V&R Academic

Schriften des Zentrums für Europäische
und Internationale Strafrechtsstudien

Band 7

Herausgegeben von Arndt Sinn

Arndt Sinn (Hg.)

Cybercrime im Rechtsvergleich

Beiträge zum deutsch-japanisch-koreanischen Strafrechtssymposium 2013

V&R unipress

Universitätsverlag Osnabrück

UNIVERSITÄT OSNABRÜCK

MIX
Papier aus verantwortungsvollen Quellen
FSC® C083411

Bibliografische Information der Deutschen Nationalbibliothek

Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über http://dnb.d-nb.de abrufbar.

ISSN 2198-5367
ISBN 978-3-8471-0472-8
ISBN 978-3-8470-0472-1 (E-Book)
ISBN 978-3-7370-0472-5 (V&R eLibrary)

Weitere Ausgaben und Online-Angebote sind erhältlich unter: www.v-r.de

Veröffentlichungen des Universitätsverlags Osnabrück
erscheinen im Verlag V&R unipress GmbH.

Printed in Germany.
Druck und Bindung: CPI buchbuecher.de GmbH, Zum Alten Berg 24, 96158 Birkach

Gedruckt auf alterungsbeständigem Papier.

Inhalt

Vorwort

In den letzten Jahren gewinnt das Phänomen »Cybercrime« mehr und mehr an Bedeutung. Die Herausforderungen, die sich dabei für das Strafrecht ergeben, sind enorm. Nicht nur, dass die geltende Gesetzeslage nicht mit der rasanten technischen Entwicklung Schritt halten konnte, vielmehr reißen die gesetzgeberischen Nachbesserungen nicht selten Lücken in die tradierte Dogmatik und Systematik. Mögen dies »nur« nationale Probleme sein, so folgt das Phänomen »Cybercrime« aber keinen nationalen Grenzen oder Souveränitätsvorstellungen. Es entzieht sich aufgrund seiner Phänomenologie einer rein nationalen Bewältigung. Das Delikt, das im Zusammenhang mit Cybercrime steht, hat regelmäßig mehrere Anknüpfungspunkte, was die Jurisdiktion mehrerer Staaten begründen kann. Für den Täter eröffnen sich Möglichkeiten des forum shoppings, für die Strafverfolgungsorgane entsteht das Problem der Jurisdiktionskonflikte. Daten, die als Beweise benötigt werden, liegen nicht mehr nur in einem Staat, was schwierige Fragen der Rechtshilfe auslöst. Strafrechtliche und strafprozessuale Eingriffsermächtigungen erscheinen vor dem Hintergrund technischer Feinheiten in einem neuen Licht.

Mit dem 1. deutsch-japanisch-koreanischen Strafrechtssymposium am ZEIS der Universität Osnabrück haben Wissenschaftlerinnen und Wissenschaftler aus den beteiligten Ländern versucht, Antworten auf die drängenden rechtlichen Fragen in einem rechtsvergleichenden Symposium zu finden. Damit wird auch am ZEIS die langjährige deutsche Tradition der wissenschaftlichen Verbundenheit mit der Strafrechtswissenschaft in Japan und Korea fortgesetzt. Der Tagungsband enthält die Vorträge, wie sie am 2. bis 4. September 2013 in Osnabrück gehalten wurden. Die Beiträge geben wertvolle Einblicke in die gegenwärtige Diskussion zu Cybercrime in den Ländern. Rechtsvergleichende Beobachtungen sollen den vergleichenden Zugang erleichtern.

Ein solcher Tagungsband kann nicht ohne das unermüdliche Engagement der beteiligten Autoren entstehen, die sich alle der Mühe unterzogen haben, die Manuskripte auf Deutsch zu erstellen. Auch das unterstreicht die tiefe Ver-

bundenheit der japanischen und koreanischen Kollegen mit der deutschen Rechtsordnung, wofür ich allen herzlich danken möchte.

Mein Dank geht aber auch an das gesamte ZEIS-Team, namentlich an Frau cand. iur. Christina Brendel und Frau Ref. iur. Felicia Eissing sowie Frau cand. iur. Eileen Müller. Sie haben mit viel Fleiß, Umsicht, Ideen und Kraft das Symposium zu einer organisatorischen Meisterleistung werden lassen. Für die Betreuung des Tagungsbandes danke ich besonders Frau Christina Brendel, die sehr fürsorglich alle Beiträge gepflegt hat sowie Frau Wiss. Mit. Anna-Maria Graue, in deren Händen die gemeinsame Endredaktion lag.

Osnabrück im September 2015 Arndt Sinn

1. Teil:
Regelungen zu Cybercrime im materiellen Strafrecht

Susanne Beck

Regelungen zu Cybercrime im materiellen Strafrecht in Deutschland

A. Einleitung

»Die Internetkriminalität entwickelt sich […] immer mehr zu einer Bedrohung für die moderne Informationsgesellschaft. […] Damit die Internetkriminalität wirksam bekämpft werden kann, ist ein Bündel von rechtlichen, administrati-

ven, personellen, finanziellen und organisatorischen Maßnahmen nötig.«[1] Von diesem Bündel werden im Folgenden die Regelungen im materiellen Strafrecht in Deutschland näher betrachtet. Grundlage dieser Betrachtung ist gerade das Bewusstsein, dass das Strafrecht nur eine von verschiedenen möglichen Maßnahmen ist und deshalb z. B. nicht jede Lücke per se problematisch und – vgl. auch die entsprechenden Beiträge – vielleicht nicht jede Vorverlagerung nötig ist.

B. Betrachtung des Phänomens

»Der Begriff Cybercrime umfasst alle Straftaten, die unter Ausnutzung der Informations- und Kommunikationstechnik (IuK) oder gegen diese begangen werden.«[2] Diese Definition des Lageberichts des BKA ist sehr breit und ermöglicht eine umfassende Analyse des Phänomens. Bezüglich der empirischen Seite befasst sich der Lagebericht mit Cybercrime im engeren Sinne, also mit Ausprägungen dieser Art von Kriminalität, »bei denen Elemente der elektronischen Datenverarbeitung (EDV) wesentlich für die Tatausführung sind«[3]. Selbst nach der engen Definition erfasst Cybercrime ganz unterschiedliche Straftatbestände– vom Ausspähen von Daten über Computerbetrug bis hin zur Fälschung technischer Aufzeichnung. Zur Orientierung bei der Darstellung dieser disparaten Delikte ist hilfreich, sich ihren Hintergrund in Erinnerung zu rufen. Hierzu dienen zunächst folgende Definitionen des Internets– aus dem Internet – als Anhaltspunkt:

> »Das Internet ist der weltweit größte Netzverbund, der jedem Teilnehmer eine nahezu grenzenlose Informations- und Kommunikationsinfrastruktur zur Verfügung stellt.«[4]
> »Das Internet ist die Gesamtheit aller weltweit zusammengeschlossenen Computer-Netzwerke, die nach einem standardisierten Verfahren miteinander kommunizieren.«[5]

Zentraler Aspekt ist also die Kommunikation, das Senden und Empfangen von Informationen. Der Nutzer kommuniziert mit dem Computer, dadurch letztlich auch mit sich selbst, der Computer kommuniziert mittels seiner Datenverarbeitungsvorgänge ebenfalls mit sich selbst und dann, gegebenenfalls, über das

1 Bundesministerium des Inneren, http://www.bmi.bund.de/DE/Themen/Sicherheit/Kriminalitaetsbekaempfung/Internetkriminalitaet-Cybercrime/internetkriminalitaet-cybercrime_node.html.
2 BKA Lagebericht 2011, Vorbemerkung, S. 5.
3 BKA Lagebericht 2011, Vorbemerkung, S. 5.
4 http://www.itwissen.info/definition/lexikon/Internet-Internet.html.
5 http://www.internet4jurists.at/intern10a.htm.

Internet mit anderen Computern und somit der Nutzer mit anderen Nutzern.[6] Diese Art der Kommunikation unterscheidet sich von herkömmlicher Kommunikation primär durch das Medium – im Übrigen gibt es auch via Internet direkte Mitteilung von Informationen durch einen Sender an einen Empfänger – etwa über E-Mail oder einen Chat – und, vergleichbar mit klassischen Medien wie Büchern, Zeitungen oder Flugblättern, Mitteilungen an einen unbestimmten Empfängerkreis. Besondere Probleme entstehen vor allem durch den globalen Netzcharakter[7], d. h. das Fehlen einer organisierenden – und regulierenden – Institution, durch die dadurch mögliche Anonymität der Kommunikationsteilnehmer, die Dauerhaftigkeit der im Netz gespeicherten Informationen und schließlich durch die Möglichkeit des heimlichen Zugriffs auf private, sogar gesicherte Kommunikation.

Aus der »Kommunikations-Perspektive« lässt sich eine Ordnung in das Gebiet »Cybercrime« bringen: Das Strafrecht schützt unterschiedliche Aspekte dieser Kommunikation – und genau über diese Aspekte werden wir uns im Folgenden den Regelungen zur Cybercrime im materiellen Strafrecht in Deutschland annähern.

C. Europarechtlicher und verfassungsrechtlicher Rahmen

Bevor auf das materielle Strafrecht eingegangen wird, soll in Kürze der europarechtliche und verfassungsrechtliche Rahmen in Erinnerung gerufen werden. Auch wenn es hier nicht um Details zu höherrangigem Recht zur Cybercrime geht, ist bei Auslegung der nationalen Normen ein gewisses Bewusstsein für die betroffenen Interessen und supranationalen und verfassungsrechtlichen Grenzen erforderlich.[8]

6 Zu den verschiedenen Arten der Internet-Kommunikation und ihren zentralen Problemen vgl. etwa *K. Beck*, Computervermittelte Kommunikation im Internet, 2006.

7 Zu den damit verbundenen Regulierungsproblemen etwa *K. Beck*, Computervermittelte Kommunikation im Internet, 2006, S. 186 ff.

8 So an der Strafbarkeit von Glücksspielen, Sportwetten und Hausverlosungen dargestellt von *Heger*, Strafbarkeit von Glücksspielen, Sportwetten und Hausverlosungen via Internet im Lichte des Europarechts, ZIS 8.9.2012, S. 396 ff., der darauf hinweist, dass in diesem europarechtlich derzeit höchst umstrittenen Bereich innerhalb der Rechtsprechung keine Einigkeit bezüglich der Anwendung besteht, S. 401; weitere internationale Regelungen werden hier, da keine deutsche Besonderheit, ausgeklammert. Vgl. auch *Hilgendorf/Valerius*, Computer- und Internetstrafrecht, 2. Aufl. 2012, S. 28 ff.

I. Europarecht

Auch wenn von einem europäischen Strafrecht im engeren Sinne noch keine Rede sein kann, spielt die EU im Bereich der Cybercrime – das sich aufgrund der grenzüberschreitenden Natur des Internets nicht nur durch Nationalstaaten bekämpfen lässt – eine bedeutende Rolle.[9] Im Vordergrund steht das Bemühen um eine gewisse Harmonisierung der nationalen Rechtsordnungen und eine zur Bekämpfung der Kriminalität ausreichende Kooperation der Strafverfolgungsbehörden.[10] Bereits seit 1996[11] befassen sich Organe der EU mit den Gefahren der Computer- und Internetkriminalität.[12] Bei einigen Dokumenten und Rechtsakten war dieser Bereich am Rande von Bedeutung; beim Rahmenbeschluss 2005/222JI des Rates vom 24. 02. 2005 standen Angriffe auf Informationssysteme explizit im Vordergrund. Insbesondere sollte durch Angleichung der entsprechenden nationalen Strafvorschriften die Kooperation zwischen mitgliedsstaatlichen Behörden verbessert werden. Auf diesem Rahmenbeschluss basiert u. a. das 41. StrÄndG vom 07. August 2007.[13]

II. Verfassungsrecht

Das Verfassungsrecht ist hier in zweierlei Hinsicht zu beachten: Zum einen werden durch Strafnormen Grundrechte eingeschränkt, zum anderen dienen sie dem Schutz individueller und allgemeiner Güter.[14] Wie dargelegt, geht es im Cyberspace und bei der Nutzung von Computern primär um Kommunikation und dadurch gewonnene Informationen, so dass bezüglich der potentiell eingeschränkten Grundrechte Art. 5 Abs. 1 GG im Vordergrund steht. Bestimmte Kommunikationsinhalte können überdies über Art. 4 GG (Glaubens- und Gewissensfreiheit), Art. 5 Abs. 3 GG (Freiheit der Kunst und Wissenschaft), Art. 12 Abs. 1 GG (Berufsfreiheit) geschützt sein.[15] Schließlich sind durch den Einsatz von Strafrecht immer auch die allgemeine Handlungsfreiheit nach Art. 2 Abs. 1 GG (durch das Handlungsverbot) sowie zumindest potentiell das allgemeine

9 *Hilgendorf/Valerius,* Computer- und Internetstrafrecht, 2. Aufl. 2012, S. 30ff.
10 *Hilgendorf/Valerius*, Computer- und Internetstrafrecht, 2. Aufl. 2012, S. 31.
11 Mitteilung der Kommission über illegale und schädigende Inhalte im Internet vom 16. 10. 1996, KOM (1996) 487 endg.
12 *Hilgendorf/Valerius*, Computer- und Internetstrafrecht, 2. Aufl. 2012, S. 35ff.
13 Das unter anderem die Einführung von §§ 202a, 202b, 202c StGB und eine Änderung des § 303b StGB zur Folge hatte. Vgl. *Hilgendorf/Valerius*, Computer- und Internetstrafrecht, 2. Aufl. 2012, S. 36.
14 Zum Folgenden im Detail *Hilgendorf/Valerius*, Computer- und Internetstrafrecht, 2. Aufl. 2012, S. 2ff.
15 *Hilgendorf/Valerius*, Computer- und Internetstrafrecht, 2. Aufl. 2012, S. 3.

Persönlichkeitsrecht aus Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG (durch den staatlichen Vorwurf bei einer möglichen Sanktionierung) berührt.[16] Als gefährdete Güter stehen diesen Rechten z. B. das Fernmeldegeheimnis nach Art. 10 GG und das allgemeine Persönlichkeitsrecht aus Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG gegenüber. Durch Computerbetrug oder Erpressung wird das Eigentum (Art. 14 GG) gefährdet. Schließlich können, nach der weiten Definition von Cybercrime, grundsätzlich die unterschiedlichsten Delikte per Computer geplant, vorbereitet und ausgeführt werden, so dass insofern auch alle sonstigen individuellen und allgemeinen Interessen, die durch die jeweiligen Straftatbestände geschützt sind, verletzt werden können.

III. Überlegungen zu geschützten und eingeschränkten Aspekten der Kommunikation

Neben den für das deutsche Recht relevanten höherrangigen Normen seien an dieser Stelle kurz einige Erwägungen zum bereits erwähnten Aspekt der Kommunikation angestellt. Im Folgenden wird sich zeigen, dass die Strafnormen zur Cybercrime ganz bestimmte Aspekte des Sendens und Empfangens von Informationen schützen – etwa durch Sicherstellung der Möglichkeit mit oder mittels des Computers zu kommunizieren, durch Bewahren von Intim- und Privatsphäre, durch Sicherung gewisser Erwartungen an die Wahrhaftigkeit der Kommunikation. Bestimmte Aspekte der Kommunikation werden dagegen eingeschränkt, z. B. durch Exklusion nicht-zahlender Teilnehmer, durch Untersagen gewisser aufgezwungener Kommunikation, durch Verbote bestimmter Kommunikationsinhalte. Das gilt auch für Äußerungen, die im Rahmen sogenannter »Äußerungsdelikte« relevant sind, vgl. dazu später – selbst wenn diese nur an einen unbestimmten Adressatenkreis gerichtet sind und noch nicht einmal wahrgenommen wurden, handelt es sich doch um eine Art »Kommunikation«, da die Information zumindest öffentlich zur Verfügung gestellt wird und damit abrufbar ist – ein Selbstgespräch in einem Zimmer, in dem sich niemand anderes befindet, wäre für das Recht grundsätzlich nicht relevant, ebenso die bloße Kommunikation mit sich selbst mittels des eigenen Computers (mit Ausnahme der »Besitzdelikte«, vgl. auch hierzu im Folgenden). Hier entstehen im Vergleich zu traditionellen Gütern wie Leben, Leib oder Vermögen

16 *Lagodny*, Strafrecht vor den Schranken der Grundrechte, Tübingen, 1996, S. 77 ff., 96 ff. Überdies ist bei Prüfung von Strafnormen die verfassungsrechtliche Einbindung staatlicher Strafgewalt zu berücksichtigen: Schuldgrundsatz, Gesetzesbestimmtheit (Art. 103 Abs. 2 GG), Verbot erniedrigender, grausamer Strafen, spezielle institutionell-verfahrensrechtliche Garantien.

neue Interessen und Schutzsphären, nicht zuletzt, weil die erhebliche Bedeutung von Kommunikation und Information im Alltag selbst neu ist.[17]

Dass mit Blick auf diese neue Entwicklung auch im Strafrecht ein gewisser Anpassungsprozess erforderlich ist,[18] der die Schranken schutzwürdiger, erlaubter, einzuschränkender und verbotener Kommunikation auslotet, ist deshalb nicht verwunderlich. Hinzu kommt, dass an Kommunikation zwangsläufig mehrere Personen beteiligt sind, dass sie ein stetiger, dynamischer und in gewissem Sinn deutungsoffener Prozess ist – gerade im Internet, in dem oft nicht einmal direkt kommuniziert wird, sondern etwa bestimmte Informationen nur bereitgestellt sind, aber erst von Interessierten abgerufen werden müssen. Auch das ist für das Strafrecht schwer zu bewältigen, ist es doch primär an der Konstellation »Täter-Opfer« und »eindeutiger Verletzungshandlung« orientiert. Diese vorerst allgemeinen Überlegungen deuten bereits einige Schwierigkeiten an, die im Folgenden an Veränderungen im Allgemeinen und Besonderen Teil verdeutlicht werden.

D. Dogmatische Besonderheiten im Allgemeinen Teil

Der Allgemeine Teil des Strafrechts trifft u. a. Regelungen zur Anwendbarkeit deutschen Strafrechts, zum Umgang mit verschiedenen Handlungsformen und -stadien, subjektiven Aspekten und Verantwortlichkeitsanteilen. Die strafrechtliche Einhegung der grenzüberschreitenden virtuellen Kommunikation stößt bereits hier auf Schwierigkeiten, z. B. bei der Lokalisierung für die Frage der Strafrechtsanwendung, bei der Verteilung der Verantwortlichkeit für die Kommunikationsakte, bei der Ermittlung der Beteiligungsformen etc.

I. Strafanwendungsrecht

Nicht nur aufgrund der Grenzüberschreitung des Internets stellen sich spezifische Fragen des Strafanwendungsrechts, sondern auch aufgrund der schweren Lokalisierbarkeit von Kommunikationsprozessen, insbesondere wenn sie keine Rechtsgutsverletzungen, sondern nur Gefährdungen oder Vorbereitungen dar-

17 Vgl. hierzu etwa die Untersuchungen von *Castells*, The Rise of the Network-Society, 2. Aufl. 2009; *Steinbicker*, Zur Theorie der Informationsgesellschaft, 2. Aufl. 2011; *Thiedeke*, Medien, Kommunikation und Komplexität: Vorstudien zur Informationsgesellschaft, 1997. Grundlegend zur Medientheorie – unter anderem auch zur Auswirkung globaler Kommunikation auf regionale Kultur – *McMarshall*, Understanding Media. The Extensions of Man, 1964.

18 Vgl. hierzu etwa *Hilgendorf*, ZStW 113 (2001), S. 650ff.

stellen.[19] Nach §§ 3 ff. StGB ist deutsches Strafrecht grundsätzlich für Inlandstaten, für Auslandstaten dagegen nur in speziellen, explizit geregelten Situationen[20] anwendbar.

Bei der Verortung des Kommunikationsvorgangs wird zunächst an den Ort, von dem die Äußerung ausgeht, angeknüpft: Befindet sich der Tatcomputer in Deutschland, handelt es sich um eine Inlandstat.[21] Anders ist die Situation zu beurteilen, wenn Daten im Ausland eingegeben wurden – dann ist zu prüfen, ob auf andere Aspekte des Prozesses abgestellt werden kann. Einigkeit besteht darüber, dass die Orte, die die Information lediglich durchläuft, ohne wahrgenommen zu werden, keine Rolle spielen: auf Transitvorgänge ist in der Regel kein deutsches Strafrecht anzuwenden – es sei denn, gerade der Transit selbst würde bestraft.

Bei Kommunikationsdelikten ist oft schwer zu bestimmen, ob es sich um Erfolgs- oder Begehungsdelikte handelt, da in beiden Fällen der Inhalt der Kommunikation wahrgenommen wird – in einem Fall verletzt dies das Rechtsgut, im anderen wird es nur gefährdet. Liegt mit Wahrnehmung eine eindeutige Rechtsgutsverletzung oder konkrete Gefährdung vor – z. B. Beleidigungsdelikte, §§ 185 ff. StGB – ist nach § 9 Abs. 1 Var. 3 StGB davon auszugehen, dass die Tat überall dort begangen wurde, wo der Erfolg eingetreten ist.[22] Bei der weltweiten Kommunikation über das Internet ist das nicht nur am Aufenthaltsort des Opfers, sondern überall dort, wo z. B. die Beleidigung wahrgenommen werden kann, der Fall. Da das eine sehr weitgehende Strafrechtsanwendbarkeit begründet, wird als teleologische Reduktion von § 9 StGB diskutiert, einen territorialen Bezug oder Bezug zum Tatortrecht zu fordern.[23] Es geht dann also nicht mehr nur um die Möglichkeit der Wahrnehmung der kommunizierten Information, sondern auch um deren Inhalte.

Stellt die Äußerung nur eine abstrakte Gefährdungen dar, z. B. §§ 130, 184 ff. StGB, ist mangels Erfolgsort eigentlich nur das Strafrecht des Ortes, an dem die

19 Zu den Schwierigkeiten des »einseitigen« Strafanwendungsrechts aufgrund des entgrenzten Internets im Detail *Wörner*, Einseitiges Strafanwendungsrecht und entgrenztes Internet?, ZIS 8. 9. 2012, S. 458. Sie kommt zu dem Schluss, dass das Strafanwendungsrecht in diesem Bereich weniger auf einem rein staatlichen Souveränitätsgedanken als auf einem Solidaritätsgedanken gegenüber den eigenen Staatsbürgern und gegenüber den anderen Staaten basieren sollte (S. 464 f.).

20 Insofern gelten für Cybercrime keine Besonderheiten – auf Auslandstaten ist deutsches Strafrecht nach dem Schutzprinzip, dem aktiven oder passiven Personalitätsprinzip oder dem Weltrechtsprinzip anwendbar, §§ 5 ff. StGB.

21 *Hilgendorf/Valerius*, Computer- und Internetstrafrecht, 2. Aufl. 2012, S. 44.

22 Erfolg i.d.S. ist nicht jedes durch die Tat hervorgerufene Ereignis, sondern der tatbestandliche Erfolg. Allerdings muss es sich hierbei nicht zwingend um Tatbestandsmerkmale i. e. S. handeln; erfasst sind vielmehr »sämtliche im Gesetz beschriebenen Umstände, die den Unwertgehalt der Tat ausmachen«, *Ambos*, in: MüKo, StGB, Bd. 1, 2. Aufl. 2012, § 9 Rn. 21.

23 *Hilgendorf/Valerius*, Computer- und Internetstrafrecht, 2. Aufl. 2012, S. 51 f.

Kommunikation initiiert wurde, anwendbar.[24] Diese Einschränkung wird z. T. durch erweiternde Auslegung vermieden, indem entweder die Handlung am Ausgangs- und Zielrechner verortet wird, ein Tathandlungserfolg für jede Realisierung der Tathandlung oder ein Erfolg überall dort, wo sich die Gefahr verwirklichen könnte, bejaht wird. Insbesondere die erstgenannten Begründungen sind mit Blick auf die Prozesshaftigkeit von Kommunikation nicht unplausibel. Die h. M. lehnt die Ausweitung aber mit Hinweis auf Spezifika abstrakter Gefährdungsdelikte[25] und der sonst drohenden Allzuständigkeit deutscher Justizbehörden[26] ab.

Anders ist die Situation bei Delikten zu bewerten, bei denen Kommunikationsmittel und -wege oder bestimmte Kommunikationssphären (Intimsphäre, Privatsphäre) geschützt sind, z. B. die Verbote des Ausspähens und Abfangens von Daten, §§ 202a f. StGB oder der Datenveränderung und Computersabotage, §§ 303a f. StGB: Bei diesen wird das Rechtsgut nicht durch einen Kommunikationsakt verletzt, der Erfolgsort ist klarer bestimmbar: er ist dort, wo sich Daten bzw. Computer befinden bzw. in die Sphäre eingedrungen wird.

II. Der Begriff der »Schrift«

Bevor auf die Detailfragen des AT einzugehen ist, sei ein zentraler Begriff in kommunikativen Vorgängen geklärt: »Schrift«. Dieser aus traditionellen Kommunikationskontexten stammende Begriff wurde durch das IuKDG (1997) mittels Gleichstellungsklausel, § 11 Abs. 3 StGB,[27] an moderne Medien angepasst. Die hier vor allem relevanten Datenspeicher[28] sind dauerhafte, stoffliche Verkörperung von Daten (Speicherung). Die Inhalte der Schrift – also die Daten – müssen wahrnehmbar sein, da sonst gerade keine Kommunikation stattfindet. Dass hierfür Hilfsmittel (z. B. Bildschirm) erforderlich sind, ist unschädlich. Das Erfordernis der Verkörperung orientiert sich an klassischen Kommunikati-

24 Vgl. zu dieser Problematik *Ambos*, in: MüKo, StGB, Bd. 1, 2. Aufl. 2012, § 9 Rn. 27 ff.

25 Die abstrakte Gefahr ist nur Motiv des Gesetzgebers, nicht Tatbestandsmerkmal, vgl. *Hilgendorf/Valerius*, Computer- und Internetstrafrecht, 2. Aufl. 2012, S. 50.

26 Dies wäre nicht nur bezüglich des Legalitätsprinzips, sondern auch politisch häufig ausgesprochen problematisch, vgl. *Hilgendorf/Valerius*, Computer- und Internetstrafrecht, 2. Aufl. 2012, S. 51.

27 Dies dient u. a. der Vereinfachung von Gesetzesänderungen. *Hilgendorf/Valerius*, Computer- und Internetstrafrecht, 2. Aufl. 2012, S. 53.

28 Datenspeicher sind alle elektronischen, elektromagnetischen, optischen, chemischen oder sonstige Speichermedien, die gedankliche Inhalte verkörpern und nur unter Zuhilfenahme technischer Geräte wahrnehmbar sind. BT-Ducks. 13/7385, S. 36; *Eser/Hecker*, in: Schönke/Schröder, StGB, 28. Aufl.2010, § 11 Rn. 67; *Saliger*, in: Kindhäuser/Neumann/Paeffgen (Hrsg.), Nomos, StGB,4. Aufl. 2013, § 11 Rn. 60; *Hilgendorf/Valerius*, Computer- und Internetstrafrecht, 2. Aufl. 2012, S. 54.

onsmitteln, die sich durch tatsächliche Übertragung von Informationen auszeichnen und denen gerade aufgrund dieser Verkörperung besondere Bedeutung zukommt – sei es aufgrund ihrer besonderen Beweiskraft, ihrer größeren Gefährlichkeit aufgrund der Möglichkeit der Weiterverbreitung und der Reaktualisierung etc.

Bei Übertragung auf moderne Medien ergibt sich, dass für die nötige Dauerhaftigkeit der Verkörperung zwar grundsätzlich auch eine vorübergehende Speicherung (z. B. in Temporary Internet Files) ausreicht. Dass aber bereits der Arbeitsspeicher eine solche Verkörperung darstellt, kann jedenfalls aufgrund des automatischen Löschens der Daten mit Ausschalten des Computers bezweifelt werden.[29] Keine Schriften sind zweifellos, mangels dauerhafter Verkörperung, die Bildschirmanzeige selbst oder Live-Übertragungen aus dem Internet.[30] Sie entsprechen aufgrund ihrer Flüchtigkeit der direkten sensuellen Wahrnehmung.

III. Die Verantwortungsverteilung bei Kommunikationsakten

An einem Kommunikationsvorgang im Internet sind nicht selten mindestens fünf Personen beteiligt: Inhaltsanbieter, Network-Provider, Host-Provider, Access-Provider, Nutzer.[31] Fraglich ist, wie sich die strafrechtliche Verantwortlichkeit unter ihnen verteilt. Jedenfalls der die Informationen Kommunizierende ist für die Inhalte verantwortlich. Fraglich ist, wie derjenige, der die Informationen speichert oder weiterleitet, strafrechtlich verantwortlich ist. Anhaltspunkte hierfür liefert das TMG, das – für alle Rechtsgebiete – Provider-Verantwortlichkeiten begrenzt. Der Anbieter wird privilegiert, wenn sich seine Tätigkeit auf rein technische (Vermittlungs-)Vorgänge beschränkt. Angesichts dessen, dass er Kommunikation nur ermöglicht – und zwar meist unendlich viele Kommunikationen – ist das durchaus plausibel.

Wer nur Durchleitung von Informationen anbietet, ist also für Inhalte grundsätzlich nicht verantwortlich (Access- und Network-Provider, § 8 TMG). Ähnliches gilt für »Caching«, die kurzfristige Speicherung, die nur der Übermittlung im Kommunikationsnetz dient (§ 8 Abs. 2 TMG) bzw. die automatische, zeitlich begrenzte Zwischenspeicherung zur Erhöhung der Effizienz der Übermittlung fremder Informationen (§ 9 TMG): Wenn die Daten nicht verändert, bestimmte Bedingungen und Standards eingehalten und bei Kenntnis illegaler Inhalte diese sofort entfernt bzw. gesperrt werden, entfällt die Verant-

29 *Hilgendorf/Valerius*, Computer- und Internetstrafrecht, 2. Aufl. 2012, S. 54 f.
30 *Hilgendorf/Valerius*, Computer- und Internetstrafrecht, 2. Aufl. 2012, S. 55.
31 *Hilgendorf/Valerius*, Computer- und Internetstrafrecht, 2. Aufl. 2012, S. 56 f.

wortlichkeit. Wer fremde Informationen dagegen dauerhaft speichert, ist von der Verantwortung nur befreit, wenn er von rechtswidrigen Handlungen bzw. Inhalten keine Kenntnis hatte oder nach Kenntniserlangung unverzüglich entsprechend tätig wird (Host-Provider, § 10 TMG). Keine Privilegierung bezüglich der Verantwortlichkeit erfährt derjenige, der eigene Inhalte über das Netz verbreitet – wobei »eigene« auch »zu eigen gemachte« Inhalte einschließt, da auch diese von dem Handelnden nach außen kommuniziert werden.[32] Strittig ist, ob »zu eigen Machen« bereits vorliegt, wenn sich der Content-Provider vom Inhalt nicht distanziert,[33] oder ob vielmehr erforderlich ist, dass er die Auswahl, Kontrolle und Verantwortung übernimmt, oder ob die Situation danach zu beurteilen ist, ob für einen objektiven Dritten der Anschein erweckt wird, dass der Anbieter die Inhalte billige.[34]

Mit Blick auf die Bedeutung der Kommunikation bleibt hier insgesamt festzuhalten, dass der Handelnde umso eher rechtlich verantwortlich ist, je näher er der Information steht.[35]

Wo die Begrenzung der Verantwortlichkeit strafrechtsdogmatisch zu verorten ist, ist strittig: Zum Teil wird sie als Vorfilter vor der Strafbarkeitsprüfung, zum Teil als Tatbestandsmerkmal, zum Teil als Element der Schuld und zum Teil als Strafausschließungsgrund behandelt.[36] Mit Blick darauf, dass es um Sanktionierung von bestimmten Aspekten der Kommunikationsteilnahme geht, spricht vieles dafür, diese Begrenzung im Tatbestand zu verorten, stellt sie doch auf die tatsächlichen Umstände gerade dieser Teilnahme und wertungsmäßig auf die Nähe zum Kommunikationsakt bzw. dessen Inhalt ab.

Über diese Inhaltsverantwortlichkeit hinaus gilt bezüglich der Einordnung als »Täter« oder »Teilnehmer«, entsprechend der allgemeinen Grundsätze,[37] dass Täterschaft grundsätzlich mit »Herrschaft«, also Kontroll- und Handlungsmöglichkeit, über die Kommunikation bzw. Information einhergehen muss.[38] So

32 Vgl. *Hilgendorf/Valerius*, Computer- und Internetstrafrecht, 2. Aufl. 2012, S. 61 ff. Besonders problematisch ist diese Frage bei der Einstellung von Hyperlinks oder der Verwaltung von Gästebüchern o. ä. jedenfalls wenn der Anbieter die Beiträge freigeben muss, entsteht eine Verantwortlichkeit. Ein Disclaimer, dass für fremde Inhalte keine Haftung übernommen wird, reicht alleine nicht aus, um die Verantwortlichkeit zu verhindern.

33 *Koch*, Zivilrechtliche *Anbieterhaftung* für *Inhalte in Kommunikationsnetzen,* CR 1997, S. 193 ff., 197.

34 Vgl. zu dem Streit *Hilgendorf/Valerius*, Computer- und Internetstrafrecht, 2. Aufl. 2012, S. 62 f.; *Gercke/Brunst*, Praxishandbuch Internetstrafrecht, 2009, S. 245 ff.

35 *Hilgendorf/Valerius*, Computer- und Internetstrafrecht, 2. Aufl. 2012, S. 62 f.

36 *Hilgendorf/Valerius*, Computer- und Internetstrafrecht, 2. Aufl. 2012, S. 59 ff. (Tatbestandslösung).

37 *Hilgendorf/Valerius*, Computer- und Internetstrafrecht, 2. Aufl. 2012, S. 72.

38 Zur möglichen Strafbarkeit externer IT-Dienstleister als Gehilfen bei einer Tat nach § 203 Abs. 3 S. 2 StGB *Çekin*, Strafbarkeitsrisiken beim IT-Outsourcing – Zum externen IT-Dienstleister als Gehilfen im Sinne des § 203 Abs. 3 S. 2 StGB, ZIS 8. 9. 2012, S. 425 ff.

ist der Content-Provider in der Regel Täter, nicht jedoch beim bloßen Verlinken fremder Inhalte, da er über diese Inhalte gerade keine Herrschaft hat. Der bloße Zugangsvermittler wird in aller Regel als Gehilfe anzusehen sein, ebenso wie der untätige Host-Provider nach Kenntniserlangung über rechtswidrige Inhalte.

IV. Die Einordnung von Kommunikation als Tun und Unterlassen

Die Abgrenzung von Tun und Unterlassen[39] ist im Rahmen von (Internet-) Kommunikationen u. a. deshalb nicht einfach, weil man auch implizit aktiv kommunizieren kann. Für den Content-Provider gilt, dass das Anbieten eigener Informationen grundsätzlich aktives Tun ist. Bei »zu eigen gemachten« Inhalten hängt die Kategorisierung davon ab, ob man – vgl. oben – davon ausgeht, dass dies schon bei Nicht-Distanzierung vorliegt (Unterlassen) oder erst bei Auswahl, Kontrolle und Verantwortungsübernahme (aktives Tun). Für Anbringen von Hyperlinks z. B. ist es plausibel, danach zu unterscheiden, ob schon zum Zeitpunkt des Anbringens auf der entsprechenden Seite strafbare Inhalte gespeichert waren – in diesem Fall liegt aktives Tun vor – oder ob sich die Inhalte nachträglich änderten – in diesem Fall käme nur eine Strafbarkeit wegen Unterlassen entsprechender Kontrolle dieser Inhalte in Betracht, wenn insofern Garantenpflicht besteht.

Eine Garantenpflicht[40] für Kommunikationsinhalte oder auch ein bestimmtes Kommunikationsverhalten (Aufklärungspflichten) kann z. B. aus vertraglicher Verpflichtung, behördlicher oder gerichtlicher Anordnung entstehen. Sie ergibt sich jedenfalls nicht schon aus dem TMG, das Verantwortlichkeiten begrenzen, nicht begründen will, oder dem bloßen Bereitstellen der notwendigen Infrastruktur (Ingerenz) – das Internet als ein zusätzlicher Kommunikationsraum ist nicht per se eine strafrechtlich relevante Gefahr.

V. Fehleinschätzungen, Missverständnisse und Irrtümer

Wie angedeutet können im subjektiven Tatbestand spezifische Probleme auftreten. Gerade weil Aspekte der Verantwortlichkeit für Kommunikationen zu betrachten sind, verschwimmen die Unterschiede zwischen deskriptiven und normativen Tatbestandsmerkmalen. Stuft man die Verantwortlichkeit nach dem TMG als Tatbestandsmerkmal ein, ist zwischen den Umständen der Verantwortlichkeit (deskriptiv) und deren rechtlicher Einordnung als verantwort-

39 Zum Folgenden *Hilgendorf/Valerius*, Computer- und Internetstrafrecht, 2. Aufl. 2012, S. 70.
40 Zum Folgenden *Hilgendorf/Valerius*, Computer- und Internetstrafrecht, 2. Aufl. 2012, S. 71 f.

lichkeitsbegründend (normativ) zu differenzieren. Irrtümer über deskriptive Aspekte sind nach § 16 Abs. 1 StGB, über rechtliche Bewertungen nach § 17 StGB[41] zu behandeln.

Hinzu kommt, dass der Täter sich bei virtueller Kommunikation oft unerkannt und unbeobachtet fühlt. Aufgrund des Gefühls der Anonymität sowie der verbreiteten Ansicht, beim Internet handle es sich um einen eigenständigen virtuellen und damit rechtsfreien Raum, wird nicht selten der kriminelle Gehalt des eigenen Verhaltens falsch eingeschätzt.[42] Auch der dezentralisierte, grenzüberscheitende Charakter des Internets trägt hierzu bei. Bei diesbezüglichen Fehlvorstellungen ist mit Blick auf das Unrechtsbewusstsein des Täters zunächst zu prüfen, ob er erkannte, dass er ein Rechtsgut verletzt[43] und anschließend, ob ihm bewusst war, dass sein Handeln von einer bestimmten Rechtsordnung erfasst wird. Das Gefühl, in einem rechtsfreien Raum zu agieren, begründet jedenfalls nicht per se einen Irrtum. Auch das fehlende Bewusstsein der tatsächlichen und rechtlichen Wirkungen der Kommunikation hat nicht als solches rechtliche Konsequenzen.

Die strafrechtliche Erfassung einzelner Aspekte virtueller Kommunikation ist häufig komplex, so dass hier nicht selten Irrtümer auftreten können; insofern bestehen jedoch hohe Anforderungen an dessen Unvermeidbarkeit i. S.v. § 17 StGB – im Zweifel muss sich der Handelnde über die rechtliche Zulässigkeit seines Verhaltens erkundigen.[44] Anders dagegen ist mit dem fehlenden Bewusstsein, dass das Verhalten auch in den Geltungsbereich fremder Rechtsordnungen fallen könnte, umzugehen. Da der grenzüberschreitende Charakter des Internets für Laien oft nur schwer fassbar ist, ihnen der Raum, in dem ihre Kommunikation wirkt, also gar nicht bewusst ist, lässt sich insofern durchaus begründen, dass sich das sonst bestehende Regel-Ausnahme-Verhältnis bezüglich der Vermeidbarkeit des Verbotsirrtums umkehrt. In diesen Fällen ist also bei Fehlen gegenteiliger Hinweise davon auszugehen, dass ein derartiger Irrtum unvermeidbar war.[45]

41 Zum Unrechtsbewusstsein im Internet *Hilgendorf/Valerius*, Computer- und Internetstrafrecht, 2. Aufl. 2012, S. 75ff.

42 *Hilgendorf/Valerius*, Computer- und Internetstrafrecht, 2. Aufl. 2012, S. 75.

43 Wobei es nicht erforderlich ist, dass dem Täter bewusst ist, dass dieses Gut gerade strafrechtlich geschützt ist. *Hilgendorf/Valerius*, Computer- und Internetstrafrecht, 2. Aufl. 2012, S. 75f.

44 Der Bezug zu einer bestimmten Rechtsordnung kann sich anhand verschiedener Indizien nachweisen lassen, wie die inhaltliche Gestaltung der Website, die Sprache der »Metadatei«, die Auflistung von Kontaktpersonen eines bestimmten Landes, die Top-Level-Domain etc. *Hilgendorf/Valerius*, Computer- und Internetstrafrecht, 2. Aufl. 2012, S. 77.

45 *Hilgendorf/Valerius*, Computer- und Internetstrafrecht, 2. Aufl. 2012, S. 78.

E. Schutz und Einschränkung computergesteuerter und virtueller Kommunikation

Im Besonderen Teil des deutschen Strafrechts finden sich Tatbestände zu verschiedenen Aspekten der computergesteuerten und virtuellen Kommunikation. So gibt es Normen, die auf den Schutz der Kommunikationsmittel und -zugänge gerichtet sind. Andere Straftatbestände schützen bestimmte Kommunikationssphären. Der Bürger wird etwa davor bewahrt, ungewollt bestimmte Informationen oder Aspekte seiner Persönlichkeit zu kommunizieren, die – letztlich interne – Kommunikation mittels seines Computers und die private Kommunikationen mit Dritten wird geschützt, bestimmte unerwünschte Kommunikation wird verhindert. Das Strafrecht reguliert jedoch nicht nur die Bedingungen für und die Grenzen der computergesteuerten und virtuellen Kommunikation, es trifft überdies auch Vorgaben bezüglich des »korrekten« bzw. verwertbaren Inhalts – insbesondere bezüglich der Pflicht wahrheitsgemäßer Angaben – und untersagt das Senden bestimmter Inhalte grundsätzlich, z. B. das Verbot der Beleidigung, Pornographiedelikte etc.

I. Kommunikationsmittel und Kommunikationszugänge

Der reibungslose Ablauf von Datenverarbeitungs- und Kommunikationsvorgängen ist in der Informationsgesellschaft von geradezu essentieller Bedeutung, weshalb er zum Teil auch strafrechtlichen Schutz genießt.

1. Angriffe auf Hardware, §§ 303a f. StGB

Grundvoraussetzung dieser Kommunikation ist eine funktionsfähige Hardware. Diese wird durch §§ 303a f. StGB geschützt, die die Sachbeschädigungsdelikte um den Schutz bestimmter computerspezifischer Interessen ergänzen, insbesondere des Interesses des Verfügungsberechtigten an der Verwendbarkeit der Daten und des Interesses von Betreibern und Nutzern am störungsfreien Ablauf von Datenverarbeitung.

§ 303a StGB verbietet es, Daten – unabhängig von Inhalt, Wert, Geheimnischarakter oder besonderer Sicherung, solange das Verfügungsrecht einer anderen Person zusteht[46] – rechtswidrig[47] zu löschen[48], zu unterdrücken[49], un-

46 *Hilgendorf/Valerius*, Computer- und Internetstrafrecht, 2. Aufl. 2012, S. 176.

47 In diesem Fall handelt es sich nicht nur um einen Hinweis auf die Rechtswidrigkeit, sondern ein eigenständiges Tatbestandsmerkmal; der Täter muss eine fremde Rechtsposition einschränken, d. h. ein anderer muss an der Unversehrtheit der Daten ein unmittelbares In-

brauchbar zu machen[50] oder zu verändern[51]. Nachteilige Konsequenzen sind nicht erforderlich.[52] Nicht strafbar sind Beeinträchtigungen mit Bagatellcharakter, die sich ohne Weiteres beseitigen lassen.[53] Strafbar sind dagegen, vgl. der Verweis auf § 202c StGB durch Abs. 3, einige Vorbereitungshandlungen.

Prozesse der Datenverarbeitung – einschließlich des Umgangs mit und der Verwertung von Daten – sind durch § 303b StGB geschützt. Diese Prozesse müssen für den Betroffenen von wesentlicher Bedeutung sein, d. h. die Funktionsfähigkeit der jeweiligen Einrichtung muss von ihnen ganz oder überwiegend abhängen.[54] Verboten ist das erhebliche[55] Stören der Verarbeitung mittels einer der beschriebenen Handlungen: Durch Begehen einer Tat nach § 303a Abs. 1 StGB (Nr. 1 ist also eine Qualifikation zu dieser), etwa mittels eines Virus; durch Eingabe oder Übermittlung von Daten in der Absicht, einem anderen einen Nachteil[56] zuzufügen (Nr. 2), etwa durch Denial-of-Service-Attacken[57]; durch Beeinträchtigung der Datenverarbeitungsanlangen oder -träger (Nr. 3)[58]. Auch insofern sind Vorbereitungshandlungen strafbar, vgl. Abs. 5.

---

teresse besitzen, *Hilgendorf/Valerius*, Computer- und Internetstrafrecht, 2. Aufl. 2012, S. 179.

48 Vollständiges unwiederbringliches Unkenntlichmachen, entweder durch Zerstören des Datenträgers oder Löschen des Datums, *Hilgendorf/Valerius*, Computer- und Internetstrafrecht, 2. Aufl. 2012, S. 177.

49 Entziehung des Zugriffs des Verfügungsberechtigten auf das Datum bzw. den Datenträger, *Hilgendorf/Valerius*, Computer- und Internetstrafrecht, 2. Aufl. 2012, S. 177. Irrelevant ist, ob der Berechtigte tatsächlich gerade verfügen wollte. Dieses Tatbestandsmerkmal kann auch durch virtuelle Sit-ins oder andere Denial-of-Service Angriffe erfüllt werden.

50 Beeinträchtigung der Gebrauchsfähigkeit von Daten, so dass sie nicht mehr bestimmungsgemäß verwendet werden können, *Hilgendorf/Valerius*, Computer- und Internetstrafrecht, 2. Aufl. 2012, S. 178.

51 Beeinträchtigung des ursprünglichen Verwendungszwecks der Daten durch neuen Informationsgehalt, *Hilgendorf/Valerius*, Computer- und Internetstrafrecht, 2. Aufl. 2012, S. 178. Dies ist zu bejahen bei manipulativen Wiederaufladen von Telefonkarten, Freischalten eines Mobiltelefons durch Abschalten des SIM-Locks, Änderung der Standard-Internetverbindung durch Installation eines Dialers, Einschleusen von Viren und dadurch bedingte Einflussnahme auf Daten, nicht aber durch »Trojaner«.

52 *Hilgendorf/Valerius*, Computer- und Internetstrafrecht, 2. Aufl. 2012, S. 176.

53 *Hilgendorf/Valerius*, Computer- und Internetstrafrecht, 2. Aufl. 2012, S. 176.

54 *Hilgendorf/Valerius*, Computer- und Internetstrafrecht, 2. Aufl. 2012, S. 179 f.

55 Erheblich bezieht sich auf die Störung der Datenverarbeitung, nicht etwa des Betriebs oder Unternehmens, *Hilgendorf/Valerius*, Computer- und Internetstrafrecht, 2. Aufl. 2012, S. 180.

56 Nachteil ist jede Beeinträchtigung rechtmäßiger Interessen; für die Absicht genügt sicheres Wissen um dessen Eintritt, *Hilgendorf/Valerius*, Computer- und Internetstrafrecht, 2. Aufl. 2012, S. 181.

57 Zur Strafbarkeit der »Lufthansa-Blockade«, die den DDoS-Attacken in strafrechtlich relevanter Hinsicht ähnelt, vgl. *Hoffmanns*, Die »Lufthansa-Blockade« 2001 – eine (strafbare) Online-Demonstration?, ZIS 8. 9. 2012, S. 409 ff.

58 Dies gilt unabhängig von der Fremdheit, so dass es sich um keine Qualifikation zu § 303 StGB handelt. Vgl. zu Details der Handlungen *Hilgendorf/Valerius*, Computer- und Internetstrafrecht, 2. Aufl. 2012, S. 181.

2. Störung von Telekommunikationsanlagen, § 317 StGB

Virtuelle Kommunikation bedarf darüber hinaus entsprechender Anlagen. Aus diesem Grund ist die Verhinderung oder Gefährdung des Betriebs einer öffentlichen Zwecken dienenden[59] Telekommunikationsanlage (§ 3 Nr. 23 TKG) nach § 317 StGB strafbar. Die Zwecksetzung setzt nicht voraus, dass die Anlage dem freien Publikumsverkehr zugänglich ist – ob jedoch auch private Telefonanschlüsse darunter fallen, ist umstritten.[60] Die Verhinderung oder Gefährdung muss mittels der aufgeführten Tathandlungen erfolgen, wobei zwar eine unmittelbare, aber nicht zwingend körperliche Einwirkung auf die Anlage erforderlich ist. Somit können auch DDoS-Attacken ein Unbrauchbarmachen i. S. d. § 317 StGB darstellen.[61]

3. Erschleichen von Leistungen, § 265a StGB

Schließlich werden im Bereich der Telekommunikation bestimmte Leistungen nur gegen Entgelt angeboten – auch das sind in einer Marktwirtschaft Voraussetzungen für deren Funktionieren. Der diesbezügliche Schutz ergibt sich aus § 265a StGB, der das Erschleichen der Leistung eines Automaten oder eines öffentlichen Zwecken dienenden Telekommunikationsnetzes verbietet (Var. 1 und 2) und dadurch, wie auch § 263a StGB, Strafbarkeitslücken aufgrund neuer Interaktionsformen mit Maschinen schließen soll.

Automaten i. S.v. Var. 1 meint Leistungs-, nicht Warenautomaten[62], da die Norm auf das Erschleichen von körperlosen »Leistungen« abzielt,[63] also etwa Fernrohre an Aussichtspunkten, Schließfächer etc. Jedenfalls nicht per se ein Automat ist ein Computerprogramm; wird ein technisches Gerät, das durch Software betrieben wird, zum Tatobjekt, geht in der Regel § 263a StGB dem nur subsidiär eingreifenden § 265a StGB vor, Abs. 1 a.E. Die erschlichene Leistung muss entgeltlich sein, vgl. § 11 Abs. 1 Nr. 9 StGB, wobei zu prüfen ist, wofür das Entgelt entrichtet wird. Wenn das nicht für die Leistung des Automaten erfolgt, ist die Anwendung der Norm abzulehnen, z. B. bei Receivern zum Empfang digitaler Fernsehprogramme oder bei Umgehung der SIM-Lock-Sperre eines Mobiltelefons.[64] Ein Telekommunikationsnetz i. S. d. Var. 2 dient öffentlichen Zwecken, wenn es insgesamt zur Benutzung für die Allgemeinheit eingerichtet

59 Zu diesem Begriff vgl. E. II.
60 Vgl. hierzu *Hilgendorf/Valerius*, Computer- und Internetstrafrecht, 2. Aufl. 2012, S. 200 f.
61 *Hilgendorf/Valerius*, Computer- und Internetstrafrecht, 2. Aufl. 2012, S. 201.
62 Für diese bleibt es bei der Strafbarkeit nach § 242 StGB.
63 *Hilgendorf/Valerius*, Computer- und Internetstrafrecht, 2. Aufl. 2012, S. 192.
64 *Hilgendorf/Valerius*, Computer- und Internetstrafrecht, 2. Aufl. 2012, S. 193.

wurde.[65] Die Leistung des Netzes besteht in Aussendung, Übermittlung und Empfang von Nachrichten, wobei alle Datenübertragungssysteme erfasst werden. Auch bei dieser Variante muss der Dienst entgeltlich geleistet werden.[66]

Als Tathandlung erfordert § 265a StGB das »Erschleichen« der Leistung. Die bloße unbefugte oder vertragswidrige Inanspruchnahme reicht nicht, vielmehr müssen durch betrugsähnliches Verhalten Kontrollen und Sicherungen umgangen werden.[67] Bei ordnungsgemäßer Bedienung ist ein Erschleichen also abzulehnen. Erfasst sind dagegen die Verwendung von Telefonkartensimulatoren, der unbefugte Gebrauch eines Probezugangs zum Telekommunikationsnetz, wenn dabei eine Leistung des Betreibers in Anspruch genommen wird, sowie der Anschluss eines Fernsprechapparats an Schaltpunkten des Telekommunikationsnetzes.[68]

4. Abhörverbot, §§ 89, 148 TKG

Bezüglich der Einwahl in ein offenes W-LAN-Netz, um so Kosten für die Internetnutzung zu sparen, ist zu diskutieren, ob dies nach §§ 89, 148 TKG strafbar ist. So wird zum Teil vertreten, dass die Zuweisung der IP-Adresse durch den Router eine Nachricht i. S. d. Norm sei, die beim »Schwarz-Surfen« abgehört werde.[69]

II. Geschützte Sphären

Das Internet birgt in besonderem Maße die Gefahr von Eingriffen in den persönlichen Lebensbereich, sei es durch die Veröffentlichung von Audio-, Bild- oder Videodateien(also erzwungene Kommunikation nach außen), sei es durch belästigende oder verletzende virtuelle Kommunikation.[70] Diesbezüglich schützt das Strafrecht bestimmte Kommunikationssphären, etwa die Entscheidung darüber, bestimmte Informationen überhaupt zu kommunizieren oder darüber, mit wem man kommunizieren möchte. Da die Straftatbestände in

65 Es geht also nicht, wie in § 317 StGB, um den Zweck der konkreten Anlage, *Hilgendorf/Valerius*, Computer- und Internetstrafrecht, 2. Aufl. 2012, S. 193.

66 *Hilgendorf/Valerius*, Computer- und Internetstrafrecht, 2. Aufl. 2012, S. 193.

67 *Hilgendorf/Valerius*, Computer- und Internetstrafrecht, 2. Aufl. 2012, S. 194.

68 *Hilgendorf/Valerius*, Computer- und Internetstrafrecht, 2. Aufl. 2012, S. 195. Hingewiesen sei auf das Zugangskontrolldiensteschutz-Gesetz, das vor allem das Pay-TV, aber auch Video-on-Demand-Angebote und Computerspiele im Internet vor unbefugter Nutzung schützt.

69 Vgl. hierzu *Marberth-Kubicki*, Computer- und Internetstrafrecht, 2. Aufl. 2010, S. 153 f.; bejahend AG Wuppertal, 3. 4. 2007–22 Ds 70 Js 6906/06 (16/07); ablehnend LG Wuppertal, 19. 10. 2010–25 QS 10 Js 1977/08–177/10, 25 QS 177/10.

70 *Hilgendorf/Valerius*, Computer- und Internetstrafrecht, 2. Aufl. 2012, S. 125 f.

diesem Bereich also vor Beeinträchtigungen von individuellen kommunikativen Freiheiten und Persönlichkeitsrechten schützen, hängt die Strafbarkeit oft von der Zustimmung des Betroffenen ab. Auch wenn nicht alle dieser Strafnormen besondere Bestimmungen gerade für die computergesteuerte oder virtuelle Kommunikation treffen, wurden sie doch parallel zu der Entwicklung dieser Kommunikationsformen, zu der gewachsenen Angreifbarkeit der Kommunikationssphären und Bedeutung des Internets ausgeweitet.[71]

1. Recht am eigenen Wort und Bild, §§ 201 f. StGB

Das Recht am eigenen Wort und Bild ist eine besondere Ausprägung des allgemeinen Persönlichkeitsrechts (Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG), die entweder durch Auf- oder Wahrnehmen gegen den Willen des Betroffenen bzw. der Konservierung durch technische Mittel (also des Festhaltens einer Momentaufnahme der eigenen verbalen oder non-verbalen Kommunikation nach außen) oder durch Verbreitung ohne Zustimmung des Betroffenen[72] (und damit der ungewollten Kommunikation eigener Inhalte, Darstellungen, Seinsformen) verletzt werden kann.[73] Entsprechend sind die Strafnormen aufgeteilt: §§ 201 Abs. 1 Nr. 1 und Abs. 2 S. 1 Nr. 1, 201a Abs. 1 StGB schützen vor Auf- und Wahrnehmung bzw. Konservierung, §§ 202 Abs. 1 Nr. 2 und Abs. 2 S. 1 Nr. 2, 201a Abs. 2 und 3 StGB vor Gebrauchen und Zugänglichmachen.

Schutzobjekt des § 201 StGB ist das nichtöffentlich[74] gesprochene Wort, das vor Aufnahme[75] und Abhören[76] ebenso geschützt wird, wie vor Verbreitung[77]

71 *Hilgendorf/Valerius*, Computer- und Internetstrafrecht, 2. Aufl. 2012, S. 126.

72 Hatte dieser schon der Aufnahme nicht zugestimmt, wird die Verletzung perpetuiert und intensiviert; war die Aufnahme berechtigt, liegt in der unberechtigten Veröffentlichung eine eigenständige Rechtsverletzung; *Hilgendorf/Valerius*, Computer- und Internetstrafrecht, 2. Aufl. 2012, S. 127.

73 *Hilgendorf/Valerius*, Computer- und Internetstrafrecht, 2. Aufl. 2012, S. 127.

74 D.h. an einen durch persönliche oder sachliche Beziehungen miteinander verbundenen Personenkreis gerichtet, *Hilgendorf/Valerius*, Computer- und Internetstrafrecht, 2. Aufl. 2012, S. 127.

75 Jede Art der Konservierung, die die akustische Wiedergabe ermöglicht, *Hilgendorf/Valerius*, Computer- und Internetstrafrecht, 2. Aufl. 2012, S. 128.

76 Das unmittelbare Wahrnehmbar-Machen durch Verstärkung oder Übertragung mit einer technischen Vorrichtung über den normalen Klangbereich hinaus, *Hilgendorf/Valerius*, Computer- und Internetstrafrecht, 2. Aufl. 2012, S. 128. Nicht erfasst ist dagegen das einfache Belauschen.

77 Der Wortlaut »so hergestellte Aufnahme« in Abs. 1 Nr. 2 bezieht sich auf die Unbefugtheit der Herstellung – es sollen also gerade die Verwertungen erfasst werden, die eine bereits geschehene Verletzung des Persönlichkeitsrechts reaktivieren oder perpetuieren, *Hilgendorf/Valerius*, Computer- und Internetstrafrecht, 2. Aufl. 2012, S. 128.