbestände zurückgreifen müssten oder wenn eine besondere Gefahr dafür besteht, dass diese Herausgabe einen unschuldigen Dritten belasten könnte. Stattdessen sollten Unternehmen ihre umfassende Bereitschaft zur Mitwirkung bekunden, jedoch erst dann Auskunft erteilen, wenn ein förmliches Auskunfts- bzw. Herausgabeverlangen vorliegt (s. näher unten 5.).

3. Telekommunikation

Einen Sonderfall stellen diejenigen Daten dar, die während einer laufenden Telekommunikation anfallen. Diese genießen besonderen Schutz jedenfalls bis zu demjenigen Zeitpunkt, in dem sie beim Empfänger ankommen und dieser die Chance hat, diese zu löschen.[14] Bis dahin sind Zugriffe auf die Inhalte der Telekommunikation[15] nur unter besonderen Voraussetzungen gestattet. So muss etwa der Verdacht einer Katalogtat (§ 100a Abs. 2 StPO) bestehen und die Tat muss „auch im Einzelfall schwer" wiegen. All dies ist aber keine Durchbrechung eines Prinzips der Verfügbarkeit, denn dieser Grundsatz bezieht sich nur auf ohnehin vorrätige, d.h. zuvor gespeicherte Daten. Eine Telekommunikationsüberwachung bezieht sich hingegen auf Daten, die noch übertragen werden und zu diesem Zeitpunkt daher gerade nicht oder nicht dauerhaft gespeichert vorliegen.

Werden aber Daten aus einer Telekommunikation anschließend dauerhaft abgespeichert – etwa in einem E-Mail-Archiv –, so ist ein Zugriff nach der Rechtsprechung des Bundesverfassungsgerichts nicht am engen Maßstab einer Telekommunikationsüberwachung zu messen, sondern bloß an einer Beschlagnahme.[16]

4. Rasterfahndung

Ein weiterer Sonderfall ist die Rasterfahndung, § 98a StPO. Dabei handelt es sich um die Suche nach potentiellen Tätern aufgrund bestimmter allgemeiner, tätertypischer Merkmale, wie etwa Alter, Herkunft, Beruf, Studiengang, Religionszugehörigkeit und Anzahl der Kinder.[17] Ein solches data mining gilt inzwischen als vielversprechendes Mittel nicht nur bei der Terrorismusbekämpfung: So gab und gibt es Bestrebungen der Europäischen Union, „verdächtige" Flugbewegungen[18] und Überweisungen[19] laufend zu überwachen. Ein solches Durchforsten von Daten ist aber mit erheblichen Grundrechtsgefährdungen verbunden: So handelt es sich dabei um die Erstellung eines umfassenden Persönlichkeitsprofils, was nach deutschem Verfassungsverständnis grundsätzlich unzulässig ist.[20] Bedeutsamer ist jedoch das erhebliche Risiko falsch-positiver Treffer, also dass bloß irgendwie auffällige Personen zu Unrecht in den Verdacht geraten, eine Straftat begangen zu haben. Das macht es notwendig, eine Rasterfahndung nur in engen Grenzen zuzulassen.

Die neuere Rechtsprechung des Bundesverfassungsgerichts konterkariert das aber: Eine Rasterfahndung soll dann nicht vorliegen, wenn bloß Daten eines Unternehmens abgefragt werden, oder wenn das Unternehmen die Suchabfrage selbst durchführt.[21] Demzufolge wäre es etwa keine Rasterfahndung, wenn eine inländische Bank befragt würde, welche deutschen Kunden in den vergangenen Jahren Überweisungen von mehr als 10.000 Euro in die Schweiz getätigt haben – um sodann Ermittlungsverfahren wegen Steuerhinterziehung ein-zuleiten.

5. Auskunftsverlangen

Unternehmen können schließlich dazu verpflichtet werden, diejenigen Festplatten bzw. Datenträger auszuhändigen, auf denen beweisrelevante Daten gespeichert sind (§ 95 Abs. 1 StPO). Zur Abwendung eines solchen weitgehenden Herausgabeverlangens hat sich in der Praxis durchgesetzt, dass das Unternehmen statt dessen Auskunft über diese Daten erteilt, also eine Kopie der beweisrelevanten Daten an die Strafverfolgungsbehörden übermittelt. Ein solches Auskunftsverlangen der Strafverfolgungsbehörden ist aber dennoch ein ho-

[12] Grundlegend BVerfGE 120, 274 m. Anm. u. Bespr. *Böckenförde*, JZ 2008, 925; *Hillgruber*, JZ 2008, 861; *Sachs/Krings*, JuS 2008, 481.
[13] Vgl. *Brodowski*, JR 2010, 546 (548 f.).
[14] BVerfGE 120, 274 (307 f.); 113, 166 (183 ff.).
[15] Verkehrsdaten – das sind Daten, aus denen sich ergibt, wer wann mit wem kommuniziert hat – sind zwar theoretisch etwas leichter zu erheben (§ 100g StPO). Praktisch ergibt sich jedoch das Problem, dass diese Daten derzeit höchstens eine Woche lang gespeichert werden, nachdem die deutsche Umsetzung der Vorratsdatenspeicherung von Telekommunikations-Verbindungsdaten für verfassungswidrig und nichtig erklärt wurde, BVerfGE 125, 260.
[16] BVerfGE 124, 43; zur Übertragung auf Datenspeicherung in der „Cloud" vgl. *Obenhaus*, NJW 2010, 651 (654).
[17] *Schäfer*, in: Erb u.a. (Fn. 8), § 98a Rn. 1; *Brodowski*, JR 2010, 546 (548).
[18] KOM (2011) 32 endg. v. 2.2.2011.
[19] KOM (2011) 429 endg. v. 13.7.2011.
[20] BVerfGE 65, 1 (53).
[21] BVerfGK 15, 71 (77 f.).

heitlicher Eingriff, also ein Zwangsmittel und keinesfalls mit einer Bitte um freiwillige Auskunft zu verwechseln.

Umstritten sind die Anforderungen an ein Auskunftsverlangen: Teile der Rechtsprechung und der Literatur begnügen sich mit einer Anordnung durch Staatsanwaltschaft oder Polizei, obwohl eine Beschlagnahme – die durch eine Herausgabe und Auskunft ja abgewendet wird – einem präventiven Richtervorbehalt unterliegt.[22] Das überzeugt nicht, denn es wird dem Zwangscharakter dieser Maßnahme nicht gerecht, bei der zudem auch mit Ordnungsgeld und ersatzweise Ordnungshaft gedroht werden kann. Zudem ist zu berücksichtigen, dass in diesen Fällen regelmäßig Drittinteressen betroffen sind. Aus diesen Gründen ist daher gemäß § 98 Abs. 1 StPO eine richterliche Anordnung zu fordern, die nur bei Gefahr im Verzug durch die Staatsanwaltschaft und deren Ermittlungspersonen ersetzt werden kann.[23]

6. Durchsuchung und Beschlagnahme

Zuletzt kommt noch eine Durchsuchung (§ 103 StPO)[24] und Beschlagnahme von Daten – bzw. der Datenträger, auf denen diese Daten gespeichert sind – in Betracht (§ 94 StPO). Allerdings ist es unverhältnismäßig, bei unbescholtenen Unternehmen sogleich eine Durchsuchung und Beschlagnahme anzuordnen – man denke etwa daran, was es bedeuten würde, die Rechenzentren einer Großbank zu beschlagnahmen, nur um die Verdächtigen im *Fallbeispiel 1* festzustellen. Vielmehr hat der Staat zunächst darauf zu vertrauen, dass sich Unternehmen rechtmäßig verhalten und ein richterlich angeordnetes Auskunftsverlangen befolgen.[25] Nur bei einer Weigerung oder bei Verdacht eines Zusammenwirkens mit dem Beschuldigten darf eine Durchsuchung und Beschlagnahme durchgeführt werden.[26]

IV. Ausnahmen und Gegenrechte

Wer Daten oder Informationen an Unternehmen preisgibt, muss daher im Ausgangspunkt stets damit rechnen, dass Strafverfolgungsbehörden auf diese ohne größeren Aufwand zugreifen können. Unternehmen sind – nach hier bestrittener Auffassung auch ohne richterlichen Beschluss – verpflichtet, Auskunft über bei ihnen gespeicherte Daten zu erteilen und diese Daten nach bestimmten Merkmalen zu durchsuchen. Wirken Unternehmen nicht freiwillig mit – was in der Praxis ausgesprochen selten geschieht –, so können sie mit Zwangsmitteln zur Herausgabe verpflichtet werden, oder aber die Datenträger können bei einer Durchsuchung beschlagnahmt werden.

Allerdings gilt es nun zu prüfen, welche Ausnahmen gelten, wann also von Unternehmen gespeicherte Daten ausnahmsweise nicht zu Strafverfolgungszwecken zur Verfügung stehen.

1. Berufsgeheimnisträger

Nach § 97 StPO dürfen Daten, die Rechtsanwälte, Wirtschaftsprüfer, Journalisten, Ärzte und Psychologen (Berufsgeheimnisträger) – bzw. deren Unternehmen – im Rahmen ihrer beruflichen Tätigkeit gespeichert haben, nur beschlagnahmt werden, wenn diese selbst im Verdacht stehen, eine Straftat begangen oder sich an einer Straftat beteiligt zu haben. Dieser Schutz entfällt aber dem Wortlaut des § 97 Abs. 2 S. 1 StPO zufolge, wenn die Daten nicht mehr „im Gewahrsam“ des Berufsgeheimnisträgers sind. Dabei ist auf die primäre Verfügungsberechtigung über die Daten abzustellen – und nicht auf die Datenträger, also Festplatten –, um den Schutzzweck der Norm zu verwirklichen: den Schutz des Vertrauensverhältnisses zu diesen Berufsgeheimnisträgern. Daher sind auch solche Daten geschützt, die bei externen Dienstleistern – etwa auf einer Internetfestplatte bzw. in der sogenannten „Cloud“ – abgespeichert sind.[27]

2. Datenspeicherung im Ausland

International tätige Unternehmen haben oft ihre Rechenzentren auf mehrere Standorte verteilt. Wenn sich nun die Anfrage deutscher Strafverfolgungsbehörden auf Daten bezieht, die – vielleicht zufälligerweise – im Ausland gespeichert sind, so zeigen sich gerade Großunternehmen meistens kooperativ, transferieren diese Daten ins Inland und händigen sie den Strafverfolgungsbehörden aus. Doch ist dies rechtmäßig?

Völkerrechtlich unzulässig ist es, wenn Strafverfolgungsbehörden Unternehmen dazu *verpflichten*, Auskunft auch über solche Daten im Ausland zu erteilen.[28] Das wird deutlich, wenn man die hypothetische Alternative betrachtet, wenn das Unternehmen die Auskunft verweigern würde: Dann müsste eine Beschlagnahme des Datenträgers *im Ausland* er-

[22] LG Bonn BKR 2003, 914; *Meyer-Goßner*, Strafprozessordnung, Kommentar, 55. Aufl. 2012, § 95 Rn. 2 m.w.N.; vgl. auch *Erb*, in: Erb u.a. (Fn. 8), § 161 Rn. 28a.

[23] So i.E. auch KG NStZ 1989, 192; *Ciolek-Krepold*, Durchsuchung und Beschlagnahme in Wirtschaftsstrafsachen, 2000, Rn. 200 ff.; *Eisenberg* (Fn. 7), Rn. 2373; *Nack*, in: Hannich (Fn. 7), § 95 Rn. 3; *Schäfer* (Fn. 17), § 95 Rn. 20 m.w.N.

[24] Da sich diese gegen einen Unverdächtigen richtet, ist sie nur unter einschränkenden Voraussetzungen (§ 103 StPO) zulässig, d.h. es müssen „Tatsachen vorliegen, aus denen zu schließen ist, daß die gesuchten“ Daten sich „in den zu durchsuchenden Räumen befinden“. Das aber schließt nur Durchsuchungen „ins Blaue hinein“ aus.

[25] *Schäfer* (Fn. 17), § 103 Rn. 8; *Meyer-Goßner* (Fn. 22), § 103 Rn. 1a m.w.N.

[26] Aus diesem Grund war es entgegen LG Darmstadt (Beschl. v. 7.8.2011 – 25 Gs 1000 AR 200594/11) rechtswidrig, dass auf Grundlage eines französischen Rechtshilfeersuchens Computersysteme der in Deutschland erstarkenden Piratenpartei beschlagnahmt wurden, weil man auf Daten zugreifen wollte, die dort von verdächtigen Dritten abgespeichert wurden. Stattdessen hätte ein Auskunftsverlangen ergehen müssen.

[27] *Nack* (Fn. 23), § 97 StPO Rn. 8.

[28] LG Hamburg StV 2009, 70 (71); *Meyer-Goßner* (Fn. 22), § 110 Rn. 7a; *Brodowski*, JR 2010, 402 (411); *Gaede*, StV 2009, 96 (101 f.); *Gercke*, StraFo 2009, 271 (272 f.); *Obenhaus*, NJW 2010, 651 (654); s. hierzu auch *Kudlich*, GA 2011, 193 (208).

folgen. Das aber darf aus völkerrechtlicher Sicht nur über den ausländischen Staat geschehen. Da ein Auskunftsverlangen eine Beschlagnahme nur ersetzt, aber gleichermaßen ein Zwangsmittel darstellt, kann für dieses nichts anderes gelten – auch nicht zwischen den Mitgliedstaaten der Europäischen Union.[29]

Dürfen Unternehmen aber freiwillig Auskunft erteilen über Daten, die im Ausland gespeichert sind? Das ist dann zulässig, wenn eine „rechtmäßige und freiwillige Zustimmung" der Person vorliegt, die „rechtmäßig befugt" ist, die Daten zu transferieren.[30] Abzustellen ist dabei erneut auf denjenigen, der primär verfügungsberechtigt über die Daten ist. Das ist bei Daten über Finanztransaktionen die Bank, aber etwa bei Internet-Festplatten oder einer Datenspeicherung in der „Cloud" der jeweilige Kunde. In letzterem Fall ist daher der justizförmige Weg zu wahren und ein Rechtshilfeersuchen zu stellen.

3. Verhältnismäßigkeit

Alle Eingriffe erfordern schließlich aus verfassungsrechtlicher Sicht, dass sie verhältnismäßig sind: Datenabfragen bei Unternehmen verfolgen ohne weiteres ein legitimes Ziel – die Strafverfolgung – und sind regelmäßig auch geeignet und erforderlich. Bei der Angemessenheit des Datenzugriffs ist aber in mehrerlei Hinsicht Vorsicht geboten:

Erstens ist zu hinterfragen, inwieweit auf die Vertraulichkeit der Kommunikation eingewirkt wird, selbst wenn sich der Zugriff nur auf archivierte Kommunikation bezieht – denn wer löscht heutzutage noch seine E-Mails? Exzessive staatliche Zugriffe auf Kommunikation führen nämlich beim Bürger zu einem generellen Gefühl des Überwacht-Seins. Das aber kann zur Gefahr übermäßig konformen, angepassten Verhaltens und auch zur reduzierten Teilhabe am freiheitlich-demokratischen Gemeinwesen führen.[31] Dies gilt es zu vermeiden, zumal ein freies und freiheitliches Internet ein notwendiger Ausgleich ist für die zunehmende Mobilität und Flexibilität von Personen: Wenn Personen sich nämlich nicht mehr in ihre Wohnungen zur geschützten Kommunikation mit nahen Angehörigen und Freunden zurückziehen können, so benötigen sie trotzdem einen Kommunikationspfad, in dem sie frei – und regelmäßig auch frei von staatlicher Überwachung – kommunizieren können. Das Internet bietet diese besondere Chance, und diese gilt es zu bewahren.

Zweitens ist das mehrpolige Grundrechtsverhältnis – auch zu mitbetroffenen Dritten – zu berücksichtigen. Das gilt umso mehr, je atypischer die Datenabfragen werden und je höher daher das Risiko unbeteiligter und unbescholtener Dritter wird, selbst in das Visier strafrechtlicher Ermittlungen zu geraten.[32] Im Sinne eines rechtsstaatlich-liberalen Strafrechtsverständnisses wiegen Strafverfolgungen gegen Unschuldige nämlich weitaus schwerer als die Nichtverfolgung von Tätern. Daher ist ein data mining, etwa bei Finanztransaktionen, bei Verbindungsdaten oder bei Flugdaten nur unter ganz besonders strikten Voraussetzungen und Verfahrenssicherungen für zulässig zu erachten.

Drittens dürfen solche Zugriffe nicht mit dem Hinweis darauf bagatellisiert werden, es handele sich nur um von Unternehmen und nicht von staatlicher Seite erfasste und gespeicherte Daten. Gefahren für die Privatsphäre gingen daher von diesen Unternehmen und gerade nicht von Seiten des Staates aus. Diese Argumentation ist nicht tragfähig: Zum einen führte sie dazu, dass staatliche Behörden (zu) exzessive Datenspeicherungen wenigstens duldeten, wenn nicht sogar implizit befürworteten, anstatt diesen entschlossen entgegenzutreten. Zum anderen ließe sie außer Acht, dass durch eine staatliche (Zweit-)Nutzung von Datenbeständen eine gänzlich andere, weitaus intensivere Grundrechtsgefährdung vorliegt.

V. Anwendung auf die drei Fallbeispiele

Was bedeutet all dies nun für die drei eingangs genannten Fallbeispiele?

Im *Fall 1* – der Suche nach Finanztransaktionen, die ein bestimmtes Konto zum Ziel hatten – akzeptierte das Bundesverfassungsgericht das Vorgehen; es verlangte nicht einmal einen präventiven Richtervorbehalt. Das Risiko, dass Unschuldige verfolgt werden können, bezeichnete es trotz der höchst ungewöhnlichen und daher risikobehafteten Datenabfrage als „unvermeidlich"[33]. Mit der hier vertretenen Auffassung überzeugt das nicht, denn die freiwillige Mitwirkung der Banken war datenschutzrechtlich unzulässig und durfte daher von der Staatsanwaltschaft auch nicht eingefordert werden. Stattdessen wäre zumindest ein richterliches Auskunftsersuchen notwendig gewesen.

Ebenfalls bedenklich ist der *Fall 2*: Dass sich die Polizei über die Begrenzungen des richterlichen Beschlusses hinwegsetzte, demzufolge nur auf E-Mails eines bestimmten Zeitraums zugegriffen werden sollte, und sichtlich gezielt nach Zufallsfunden suchte, begründet einen derart schwerwiegenden Verfahrensmangel, dass ein Beweisverwertungsverbot zu bejahen ist. Eine andere Auffassung vertritt freilich das zuständige Landgericht Mannheim.[34]

[29] Sowohl die Europäische Beweisanordnung (ABl. EU 2008 Nr. L 350 v. 29.12.2008, S. 72) als auch die geplante Europäische Ermittlungsanordnung (zuletzt Ratsdok. 18918/11) sehen keine unmittelbare Beweiserhebung eines Staates im Hoheitsgebiet eines anderen Staates vor, sondern nur eine erleichterte Zusammenarbeit beider Staaten. Allein bei Telekommunikationsüberwachungen, die grenzüberschreitend und ohne Mitwirkung des anderen Staates durchgeführt werden können, gestattet das europäische Beweiserhebungsrecht die unmittelbare Durchführung einer transnationalen Beweiserhebung, kombiniert allerdings mit einer Notifikationspflicht und der Möglichkeit des betroffenen anderen Staates, dieser zu widersprechen (Art. 20 Rechtshilfeübereinkommen-2000 [ABl. EU 2000 Nr. C 197 v. 12.7.2000, S. 3]; Art. 27d Europäische Ermittlungsanordnung-E).

[30] So die Formulierung des Art. 32 lit. b Übereinkommen des Europarats über Computerkriminalität v. 23.11.2001 (BGBl. II 2008, S. 1242) – SEV 185, der kodifiziertes Völkergewohnheitsrecht darstellen dürfte.

[31] Vgl. BVerfGE 65, 1 (43).

[32] *Brodowski*, JR 2010, 546 (547, 549).

[33] BVerfGK 15, 71 (82).

[34] LG Mannheim StV 2011, 352.

Im *Fall 3* – der Gesichtserkennung mittels Facebook – würde nur auf Daten eines einzelnen Unternehmens zugegriffen. Zudem scheint sich die Rechtspraxis bei einer freiwilligen Mitwirkung des Unternehmens über die Frage hinwegzusetzen, ob die maßgeblichen Daten zuvor im Ausland gespeichert waren. Daher wage ich die Prognose, dass die Rechtsprechung auch dieses Vorgehen als rechtmäßig erachten würde.

VI. Fazit

Daten, die Privatpersonen Unternehmen zur Speicherung oder Verarbeitung anvertraut haben, sind für die Strafverfolgungsbehörden ohne größere Schwierigkeiten verfügbar; ein Grundsatz der Verfügbarkeit ist in diesem Verhältnis umfassend verwirklicht. Dieses Ergebnis folgt angesichts der in Deutschland vorherrschenden Rechtsprechung: Die freiwillige Mitwirkung von Unternehmen erachtet sie in weiten Teilen als unproblematisch, selbst wenn das Unternehmen hierzu auf im Ausland gespeicherte Daten zugreift. Eine Rasterfahndung sieht sie nur dann für gegeben an, wenn Datenbestände *mehrerer* Unternehmen abgeglichen werden. Das Risiko der Strafverfolgung Unschuldiger wird als „unvermeidliche Gefahr“[35] heruntergespielt. Auch auf Verfahrenssicherungen – also auf einen präventiven Richtervorbehalt – verzichtet jedenfalls ein Teil der Rechtsprechung. An diesen Maßstäben würde auch der nunmehr von der Europäischen Kommission vorgelegte Vorschlag für eine Richtlinie über den Datenschutz in der Strafverfolgung[36] nichts ändern, denn dieser gestattet es den Strafverfolgungsbehörden generell, Daten zur Wahrnehmung ihrer gesetzlicher Aufgabe – also der Strafverfolgung – zu erheben und zu verarbeiten. Hingegen sind in diesem Entwurf keine über weiche Generalklauseln hinausgehenden nennenswerten Verfahrenssicherungen oder materiellen Einschränkungen vorgesehen.

All dies stimmt bedenklich: Es thematisiert nur unzureichend das mehrpolige Grundrechtsverhältnis, in dem auch die Grundrechtspositionen derjenigen zu berücksichtigen sind, die als unbescholtene Bürger von einer Strafverfolgungsmaßnahme mitbetroffen sind. Nicht zu unterschätzen sind ferner die aufgezeigten Kollateralschäden für das freiheitlich-demokratische Gemeinwesen. Schließlich ist auch grundsätzlich zu hinterfragen, ob es nur positiv ist, wenn der Staat auf nahezu sämtliche Datenbestände schrankenlos zugreifen kann. Es spricht nämlich vieles dafür, anerkannte Institute wie dasjenige der beleidigungsfreien Sphäre[37] auch normativ zu stärken und behutsam auf andere Vertrauensverhältnisse und Kommunikationsinhalte zu erstrecken.

Was ist angesichts der aufgezeigten Risiken einer zu weitgehenden Verfügbarkeit von Daten zu fordern? Erstens eine Zurückhaltung der Strafverfolgungsbehörden bei sämtlichen Maßnahmen – wie etwa bei data mining –, die mit einem hohen Risiko verbunden sind, dass Unschuldige ins Visier der Strafverfolger geraten. Zweitens ist der präventive Richtervorbehalt bei Auskunftsverlangen zu stärken. Drittens darf die Verhältnismäßigkeitsprüfung nicht zu einer bloßen Formsache verkommen, sondern muss von Polizei, Staatsanwaltschaft und (Ermittlungs-)Richtern ernst genommen werden. Viertens vertragen Demokratie und Freiheitlichkeit kein Ende der Privatsphäre – daher ist auf Datenbestände von Unternehmen von staatlicher Seite nur zurückhaltend zuzugreifen, um nicht mit schlechtem Beispiel voranzuschreiten. Vielmehr ist es staatliche Pflicht, die so oft unterschätzte Bedeutung der Privatheit von Daten zu unterstreichen.

[35] BVerfGK 15, 71 (82).

[36] Vorschlag für [eine] Richtlinie des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Aufdeckung, Untersuchung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr, KOM (2012) 10 endg. v. 25.1.2012.

[37] S. nur *Lenckner/Eisele*, in: Schönke/Schröder (Fn. 8), Vorbem. §§ 185 ff. Rn. 9 m.w.N.

Informationstechnologische Herausforderungen an das Strafprozessrecht*

Von RiOLG Prof. Dr. **Joachim Vogel**, München**

I. Das mir zugewiesene Thema „Informationstechnologische Herausforderungen an das Strafprozessrecht" ist so allgemein gefasst, dass ich über alles und nichts reden kann. Genau das möchte ich im Folgenden tun und mich folgenden übergreifenden Fragen stellen: Wie verändert die Informationstechnologie den Strafprozess? Welche rechtlichen Probleme ergeben sich hieraus und in welche Richtungen sind Lösungen zu suchen? Mit dem Mut zur gröblichen Vereinfachung[1] möchte ich hierzu drei Thesen aufstellen:

- Über kurz oder lang wird Strafrechtspflege zur „e-criminal justice" mit elektronischer Akten-, Prozess- und Beweisführung werden. Das zentrale rechtliche Problem ist der Datenschutz; die Lösungen sind bereits im geltenden Datenschutzrecht vorgezeichnet.
- Die Auswertung und Überwachung der „e-Sphäre" von Beschuldigten wird zu einer strafprozessualen Standardermittlungs- und -beweismaßnahme werden. Die zentralen rechtlichen Probleme sind die aller strafprozessualen Ermittlungs- und Beweismaßnahmen: Gesetzlichkeit, Verhältnismäßigkeit, Schutz des Kernbereichs der privaten Lebensgestaltung und Beachtung der strafprozessualen Garantien und Privilegien namentlich zugunsten des Beschuldigten und seines Verteidigers. Sie müssen mutatis mutandis in der „e-Sphäre" in gleicher, gleich wirksamer Weise gewährleistet werden wie außerhalb der „e-Sphäre".
- Auch die „e-Sphäre" von Nichtbeschuldigten und Unverdächtigen, im äußersten Fall der gesamten Bevölkerung, wird zunehmend in strafprozessuale Ermittlungen und Beweisführungen einbezogen werden, insbesondere indem Register eingerichtet und ausgewertet und Private zu bereichsspezifischer Datenerfassung und -speicherung betreffend andere Private verpflichtet werden, um diese Daten im Verdachtsfall durch Datenabgleich nach dem Rasterprinzip auswerten zu können (Vorratsdatenspeicherung). Zentrales rechtliches Problem ist die Wahrung des Grundrechts auf informationelle Selbstbestimmung (und weniger der rechtsstaatlichen Unschuldsvermutung). Es gebietet, dass die „e-Sphäre" von Nichtbeschuldigten und Unverdächtigen grundsätzlich nicht in strafprozessuale Ermittlungen und Beweisführungen einbezogen wird und Vorratsdatenspeicherungen grundsätzlich unterbleiben; zu möglichen Ausnahmen komme ich noch.

Diese Thesen bedürfen der Erläuterung und Begründung, die in diesem Kurzvortrag nur skizzen- und bruchstückartig möglich sind:

II. Es ist eine Binsenwahrheit, dass Informationstechnologie längst bei der Polizei, den Staatsanwaltschaften, Gerichten und nicht zuletzt der Verteidigung Einzug gehalten hat. Akten werden gescannt und mit Verwaltungs- und Suchprogrammen ausgewertet; es werden Textverarbeitungs-, Kalkulations- sowie Präsentationssoftware verwendet und Datenbanken sowie Netzinhalte genutzt; Kommunikation findet via E-Mail, Chats und dergleichen statt.

Diese faktischen Phänomene genügen allerdings nicht zur Begründung einer „e-criminal justice", die vielmehr erst dann entsteht, wenn es zudem einen expliziten juristischen Rahmen für elektronische Akten-, Prozess- und Beweisführung gibt. Ein solcher Rahmen ist im deutschen Strafprozessrecht bislang nicht vorhanden, wohl aber im Ordnungswidrigkeitenrecht: § 110a OWiG lässt es zu, formgebundene Verfahrensdokumente elektronisch zu erstellen und bei Behörden und Gerichten einzureichen, sofern sie mit einer qualifizierten elektronischen Signatur nach dem Signaturgesetz versehen und für die Bearbeitung durch die Behörde oder das Gericht geeignet sind; spiegelbildlich lässt § 110c OWiG die Erstellung elektronischer Dokumente durch Behörden und Gerichte zu. § 110b OWiG ermöglicht die elektronische Aktenführung, wobei § 110d OWiG u.a. die Akteneinsicht regelt. Und § 110e OWiG stellt elektronische Dokumente beweisrechtlich Urkunden oder anderen Schriftstücken gleich. Obwohl es sich um eine durchaus magere, rechtlich bis heute längst nicht in allen Bundesländern umgesetzte und vor allem faktisch keineswegs flächendeckend angewendete Regelung handelt, verdeutlicht sie die Bereiche und Sachfragen, die im Zuge der Schaffung einer „e-criminal justice" zu regeln sind:

Im Bereich der elektronischen Aktenführung sind erstens das „Ob" und zweitens das „Wie" ihrer Zulässigkeit zu regeln: Soll es Pflicht sein oder im Ermessen der Behörden und Gerichte stehen, elektronische Akten zu führen? Soll es möglich sein, neben einer elektronischen Akte eine Papierakte zu führen, und welche Aktenform soll führen? Wie geht man mit sächlichen – auch „papiernen" – Beweismitteln um? In welchem elektronischen Format mit welchen elektronischen Schnittstellen werden elektronische Akten geführt und wie werden sie aufgebaut bzw. handhabbar gemacht? Wie werden Authentizität und Integrität der elektronischen Akte geschützt und wie werden Vertraulichkeit und Zweckbindung gewährleistet? An dieser Stelle sind nicht nur technische, organisatorische und nicht zuletzt finanzielle Herausforderungen zu bewältigen, sondern es muss auch Überzeugungsarbeit im

---

* Vortrag im Rahmen der von der Deutschen und der Türkischen Landesgruppe der Association Internationale de Droit Pénal (AIDP), der Istanbul Bílgí University und der Istanbul Bar Association veranstalteten Tagung „Cybercrime: Ein deutsch-türkischer Strafrechtsdialog", Istanbul, 12.-15.10. 2011.

** Der *Verf.* ist Inhaber des Lehrstuhls für Strafrecht, Strafprozessrecht und Wirtschaftsstrafrecht der Ludwig-Maximilians-Universität München und im Nebenamt Richter am Oberlandesgericht München. Im folgenden Text ist die ursprüngliche Fassung des Kurzvortrages beibehalten und nur um wenige Nachweise ergänzt sowie stellenweise aktualisiert worden.

[1] Zu den Einzelheiten *Freiling/Brodowski*, Cyberkriminalität, Computerstrafrecht und die digitale Schattenwirtschaft, 2011, besonders S. 46 ff., 122 ff. zum „Computerstrafprozessrecht"; *Gercke/Brunst*, Praxishandbuch Internetstrafrecht, 2009, besonders Rn. 633 ff. zum Strafprozessrecht.

Kriminaljustizsystem geleistet werden,[2] wie sie am besten gelingt, wenn ein Einstieg mit Modellversuchen auf freiwilliger Grundlage unternommen wird, aus denen die Praxis lernen und von denen ausgehend Schritt für Schritt weiter gegangen werden kann.

Der weitere Bereich der elektronischen Prozessführung betrifft insbesondere die Zulässigkeit von elektronischen Prozesshandlungen, sei es solcher der Staatsanwaltschaften oder Gerichte wie beispielsweise bei elektronischer Anklageerhebung oder Urteilszustellung, sei es solcher der Beschuldigten, Verteidiger oder weiterer Verfahrensbeteiligter, beispielsweise bei elektronischer Antragstellung oder Rechtsmitteleinlegung. Wiederum sind „Ob" und „Wie" zu regeln, wobei die Einzelfragen denen zur elektronischen Aktenführung verwandt sind; namentlich stellen sich die Fragen des Nebeneinanders von elektronischen und herkömmlichen Prozesshandlungen sowie der Gewährleistung von Authentizität und Integrität beispielsweise durch elektronische Signatur. Praktisch bedeutsam ist weiterhin die Frage, ob Bürger oder Rechtsanwälte verpflichtet werden sollen, Vorsorge für den Zugang staatlicher elektronischer Prozesshandlungen – etwa durch Einrichtung neuer oder Freigabe bestehender elektronischer Postfächer – zu treffen.

Die elektronische Beweisführung schließlich betrifft einerseits die Nutzung von Informationstechnologie zur Erhebung traditioneller Beweise, beispielsweise bei audiovisuell übertragenen Zeugenvernehmungen, und andererseits „elektronische Beweise", seien es in elektronischer Form gespeicherte traditionelle Beweise wie z.B. audiovisuell aufgezeichnete Zeugenvernehmungen oder aus der „e-Sphäre" von Beschuldigten oder Dritten herrührende Beweise. Auch hier stellen sich Fragen des Verhältnisses von traditionellen und elektronischen Beweisen und solche der Authentizität und Integrität.

Ein bedeutsamer Schritt hin zur Einführung einer „e-criminal justice" im deutschen Strafverfahren ist der im Juni 2012 vorgelegte Diskussionsentwurf des Bundesministeriums der Justiz „Entwurf eines Gesetzes zur Einführung der elektronischen Akte in Strafsachen" (Stand 30.5.2012)[3]. Nach diesem Entwurf soll die elektronische Akte in Strafsachen bundesweit flächendeckend für Strafverfahren jedweder Art zwingend, d.h. unter Verbot der Papieraktenführung, und grundsätzlich zum 1.1.2017, je nach Bundesland spätestens zum 1.1.2020, eingeführt werden. Es handelt sich um eine – gerade auch im internationalen Vergleich – sehr ehrgeizige und weitgehende Initiative, die freilich bei den Bundesländern auf erheblichen Widerstand gestoßen ist, nicht zuletzt aus dem Grund, dass, würde der Entwurf Gesetz, die Länder sehr erhebliche Kosten für Hard- und Software sowie Administration tragen müssten.

Ungeachtet dieser fiskalischen Querelen zeichnet sich ab, dass Datenschutz eine zentrale juristische Problematik von „e-criminal justice" sein wird. Nicht wirklich von der Hand zu weisende Szenarien möglicher Manipulationen von elektronischen Akten oder derer illegaler, aber nicht mehr reversibler Publikation im Internet deuten auf wirkliche Probleme hin. Die Lösungen sind im Daten- und Datenverkehrsschutzrecht vorgezeichnet und bestehen in der rechtlichen, aber auch faktischen (technischen) Gewährleistung der Authentizität, Integrität, Vertraulichkeit und Zweckbindung elektronischer Akten nach tradierten daten- und datenverkehrsschutzrechtlichen Grundsätzen, wie sie sich im deutschen Recht aus dem BDSG, den LDSGen und dem Rechtsrahmen für digitale Signaturen ergeben.

III. Wer Informationstechnologie nutzt, hinterlässt elektronische Spuren, deren Inbegriff man als „e-Sphäre" eines Menschen bezeichnen kann: Jedes Telefonat, jede E-Mail, jeder Chat, jede Internetrecherche, aber auch jeder elektronische Zahlvorgang, jede Autofahrt mit Navigationsgerät oder jede Flugreise generieren elektronische Daten, deren (Gesamt-)Auswertung Kommunikations-, Mobilitäts- oder Interessenbilder zu zeichnen ermöglicht. Hinzu kommen soziale Netzwerke, in denen immer mehr Menschen immer persönlichere Daten kommunizieren oder publizieren, was Persönlichkeitsbilder zu erstellen ermöglicht.

Aus Sicht der Strafverfolgungsbehörden ist die Auswertung und Überwachung der „e-Sphäre" von Beschuldigten ein hochinteressantes, weil potenziell hoch ergiebiges Mittel der Aufklärung von Straftaten. In der Tat sind Ermittlungen in der „e-Sphäre" eines Beschuldigten längst zu Standardmaßnahmen geworden, und zwar nicht nur im Bereich der Cyberkriminalität, wo es gleichsam in der Natur der Sache liegt, sondern auch in „normalen" Kriminalitätsbereichen:

- So folgt etwa der Festnahme eines Betäubungsmittelstraftäters üblicherweise als erste Standardmaßnahme die Durchsuchung nach einem Mobiltelefon, dessen Beschlagnahme und Auswertung: Mit wem hat er/sie telefoniert oder SMS-Verkehr gehabt, welche Kontakte hat er/sie gespeichert, welche Kalendereinträge oder Notizen finden sich u.ä.?
- Oder in Wirtschaftsstrafsachen richtet sich die Durchsuchung des betreffenden Unternehmens längst nicht mehr nur auf Papierdokumente, sondern auch und vor allem auf

[2] Instruktiv hierzu BGH (Dienstgericht des Bundes), Urt. v. 21.10.2010 – RiZ (R) 5/09 = DRiZ 2011, 66 = MDR 2011, 140: kein Anspruch eines Richters auf Zurverfügungstellung von Papierausdrucken nach Einführung elektronischer Aktenführung; a.A. noch die Vorinstanz OLG Hamm (Dienstgerichtshof für Richter), Beschl. v. 20.10.2009 – 1 DGH 2/08.

[3] Im Internet abrufbar unter www.bmj.de/SharedDocs/Downloads/DE/pdfs/Diskussionsentwurf_Gesetz_zur_Einfuehrung_der_elektronischen_Akte_in_Strafsachen.pdf?__blob=publicationFile (14.9.2012). Die Vorarbeiten reichen mindestens bis ins Jahr 2007 zurück, als das Bundesministerium der Justiz die Große Strafrechtskommission des Deutschen Richterbundes mit einem Gutachten „Die elektronische Akte im Strafverfahren" beauftragte, das noch 2007 vorgelegt wurde, ebenfalls im Internet abrufbar unter www.bmj.de/SharedDocs/Downloads/DE/Fachuntersuchungen/elektronische_akte_im_strafverfahren.pdf?__blob=publicationFile (14.9.2012). Im Nachgang hierzu befasste sich eine Projektgruppe „Elektronische Akte in Strafsachen" des Bundesministeriums der Justiz mit der Problematik.

elektronische Informationssysteme aller Art und die in ihnen gespeicherten Daten, die sich nicht selten in Terabytes bemessen.
- Und in Staatsschutzsachen werden Terrorismusverdächtige zunehmend einer Rundum-Überwachung ihrer „e-Sphäre" unterzogen, indem namentlich der Telekommunikations-, Zahlungs- und Reiseverkehr insgesamt überwacht wird.[4]

Da alles das potenziellen oder aktuellen Straftätern nicht unbekannt ist, kommt es zu einer Art elektronischem Wettrüsten zwischen Strafverfolgungsbehörden und kriminellen Milieus: Diese verwenden zunehmend unkonventionelle elektronische Mittel, namentlich Verschlüsselungstechniken aller Art; jene bemühen sich dann, bereits an der „Quelle" der Eingabe noch unverschlüsselter Daten anzusetzen, sog. Quellen-Telekommunikationsüberwachung, die wiederum eine Infiltrierung des betreffenden informationstechnischen Systems mit einer Remote Forensic Software voraussetzt.

Die juristische Problematik von Ermittlungsmaßnahmen in der „e-Sphäre" ist im Prinzip keine andere als die aller Ermittlungsmaßnahmen: Da und soweit es sich um einen Eingriff in Grundrechte handelt, namentlich in das Recht auf informationelle Selbstbestimmung und das (Auffanggrund-) Recht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme, bedarf es einer verfassungsmäßigen Ermächtigungsgrundlage. Das bewährte verfassungsrechtliche Prüfraster umfasst die Prinzipien der Gesetzlichkeit, der Verhältnismäßigkeit und des Schutzes des Kernbereichs der privaten Lebensgestaltung sowie den Schutz der strafprozessualen Garantien und Privilegien.

Das strafprozessuale Gesetzlichkeitsprinzip gebietet, dass Ermittlungsmaßnahmen in der „e-Sphäre" auf eine hinreichend bestimmte, das Wesentliche regelnde gesetzliche Ermächtigungsgrundlage gestützt werden können. Dabei ist insbesondere zu bedenken, dass „alte" Ermächtigungsgrundlagen nicht ohne weiteres infolge technischen Fortschritts möglich gewordene „neue" Ermittlungsmaßnahmen tragen, die der historische Gesetzgeber nicht vor Augen hatte und haben konnte. So hat sich der *3. Strafsenat* des BGH[5] mit Recht geweigert, die „neue" sog. Online-Durchsuchung informationstechnischer Systeme nach Installation einer Remote Forensic Software, die den Strafverfolgungsbehörden Administratorenrechte gibt, unmittelbar oder entsprechend auf die „alten" Durchsuchungsvorschriften der StPO – auch nicht in Verbindung mit den Vorschriften über Telekommunikationsüberwachung – zu stützen. Dahinter steht die richtige Überlegung, dass es Sache der Rechtspolitik ist, durch Gesetz über Zulässigkeit und Reichweite dieser weitreichenden heimlichen Ermittlungsmaßnahme zu bestimmen. Diese Erwägung hätte auch mehr Gewicht in der Rechtsprechung verdient, wonach E-Mail-Beschlagnahmen im Prinzip auf die „alten" Vorschriften zur (Post-) Beschlagnahme in §§ 94 ff. StPO[6] oder Quellen-Telekommunikationsüberwachungen umstandslos auf § 100a StPO[7] gestützt werden können.

Das strafprozessuale Verhältnismäßigkeitsprinzip gebietet, auf nicht geeignete, nicht erforderliche oder nicht angemessene Ermittlungsmaßnahmen zu verzichten, was selbstverständlich auch in der „e-Sphäre" von Beschuldigten gilt. Für den Gesetzgeber folgt hieraus, dass er sich von der abstrakt-generellen Eignung, Erforderlichkeit und Angemessenheit einer elektronischen Ermittlungsmaßnahme wie z.B. der strafprozessualen Online-Durchsuchung im Rahmen seiner Einschätzungsprärogative überzeugen muss; der Wunsch von Ermittlungsbehörden nach bestimmten Ermittlungsmaßnahmen belegt noch nicht zureichend deren Verhältnismäßigkeit. Der Ermittlungsrichter muss die Verhältnismäßigkeit im konkret-individuellen Einzelfall feststellen; insbesondere bedarf es tragfähiger Grundlagen für die Feststellung, dass die Erforschung des Sachverhalts nur mit traditionellen Ermittlungsmaßnahmen aussichtslos oder wesentlich erschwert wäre.

Aus der Menschenwürdegarantie des Grundgesetzes (Art. 1 Abs. 1 GG) hat das BVerfG bekanntlich hergeleitet, dass der Kernbereich der privaten Lebensgestaltung auch und gerade durch elektronische Ermittlungsmaßnahmen nicht ausgeforscht werden darf.[8] In der Datenerhebungsphase muss sichergestellt werden, dass kernbereichsrelevante Daten nach Möglichkeit nicht erhoben werden und nicht zur Kenntnis staatlicher Stellen gelangen; in der Datenauswertungsphase müssen kernbereichsrelevante Daten unverzüglich gelöscht werden und eine Weitergabe oder sonstige Verwendung ist auszuschließen. Die praktische Umsetzung dieses verfassungskräftigen und z.B. in § 100a Abs. 4 StPO auch einfachgesetzlich verankerten Verbots stößt freilich weiterhin auf Schwierigkeiten.[9] Bislang nur formelhaft bewältigt ist auch das

[4] Hinzu können auf präventiv-polizeilicher Grundlage (z.B. § 20k BKAG) elektronische Informationssysteme wie Mobiltelefone oder Personalcomputer durch Remote Forensic Software infiltriert, überwacht und „on line" durchsucht werden, ohne dass der Verdächtige etwas bemerken würde.

[5] BGH, Beschl. v. 31.1.2007 – StB 18/06 = BGHSt 51, 211; ebenso bereits BGH (Ermittlungsrichter), Beschl. v. 25.11. 2006 – 1 BGs 184/06 = JR 2007, 77; a.A. noch BGH (Ermittlungsrichter), Beschl. v. 21.2.2006 – 3 BGs 31/06 = StV 2007, 60.

[6] Zutr. krit. *Freiling/Brodowski* (Fn. 1), S. 141 f. m.w.N.

[7] Zutr. krit. *Freiling/Brodowski* (Fn. 1), S. 143 f. m.w.N.

[8] Grundlegend BVerfG, Urt. v. 3.3.2004 – 1 BvR 2378/98, 1 BvR 1084/99 = BVerfGE 109, 279 (337 f.) – akustische Wohnraumüberwachung („großer Lauschangriff"); s. weiterhin Urt. v. 27.7.2005 – 1 BvR 668/04 = BVerfGE 113, 348 (392) – präventiv-polizeiliche Telekommunikationsüberwachung; Urt. v. 27.2.2008 – 1 BvR 370/07, 1 BvR 595/07 = BVerfGE 120, 274 (337 ff.) – Online-Durchsuchung; und nunmehr Beschl. v. 12.10.2011 – 2 BvR 236/08, 2 BvR 237/08, 2 BvR 422/08 = BVerfGE 129, 208 (209 ff.) – strafprozessuale Telekommunikationsüberwachung.

[9] S. hierzu Bundesbeauftragter für den Datenschutz und die Informationsfreiheit, Bericht gemäß § 26 Abs. 2 Bundesdatenschutzgesetz über Maßnahmen der Quellen-Telekommunikationsüberwachung bei Sicherheitsbehörden des Bundes v. 31.1.2012 – V-620/057#0146-VS-NfD, S. 12: Mitschnitt von Telefonsex und staatsanwaltschaftliche Anordnung der Nichtlöschung dieses Mitschnitts (!) im Rahmen einer Quellen-Telekommunikationsüberwachung.

Problem der sog. Rundum-Überwachung. Zwar entspricht es ständiger Rechtsprechung des BVerfG, dass eine Überwachung unzulässig ist, wenn sie sich über einen längeren Zeitraum erstreckt und derart umfassend ist, dass nahezu lückenlos alle Bewegungen und Lebensäußerungen des Betroffenen registriert werden und zur Grundlage für ein Persönlichkeitsprofil werden können;[10] in der Praxis ist aber – soweit ersichtlich – noch nie ein solcher Fall anerkannt worden.

Schließlich gilt es, den Schutz von strafprozessualen Garantien und Privilegien auch bei Ermittlungen in der „e-Sphäre" von Beschuldigten zu gewährleisten. Die Problematik stellt sich vor allem bei heimlichen elektronischen Überwachungsmaßnahmen wie der Telekommunikationsüberwachung (einschließlich Quellen-Telekommunikationsüberwachung) oder der akustischen Wohnraumüberwachung: Hier können staatliche Stellen ohne weiteres Kenntnis von selbstbelastenden Äußerungen des Verdächtigen bzw. Beschuldigten erlangen, aber auch von Kommunikationen mit Zeugnisverweigerungsberechtigten, beispielsweise Angehörigen oder Verteidigern. Allerdings gilt das Verbot des Zwanges zur Selbstbelastung (nemo tenetur se ipsum accusare) im Ausgangspunkt nur für Vernehmungen des Verdächtigen bzw. Beschuldigten durch Amtsträger und steht damit nicht a limine heimlichen elektronischen Überwachungsmaßnahmen entgegen. Doch rechtfertigt der Umgehungsgedanke durchaus die Erstreckung des Anwendungsbereichs des nemo tenetur-Grundsatzes auf de facto vernehmungsähnliche Konstellationen und auch überwachte Selbstgespräche können unter dem Gesichtspunkt des Kernbereichsschutzes unverwertbar sein.[11] Zumindest in der Freiheit des Gesetzgebers steht es, die Überwachung von Kommunikationen mit Zeugnisverweigerungsberechtigten aus dem zulässigen Anwendungsbereich elektronischer Überwachungsmaßnahmen auszunehmen oder deren Verwertbarkeit auszuschließen oder einzuschränken. Mit § 160a StPO hat der deutsche Gesetzgeber für Berufsgeheimnisträger eine abgestufte Regelung getroffen, die zwischen absolut geschützten Kommunikationen mit Geistlichen, Verteidigern oder Abgeordneten einerseits und nur relativ (nach Maßgabe einer Abwägung im Einzelfall) geschützten Kommunikationen mit anderen Berufsgeheimnisträgen, z.B. Ärzten oder Journalisten, andererseits unterscheidet, was vom BVerfG für verfassungsrechtlich möglich erachtet worden ist.[12]

IV. Im klassischen Strafprozess richten sich die Ermittlungen im Prinzip nur gegen Verdächtige bzw. Beschuldigte, und Nichtbeschuldigte bzw. Unverdächtige können zwar als Verletzte, Zeugen oder Sachverständige verfahrensbeteiligt sein, sind aber im Prinzip nicht von Ermittlungen betroffen.[13] Das hat sich mit der Informationstechnologie prinzipiell geändert: Mittlerweile hat die überwältigende Mehrheit der Bevölkerung eine „e-Sphäre" im oben beschriebenen Sinne und es sind gewaltige „Datenberge" entstanden, die für Strafverfolgungsbehörden von größtem Interesse sind, und zwar auch und gerade in den Fällen, in denen noch kein Straftatverdacht besteht oder in denen zwar ein Straftatverdacht besteht, der sich aber gegen Unbekannt richtet: Einerseits können im Wege des sog. data mining Telekommunikations-, Bewegungs- oder Zahlungsmuster ermittelt werden, die nach kriminalistischer Erfahrung als straftatverdächtig gelten müssen und dann Anlass zu weiteren, spezifischen Ermittlungen geben, beispielsweise wenn Medienberichten zufolge die CIA über das Abhörsystem Echelon abgehörte Telekommunikationen nach bestimmten Schlagwörtern und Mustern filtere, um etwa Terrorismusverdächtige zu identifizieren. Andererseits können bei von Unbekannt begangenen Straftaten durch Datenabgleich von Merkmalen, die über den oder die Verdächtigen bekannt sind, mit über die Bevölkerung oder einen Teil von ihr gespeicherten Merkmalen nach dem Rasterprinzip eine verdächtige Bevölkerungsgruppe herausgefiltert werden, beispielsweise wenn über einen ansonsten unbekannten Bankräuber bekannt ist, dass er in einem bestimmten Zeitraum in einem bestimmten Gebiet mit seinem Mobiltelefon telefoniert hat und sodann alle Personen ermittelt werden, die im fraglichen Zeitraum und Gebiet mit Mobiltelefonen telefoniert haben (sog. Funkzellenabfrage, § 100g Abs. 2 StPO).[14]

Weiterhin ist daran zu erinnern, dass Staaten typischerweise Daten über ihre Bevölkerung sammeln, die – auch wenn sie nicht in einem strafrechtlichen Zusammenhang oder zur Strafverfolgungsvorsorge erhoben worden sind – gegebenenfalls zu Strafverfolgungszwecken verwendet werden können. Ein instruktives Beispiel bietet § 24c KWG, wonach Kreditinstitute Dateien mit den Kontenstammdaten ihrer Kunden führen müssen, die von der Bundesanstalt für Finanzdienstleistungsaufsicht im automatisierten Verfahren abgerufen werden können, was zunehmend von Steuer- oder Sozialbehörden zur Aufdeckung von Steuer- oder Sozialbetrug genutzt wird. Aber auch Melde-, Kfz- und weitere Register können jedenfalls im Verdachtsfall so genutzt werden. Erst recht gilt dies für der Straftatverhütung und Strafverfolgungsvorsorge dienende Register wie solche, in denen biometrische Merkmale, Fingerabdrücke und DNA-Profile gespeichert sind, aber auch solche, in denen gefährliche Personen wie „Extremisten" oder „Hooligans" gespeichert sind. Im Verdachtsfall gehört der Datenabgleich mit solchen Registern mittlerweile zu den polizeilichen bzw. staatsanwaltschaftlichen Standardmaßnahmen.

Die juristische Problematik des data mining und des Abgleichs von über die Straftat bekannten Daten mit staatlichen oder privaten Dateien ergibt sich in erster Linie aus dem Grundrecht auf informationelle Selbstbestimmung, dessen Schutzbereich durch jede staatliche oder auch nur staatlich

[10] S. zuletzt BVerfG, Beschl. v. 7.12.2011 – 2 BvR 2500/09, 2 BvR 1857/10, Rn. 71 ff. (insoweit nicht in NJW 2012, 907).

[11] Aus neuerer Zeit BGH, Urt. v. 22.12.2011 – 2 StR 509/10 = BGHSt 57, 71.

[12] BVerfG, Beschl. v. 12.10.2011 – 2 BvR 236/08, 2 BvR 237/08, 2 BvR 422/08 = BVerfGE 129, 208 (243 ff.).

[13] Eine instruktive Ausnahme enthält § 103 StPO (Durchsuchung bei Unverdächtigen).

[14] Vgl. zur problematisch weitgehenden Praxis Berliner Beauftragter für Datenschutz und Informationsfreiheit, Abschlussbericht zur rechtlichen Überprüfung von Funkzellenabfragen v. 3.9.2012 – 51.1028.32.

veranlasste Datenerhebung, -speicherung und -verarbeitung betroffen ist. Es gewährleistet, dass Daten über die Bevölkerung oder bestimmte Bevölkerungsgruppen nur auf gesetzlicher Grundlagen, nur zu Gemeinwohlzwecken und nur nach den Grundsätzen der Datensparsamkeit und Verhältnismäßigkeit erhoben werden dürfen und nach dem Zweckbindungsgrundsatz grundsätzlich nur für die Zwecke verwendet werden dürfen, zu denen sie erhoben worden sind. Vor allem der Zweckbindungsgrundsatz setzt schrankenlosem data mining und Datenabgleich durchaus Grenzen.[15] Zudem dürften bereits die Grundsätze der Datensparsamkeit und Verhältnismäßigkeit verbieten, zu Zwecken der Strafverfolgungsvorsorge die gesamte Bevölkerung in biometrischen, Fingerabdruck- oder DNA-Registern zu erfassen, ohne dass auf die Menschenwürde oder andere „große Münzen" des Verfassungsrechts zurückgegriffen werden müsste. Allgemein gilt, dass die „e-Sphäre" von Nichtbeschuldigten und Unverdächtigen grundsätzlich nicht in strafprozessuale Ermittlungen und Beweisführungen einbezogen werden dürfen und Vorratsdatenspeicherungen grundsätzlich unterbleiben müssen.

Nicht oder jedenfalls nicht in erster Linie ergeben sich Grenzen für die Erfassung und Verwendung von Daten Unverdächtiger aus der strafprozessualen Unschuldsvermutung. Diese verbietet, jemanden als schuldig zu behandeln und ihn insbesondere einer Strafe oder vergleichbaren Rechtsfolge zu unterwerfen, bevor seine Schuld rechtsförmig erwiesen ist (vgl. Art. 6 Abs. 2 EMRK). Ermittlungsmaßnahmen setzt die Unschuldsvermutung allenfalls mittelbar Grenzen. Das gilt erst recht für ermittlungsvorbereitende Maßnahmen wie Erhebung und Verarbeitung personenbezogener Daten. Die häufig anzutreffende politische Aussage, durch die Vorratsdatenspeicherung werde die Bevölkerung unter einen Generalverdacht gestellt, der der rechtsstaatlichen Unschuldsvermutung zuwiderlaufe, ist daher juristisch kaum zutreffend.

Umgekehrt ist das nicht nur an Stammtischen gebrauchte politische Argument, die Erhebung, Speicherung und Verarbeitung personenbezogener Daten müssten den rechtstreuen Bürger nichts angehen, weil, wer nichts Strafbares tue, hiervon nichts zu befürchten habe, und dem, der strafbar gehandelt habe, geschehe es recht, wenn er ermittelt werde, juristisch unzutreffend, weil der Schutzbereich des Rechts auf informationelle Selbstbestimmung auch und gerade des rechtstreuen Bürgers betroffen ist. Eben hiervon hat die neuere Rechtsprechung freilich Ausnahmen gemacht, deren künftige Tragweite sich kaum abschätzen lässt:

In ihrem Nichtannahmebeschluss[16] hat die 2. Kammer des *Zweiten Senats* des BVerfG die sog. Aktion „Mikado" für verfassungsrechtlich unbedenklich erklärt. In dem zugrundeliegenden Verfahren war die Staatsanwaltschaft auf eine Internetseite aufmerksam geworden, die den Zugang zu kinderpornographischen Inhalten vermittelte, wofür 79,99 $ per Kreditkarte an eine philippinische Bank gezahlt werden mussten. Die Staatsanwaltschaft schrieb daher die Institute an, die Mastercard- und Visa-Kreditkarten in Deutschland ausgeben, und forderte sie auf, alle Kreditkartenkonten anzugeben, die eine solche Überweisung aufwiesen. Die Kreditkarteninstitute glichen Millionen Kreditkartenkonten mit den Daten ab und ermittelten 322 Karteninhaber, deren Daten an die Staatsanwaltschaft übermittelt wurden und bei denen sich später in der Tat kinderpornographische Inhalte fanden. Die Beschwerdeführer zählten zu den „no hits", die keine 79,99 $ überwiesen hatten. Nach Auffassung der Kammer wurden sie schon nicht in ihrem Recht auf informationelle Selbstbestimmung betroffen, weil ihre Daten nicht an staatliche Stellen weitergeleitet worden waren. Wenn das so ist, sind Datenabgleiche mit von Privaten geführten Dateien unbeschränkt und ohne spezifische gesetzliche Grundlage[17] möglich – ein problematisches Ergebnis.

Nicht derart weitgehend, aber doch in eine nicht unähnliche Richtung hat der *Erste Senat* des BVerfG zur Frage der Vorratsdatenspeicherung argumentiert.[18] Zwar liege in der gesetzlichen Anordnung gegenüber Kommunikationsunternehmen, Telekommunikationsverbindungsdaten zu erheben, zu speichern und an staatliche Stellen zu übermitteln, jeweils ein Eingriff in Art. 10 Abs. 1 GG. Jedoch unterfalle eine anlasslose Speicherung der Telekommunikationsverkehrsdaten der gesamten Bevölkerung für sechs Monate nicht schon als solche einem strikten verfassungsrechtlichen Verbot. Die Daten würden nur bei Privaten gespeichert und seien als solche staatlichen Stellen nicht zugänglich, sondern nur, wenn unter engen verfassungsrechtlichen Voraussetzungen ein Datenabruf und -abgleich erfolge. Auf Totalerfassung der Kommunikationen und Aktivitäten der Bürger sei die Vorratsdatenspeicherung nicht angelegt und Inhalte würden nicht gespeichert.

Es zeigt sich, dass es weniger staatliche als private Dateien sind, in Bezug auf die sich die Problematik der Ermittlung auch gegen Unverdächtige durch data mining und Datenabgleich drängend stellt – man denke nur an die neuere europäische Entwicklung im Bereich der von Flugreiseunternehmen geführten passenger name records (PNR).[19] Hier bedarf es

[15] Vgl. hierzu auch BVerfG, Beschl. v. 7.12.2011 – 2 BvR 2500/09, 2 BvR 1857/10, Rn. 130 ff., insb. 145.

[16] BVerfG, Beschl. v. 17.2.2009 – 2 BvR 1372/07, 2 BvR 1745/07 = NJW 2009, 1405.

[17] Die Kammer hat noch thematisiert, ob die Anfrage der Staatsanwaltschaft eine ausreichende gesetzliche Grundlage hatte, diese jedoch in der Ermittlungsgeneralklausel nach § 161 Abs. 1 StPO erblickt, BVerfG, Beschl. v. 17.2.2009 – 2 BvR 1372/07, 2 BvR 1745/07, Rn. 20 ff.

[18] BVerfG, Urt. v. 2.3.20120 – 1 BvR 256/08, 1 BvR 263/08, 1 BvR 586/08 = BVerfGE 125, 260.

[19] Vgl. (für transatlantische Flüge) Abkommen zwischen den Vereinigten Staaten von Amerika und der Europäischen Union über die Verwendung von Fluggastdatensätzen und deren Übermittlung an das United States Department of Homeland Security = ABl. EU 2012 Nr. L 215, S. 5; weiterhin (für innereuropäische Flüge) Europäische Kommission, Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates über die Verwendung von Fluggastdatensätzen zu Zwecken der Verhütung, Aufdeckung, Aufklärung und strafrechtlichen Verfolgung von terroristischen Straftaten und

auch von Seiten der Strafprozessrechtswissenschaft neuer Ansätze, die sich beispielsweise an der Verfassungsrechtsdogmatik der mittelbaren Drittwirkung von Grundrechten orientieren könnten.

schwerer Kriminalität = KOM (2011) 32 endg. (derzeit vor der 1. Lesung im Europäischen Parlament).