Nadine Dombrowski

Extraterritoriale Strafrechtsanwendung im Internet

Schriftenreihe des Max-Planck-Instituts für
ausländisches und internationales Strafrecht

Strafrechtliche Forschungsberichte

Herausgegeben von Ulrich Sieber

in Fortführung der Reihe
„Beiträge und Materialien aus dem Max-Planck-Institut
für ausländisches und internationales Strafrecht Freiburg“
begründet von Albin Eser

Band S 142

Max-Planck-Institut für ausländisches
und internationales Strafrecht

Extraterritoriale Strafrechtsanwendung im Internet

Nadine Dombrowski

Duncker & Humblot · Berlin

Bibliografische Information der Deutschen Nationalbibliothek

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

Vertrieb in Gemeinschaft mit Duncker & Humblot GmbH, Berlin
http://www.duncker-humblot.de

Umschlagbild: © Victoria / fotolia.com
Foto der Autorin: PicturePeople GmbH & Co. KG, Neuss
Druck: Stückle Druck und Verlag, Stückle-Straße 1, 77955 Ettenheim
Printed in Germany
Gedruckt auf alterungsbeständigem (säurefreiem) Papier
entsprechend ISO 9706 ∴

ISSN 1860-0093
ISBN 978-3-86113-814-3 (Max-Planck-Institut)
ISBN 978-3-428-14541-6 (Duncker & Humblot)
DOI https://doi.org/10.30709/978-3-86113-814-3

Vorwort

Die im Frühjahr 2011 abgeschlossene Arbeit hat die Juristische Fakultät der Universität Potsdam als Dissertation angenommen. Im Wintersemester 2011/2012 erfolgte die Disputation. Für die Veröffentlichung wurde die Arbeit mit Blick auf Gesetzgebung, Rechtsprechung und Literatur Stand November 2013 aktualisiert.

Ich danke meinem Doktorvater, Herrn Prof. Dr. *Uwe Hellmann*, für seine tatkräftige Betreuung und Förderung. Ohne seine Unterstützung hätte die Arbeit nicht die vorliegende Qualität. Die Früchte seiner strengen Schule werden für mich ein Leben lang wertvoll bleiben. Herrn Prof. Dr. *Georg Küpper* gilt mein Dank für das zügige Erstellen des Zweitgutachtens und Frau Prof. Dr. *Dorothea Assmann* für die angenehme Prüfung während der Verteidigung.

Die Arbeit entstand im Wesentlichen während meiner Referententätigkeit am Max-Planck-Institut für ausländisches und internationales Strafrecht in Freiburg i.Br. Ich danke Herrn Prof. Dr. Dr. h.c. mult. *Ulrich Sieber*, Direktor am Institut und Leiter der strafrechtlichen Abteilung, für die mir gewährten Freiräume während meiner Tätigkeit, die wertvollen fachlichen Anregungen und die hervorragenden Arbeitsbedingungen am Institut. Ferner danke ich ihm für die Aufnahme meiner Dissertation in die Reihe „Strafrechtliche Forschungsberichte".

Ein großes Dankeschön verdienen zudem die vielen ehemaligen Kolleginnen und Kollegen am Max-Planck-Institut für ausländisches und internationales Strafrecht, insbesondere des Referats Informationsrecht und Rechtsinformatik, welche mich bei der Erstellung der Arbeit mit intensiven Diskussionen und zahlreichen Anregungen unterstützt haben. Allen voran möchte ich Herrn Rechtsanwalt *Frank Michael Höfinger* und Frau Dr. Dr. h.c. mult. *Karin Cornils* danken, welche die Arbeit in einem späten Stadium lasen und mit wertvollen Anstößen förderten. Gleichfalls bedanke ich mich bei Herrn Dr. *Phillip Brunst* und Frau Rechtsanwältin *Malaika Nolde*, LL.M. für die vielen hilfreichen Diskussionen.

Last but not least geht mein größter Dank an meinen Ehemann *Jan Dombrowski*, der mich zu jedem Zeitpunkt auf vielfältigste Weise unterstützt hat und ohne dessen Hilfe ich die Arbeit so nicht hätte fertigstellen können. Ebenfalls danken möchte ich meinen Eltern, insbesondere meiner Mutter *Angelika Gröseling*, die den Glauben an den erfolgreichen Abschluss nie verloren hat.

Neuss, im September 2014 *Nadine Dombrowski*

Inhaltsübersicht

Inhaltsverzeichnis

Dritter Teil

Territoriale Reichweite der Ermittlungsbefugnisse deutscher Strafverfolger

Abkürzungsverzeichnis

a.A.	anderer Ansicht
ABl. EG	Amtsblatt der Europäischen Gemeinschaften
ABl. EU	Amtsblatt der Europäischen Union
ABl. Bbg.	Amtsblatt des Landes Brandenburg
Abs.	Absatz
a.E.	am Ende
AEUV	Vertrag über die Arbeitsweise der Europäischen Union
a.F.	alte Fassung
AfP	Zeitschrift für Medien- und Kommunikationsrecht
AG	Amtsgericht
AIDP	Association Internationale de Droit Pénal
AJIL	The American Law Journal of International Law
a.l.i.c.	actio libera in causa
Alt.	Alternative
AOL	America Online
Art.	Artikel
AT	Allgemeiner Teil
Aufl.	Auflage
Az.	Aktenzeichen
BAnz.	Bundesanzeiger
BayObLG	Bayerisches Oberstes Landesgericht
BayObLGSt	Entscheidungen des Bayerischen Obersten Landesgerichts in Strafsachen
BB	Betriebs-Berater
Bd.	Band
BerDGesVölkR	Berichte der Deutschen Gesellschaft für Völkerrecht
BfV	Bundesamt für Verfassungsschutz
BGBl.	Bundesgesetzblatt
BGH	Bundesgerichtshof
BGHSt	Entscheidungen des Bundesgerichtshofes in Strafsachen

BKA	Bundeskriminalamt
BKAG	Bundeskriminalamtgesetz
BMI	Bundesministerium des Innern
BMJ	Bundesministerium der Justiz
BtMG	Gesetz über den Verkehr mit Betäubungsmitteln
BT-Drucks.	Drucksachen des deutschen Bundestages
BVerfG	Bundesverfassungsgericht
BVerfGE	Entscheidungen des Bundesverfassungsgerichts
BVerwG	Bundesverwaltungsgericht
BW	Baden-Württemberg
BYIL	The British Yearbook of International Law
bzw.	beziehungsweise
CCC	Convention on Cybercrime
CR	Computer und Recht
CRi	Computer Law Review International
dass.	dasselbe
DAV	Deutscher Anwaltsverein
DECIX	Deutscher Commercial Internet Exchange
ders.	derselbe
dies.	dieselbe/n
DDoS	Distributed Denial of Service
DoS	Denial of Service
DRiZ	Deutsche Richterzeitung
DStR	Deutsches Steuerrecht
DuD	Datenschutz und Datensicherheit
E	Entwurf
ECRL	E(lectronic)-Commerce-Richtlinie
EDV	Elektronische Datenverarbeitung
EG	Europäische Gemeinschaft(en)
EGBGB	Einführungsgesetz zum Bürgerlichen Gesetzbuch
EGMR	Europäischer Gerichtshof für Menschenrechte
EGStGB	Einführungsgesetz zum Strafgesetzbuch
EIGVG	Elektronischer-Geschäftsverkehr-Vereinheitlichungsgesetz

E-Mail	Electronic-Mail
EMRK	Konvention zum Schutze der Menschenrechte und Grundfreiheiten
endg.	endgültig
Ergl.	Ergänzungslieferung
ETS	European Treaty Series
EU	Europäische Union
EuGH	Europäischer Gerichtshof
EuRhÜbk	Europäisches Übereinkommen über die Rechtshilfe in Strafsachen
EU-RhÜbk	Übereinkommen über die Rechtshilfe in Strafsachen zwischen den Mitgliedstaaten der Europäischen Union
EUV	Vertrag über die Europäische Union
EuZW	Europäische Zeitschrift für Wirtschaftsrecht
EWG	Vertrag zur Gründung der Europäischen Wirtschafts-gemeinschaft
f.	folgende
ff.	folgenden
FBI	Federal Bureau of Investigation
Fn.	Fußnote
FS	Festschrift
G 10	Gesetz zur Beschränkung des Brief-, Post- und Fernmelde-geheimnisses (Artikel 10-Gesetz)
GA	Goltdammer's Archiv für Strafrecht
GBl. BW	Gesetzblatt für das Land Baden-Württemberg
gem.	gemäß
GG	Grundgesetz
ggf.	gegebenenfalls
GIZ	Gemeinsames Internetzentrum
GRURInt	Zeitschrift der Deutschen Vereinigung für gewerblichen Rechtsschutz und Urheberrecht Internationaler Teil
GVBl. Bbg.	Gesetz- und Verordnungsblatt für das Land Brandenburg
h.M.	herrschende Meinung
HRRS	Höchstrichterliche Rechtsprechung Strafrecht
Hrsg.	Herausgeber

HS	Halbsatz
HTML	HyperText Markup Language
HTTP	HyperText Transfer Protocol
ICANN	Internet Corporation for Assigned Names and Numbers
ICJ Rep.	International Court of Justice, Reports of Judgments, Advisory Opinions and Orders
i.d.R.	in der Regel
IFV	Internationaler Fernmeldevertrag
IGH	Internationaler Gerichtshof
IJCLP	International Journal of Communications Law and Policy
ILC	International Law Commission
IP	Internet Protocol
IPRax	Praxis des Internationalen Privat- und Verfahrensrechts
IRG	Gesetz über die internationale Rechtshilfe in Strafsachen
i.S.d.	im Sinne des/der
i.S.v.	im Sinne von
IStR	Internationales Steuerrecht
IT	Information und Telekommunikation
i.V.m.	in Verbindung mit
JA	Juristische Arbeitsblätter
JMStV	Jugendmedienschutz-Staatsvertrag
JR	Juristische Rundschau
Jura	Juristische Ausbildung
JurPC	Internet-Zeitschrift für Rechtsinformatik und Informationsrecht
JuS	Juristische Schulung
JZ	Juristenzeitung
Kap.	Kapitel
K&R	Kommunikation und Recht
KG	Kammergericht
KK-StPO	Karlsruher Kommentar zur Strafprozessordnung
KOM	Dokument der Kommission der Europäischen Gemeinschaften
KritV	Kritische Vierteljahresschrift für Gesetzgebung und Rechtswissenschaft

LG	Landgericht
LKA	Landeskriminalamt
LK-StGB	Leipziger Kommentar zum Strafgesetzbuch
LR-StPO	Löwe-Rosenberg Kommentar zur Strafprozessordnung
LS	Leitsatz
MDStV	Mediendienstestaatsvertrag
MMR	MultiMedia und Recht
m.w.N.	mit weiteren Nachweisen
NJ	Neue Justiz
NJW	Neue Juristische Wochenschrift
NJW-CoR	NJW-Computerreport
N.N.	Nomen nominandum
No., Nr.	Number, Nummer
NS	Nationalsozialismus
NStZ	Neue Zeitschrift für Strafrecht
NStZ-RR	NStZ- Rechtsprechungs-Report Strafrecht
o.Ä.	oder Ähnliches
OECD	Organisation for Economic Co-operation and Development
ÖJZ	Österreichische Juristen-Zeitung
OLG	Oberlandesgericht
ÖZöRV	Österreichische Zeitschrift für öffentliches Recht und Völkerrecht
PCIJ	Publications de la Cour permanente de Justice internationale
RabelsZ	Rabels Zeitschrift für ausländisches und internationales Privatrecht
Rec.	Recommendation
Rel.	Relation
RGBl.	Reichsgesetzblatt
RGSt	Entscheidungen des Reichsgerichts in Strafsachen
RiStBV	Richtlinien für das Straf- und Bußgeldverfahren

RiVASt	Richtlinien für den Verkehr mit dem Ausland in strafrechtlichen Angelegenheiten
RIW	Recht der Internationalen Wirtschaft
Rn.	Randnummer
Rs.	Rechtssache
RStGB	Reichsstrafgesetzbuch
S.	Seite
SchwBGE	Entscheidungen des Schweizerischen Bundesgerichts
SchwZStR	Schweizerische Zeitschrift für Strafrecht
SDÜ	Übereinkommen zur Durchführung des Übereinkommens von Schengen
sic!	Zeitschrift für Immaterialgüter-, Informations- und Wettbewerbsrecht
SK-StGB	Systematischer Kommentar zum Strafgesetzbuch
Slg.	Sammlung
SOCA	Serious Organised Crime Agency
sog.	sogenannt
StGB	Strafgesetzbuch
StIGH	Ständiger Internationaler Gerichtshof
StIGHE	Entscheidungen des Ständigen Internationalen Gerichtshofes in deutscher Übersetzung
StPO	Strafprozessordnung
StraFo	Strafverteidiger Forum
StrRG	Gesetz zur Reform des Strafrechts
StV	Strafverteidiger
TCP	Transmission Control Protocol
TDG	Teledienstegesetz
TKG	Telekommunikationsgesetz
TKÜV	Telekommunikations-Überwachungsverordnung
TMG	Telemediengesetz
TU	Technische Universität
Tz.	Textziffer
u.a.	und andere, unter anderem
ULD	Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein

UMTS	Universal Mobile Telecommunications System
UN	United Nations
UNTS	United Nations Treaty Series
US	United States
USA	United States of America
u.U.	unter Umständen
Var.	Variante
vgl.	vergleiche
VO	Verordnung
vol.	volume
Vorbem	Vorbemerkung
VPN	Virtual Private Network
VStGB	Völkerstrafgesetzbuch
wistra	Zeitschrift für Wirtschafts- und Steuerstrafrecht
WP	Working Party
WPostVtr	Weltpostvertrag
WStG	Wehrstrafgesetz
WWW	World Wide Web
YBILC	Yearbook of the International Law Commission
ZaöRV	Zeitschrift für ausländisches öffentliches Recht und Völkerrecht
ZaRD	Zentralstelle für anlassunabhängige Recherche in Datennetzen
z.B.	zum Beispiel
Ziff.	Ziffer
zit.	zitiert
ZRP	Zeitschrift für Rechtspolitik
ZStrR	Schweizerische Zeitschrift für Strafrecht
ZStW	Zeitschrift für die gesamte Strafrechtswissenschaft
ZUM	Zeitschrift für Urheber- und Medienrecht
ZVglRWiss	Zeitschrift für Vergleichende Rechtswissenschaft

Einleitung

Prägend für die Kriminalität des 21. Jahrhunderts sind die neuartigen grenzüberschreitenden Phänomene, welche insbesondere auf die rasante technische Entwicklung im Zeitalter der Informationsgesellschaft zurückgehen. Das gegenwärtig klassische Beispiel einer globalen Kriminalitätsform ist die Straftatbegehung im Internet (kurz für: *interconnected set of networks*). Das weltumspannende „Netz der Netze" lässt aufgrund seines dezentralen Aufbaus staatliche Grenzen nicht nur für gesetzeskonform handelnde Nutzer, sondern auch für Straftäter verschwimmen. Die zahlreichen praktischen Fälle etwa des Verbreitens und Zugänglichmachens illegaler Inhalte, insbesondere kinderpornografischer oder rassistischer Schriften, wie auch die der Gefährdung der IT-Sicherheit, beispielsweise durch Hacking, den Einsatz von Malware oder die Veranlassung von Distributed Denial of Service Attacks, belegen den sich in Sekundenschnelle ausweitenden Aktions- bzw. Betroffenheitsradius von Tätern und Opfern über den gesamten Erdball. Diese Globalisierung und Internationalisierung von Straftaten im Internet zwingt die Strafverfolgungsbehörden, neue Wege zu beschreiten.

Die Idee eines über weite Strecken reichenden, schnellen Kommunikationssystems war zwar nicht völlig neu; südamerikanische Schnellläuferketten, indianische Rauchzeichen oder aus neuerer Zeit stammende Flügeltelegrafen und Telefonnetze belegen dies. Aber dennoch war und ist die Entwicklung des Internet als weltumspannendes Computernetz nicht nur für legale Anwendungen revolutionär, sondern stellt auch einen Innovationssprung bei der Kriminalitätsentwicklung dar. Gleichermaßen umwälzend gestaltet sich die Verfolgung von Straftaten unter Zuhilfenahme dieses Kommunikationsmediums, bei der die Strafverfolgungsbehörden häufig immer noch juristisches Neuland betreten. Die Strafverfolger müssen, wollen sie der Internetkriminalität wirksam entgegentreten, das „Netz der Netze" zum Ereignisraum ihrer Ermittlungen machen. Aber auch abseits der Verfolgung im Internet begangener Straftaten kommen die Ermittler nicht umhin, die neuen technischen Möglichkeiten in ihrer Arbeit nachzuvollziehen, z.B. für die Verfolgung klassischer Straftaten, bei denen der Täter das Internet u.U. nur zur Kommunikation nutzt oder bei Straftaten ohne jeglichen Internetbezug, beispielsweise für Fahndungsmaßnahmen. Die Zuhilfenahme des Internet bei den Ermittlungen in Strafsachen gewinnt daher in der Praxis erheblich an Bedeutung und infolgedessen auch in der Rechtswissenschaft, welche die mit der Ermittlungsarbeit verbundenen rechtlichen Fragestellungen lösen muss.

Bei Ermittlungen im Internet stoßen die Strafverfolger auf eine Vielzahl nicht abschließend geklärter Rechtsprobleme. Zwar sind mittlerweile umfangreiche Bei-

träge in der Literatur und Rechtsprechung sowohl zum deutschen materiellen Informationsstrafrecht als auch zum Strafprozessrecht zu finden, diese fokussieren sich aber im Wesentlichen auf Betrachtungen der nicht grenzüberschreitenden Begehung von Straftaten und deren Verfolgung. Die Herausforderungen internationaler Sachverhalte gehen die Stellungnahmen hingegen bloß gelegentlich und zumeist nur aus dem Blickwinkel nationalen Straf(anwendungs)rechts an. Das spezifische Charakteristikum der Transnationalität der Straftatbegehung, welches bei der Aufklärung von Straftaten mit Internetbezug nicht mehr nur den Ausnahme-, sondern den Regelfall darstellt, klammert der überwiegende Teil der zur deutschen Strafrechtspflege existierenden Arbeiten aus.

An diesem Scheideweg, wo das nationale Recht an seine territorialen Grenzen stößt, setzt die vorliegende Arbeit an, indem sie die Probleme der extraterritorialen Rechtsanwendung im Strafrecht und Strafprozessrecht bei den Ermittlungen der Strafverfolgungsbehörden im Internet analysiert. Die Herausforderungen der grenzüberschreitenden Computerkriminalität und ihrer Verfolgung werden unter Berücksichtigung der überstaatlichen Rechtsordnung des Völkerrechts untersucht, indem zunächst die dem nationalen Recht für extraterritoriale Hoheitsausübungen gesetzten Grenzen aufgezeigt werden. Anschließend vertieft die Untersuchung die allgemein erläuterten Grenzen unter dem im Common Law für Fragen der Zuständigkeit verwendeten Begriff der *jurisdiction*. Der technisch bedingte, grenzüberschreitende Charakter des „Netzes der Netze" tangiert die Befugnis eines Staates, auf einem bestimmten Territorium Recht zu setzen *(jurisdiction to prescribe)*, zu sprechen *(jurisdiction to adjudicate)* bzw. durchzusetzen *(jurisdiction to enforce)*,[1] insbesondere in zwei Fragestellungen. Die erste Kompetenzfrage betrifft die Anwendbarkeit nationalen Strafrechts auf Internetsachverhalte mit Auslandsbezug, also die Regelungskompetenz eines Staates in diesen Sachverhaltskonstellationen, die zweite die territoriale Reichweite der Ausübungskompetenz nationaler Ermittlungsbehörden bei der grenzüberschreitenden Strafverfolgung innerhalb von Computernetzwerken.

Ziel des ersten Teils der Arbeit ist die Darstellung der Grundlagen und Grenzen des Völkerrechts für extraterritoriale Hoheitsausübungen. Zu diesem Zweck ist zu erforschen, inwieweit der Grundsatz der Gebietshoheit auch für Internetsachverhalte gilt. Des Weiteren werden die Grundanforderungen an die Befugnis zur Ausübung grenzüberschreitender Hoheitsakte herausgearbeitet.

---

[1] American Law Institute, Restatement Foreign Rel. Law 2nd, § 6, comment a – unterscheidet wohl erstmals zwischen den einzelnen Jurisdiktionen, wobei die *jurisdiction to adjudicate* noch als Teil der *jurisdiction to enforce* gezählt wird; dass., vol. 1 Restatement Foreign Rel. Law 3rd, § 401; *Bertele*, Souveränität und Verfahrensrecht, S. 100 f.; Council of Europe, Extraterritorial criminal jurisdiction, S. 18; *Gärditz*, in: Menzel u.a., Völkerrechtsprechung, S. 285; *Koops/Brenner*, in: dies., Cybercrime and Jurisdiction, S. 1, 3; *Meng*, Extraterritoriale Jurisdiktion im öffentlichen Wirtschaftsrecht, S. 1 ff.; *Stein/v. Buttlar*, Völkerrecht, Rn. 536.

Im zweiten Teil beleuchtet die Arbeit in Anwendung der entwickelten Grundlagen die spezifischen völkerrechtlichen Grenzen bei der Bestimmung des Tatorts einer mittels Internet begangenen grenzüberschreitenden Straftat nach dem völkerrechtlich anerkannten Territorialitätsprinzip. Dabei werden nicht nur die dem nationalen Recht durch das Völkerrecht gesetzten Grenzen aufgezeigt, sondern auch das für das Gemeinschaftsrecht prägende und aus der E-Commerce-Richtlinie ins deutsche Telemediengesetz übernommene Herkunftslandprinzip für Informations- und Kommunikationsdienste in seiner Reichweite für das Strafrecht erforscht.

Der dritte Teil der Arbeit nimmt das Strafprozessrecht in den Blick und ermittelt die territoriale Reichweite nationalstaatlicher Ermittlungsbefugnisse. Ausgehend vom einfachen nationalen Recht werden die Vorgaben aktueller internationaler Instrumente, insbesondere der Convention on Cybercrime des Europarats, untersucht. Soweit mangels spezieller Regelung erforderlich, werden auch die allgemeinen völkerrechtlichen Grenzen extraterritorialer Hoheitsausübung herausgearbeitet.

Die aufgezeigten Ziele verfolgt die Arbeit sowohl auf rechtsdogmatische als auch auf rechtssystematische Weise. Die letzten beiden Teile der Untersuchung beleuchten die Vorgaben des Völker- und Europarechts für die Verfolgung von Straftaten im Internet jeweils ausgehend vom geltenden deutschen Recht.

Teil 1

Extraterritoriale Rechtsanwendung im Lichte des Völkerrechts

Die Zunahme grenzüberschreitender Kriminalitätsphänomene[1] zwingt den nationalen Gesetzgeber sowie den Rechtsanwender zum Blick über den Tellerrand des eigenen Staatsgebiets. Infolge der Transnationalität der Straftatbegehung entstehen nämlich Konfliktsituationen zwischen den Staaten nicht nur bei der Anwendung nationalen Rechts auf Sachverhalte mit Auslandsbezug, sondern auch bei der Aufnahme der Verfolgung solcher Taten.[2] Das nationale Recht stößt hierbei an seine territorialen Grenzen. Zur Lösung der Konflikte bedarf es daher des Rückgriffs auf eine überstaatliche Rechtsordnung, der des Völkerrechts, welches die Beziehungen zwischen Völkerrechtssubjekten regelt.

Der deutsche Gesetzgeber und der nationale Rechtsanwender haben bereits nach der Verfassung das Völkerrecht in seinem Kern zu beachten. Gemäß Art. 25 Satz 1 GG sind nämlich die allgemeinen Regeln des Völkerrechts Bestandteil des Bundesrechts und gehen den einfachen Gesetzen vor. Zu diesen allgemeinen Regeln des Völkerrechts zählt das universell geltende Völkergewohnheitsrecht, ergänzt durch anerkannte allgemeine Rechtsgrundsätze.[3] Die allgemeinen Regeln erlangen also über Art. 25 Satz 1 GG selbst unmittelbar Bedeutung; eines Transformationsgesetzes oder anderweitiger Umsetzungsakte ins deutsche Recht bedarf es nicht.[4] Darüber hinaus sind völkerrechtliche Vereinbarungen in der Form des Vertragsrechts denkbar (vgl. dazu Art. 59 Abs. 2 GG), die als Rechtsquelle in einfacher Gesetzesform erst mit der Umsetzung ins deutsche Recht unmittelbar beachtlich werden.[5]

---

[1] Zu Beispielen für transnationale Internetkriminalität siehe *Sofaer/Goodman*, in: dies., The Transnational Dimension of Cyber Crime and Terrorism, S. 1, 7 ff.

[2] AIDP, International Review of Penal Law, vol. 66 (1995), No. 1/2, 60, Tz. 22; OECD, Computer-related Crime: Analysis of Legal Policy, S. 66 ff.; *Sieber*, The international handbook on computer crime, S. 113 f.; *Sofaer*, in: Sofaer/Goodman, The Transnational Dimension of Cyber Crime and Terrorism, S. 221, 232 f. i.V.m. 234 ff.

[3] BVerfGE 15, 25, 32 f.; 23, 288, 317; 66, 39, 64 f.; *Jarass*, in: Jarass/Pieroth, GG, Art. 25, Rn. 5 ff.

[4] *Streinz*, in: Sachs, GG, Art. 25, Rn. 38 ff.

[5] Ebenda, Rn. 60 ff.

I. Fundamente des Völkerrechts

Das Völkerrecht ruht im Wesentlichen auf zwei Fundamenten – der Gleichheit und der Souveränität der Staaten. Aus beiden leitet sich das sogenannte Gebot der Achtung der souveränen Staatengleichheit ab, das sich in Europa bereits infolge des Dreißigjährigen Krieges mit der Anerkennung der Macht der Regionalfürsten und der Herausbildung der Nationalstaaten durchsetzte.[6] Es ist heute insbesondere in Art. 2 Ziff. 1 UN-Charta[7] und der Friendly Relations Declaration[8] niedergelegt. Nach dem Staatengleichheitssatz hat jeder Staat formal betrachtet die gleichen völkerrechtlichen Rechte und Pflichten.[9] Das Souveränitätsprinzip steht dagegen für die Unabhängigkeit eines Staates in seinen Entscheidungen gegenüber anderen Staaten.[10]

Beide Grundprinzipien des Völkerrechts haben verschiedene Ausformungen, die, als Rechtssätze gefasst, deren näheren Anwendungsbereich umreißen. Es handelt sich u.a. um das Gebot der Achtung der Gebietshoheit, das Einmischungs- und Interventionsverbot sowie das Gebot der Achtung fremder Hoheitsakte.

Das Gebot der Achtung der Gebietshoheit besagt, dass kein Staat – vorbehaltlich einzelner, seltener Ausnahmen – berechtigt ist, unmittelbar auf fremdes Territorium einzuwirken.[11] Dieses Verbot gilt unabhängig davon, ob die Einwirkung hoheitlicher (z.B. Ladung eines Zeugen) oder rein tatsächlicher (z.B. Ausstoß von Immis-

---

[6] Siehe das Allgemeine Friedensgebot in § 1 des Münsterschen Friedensvertrages, welches alle Fürsten gleichberechtigt nennt, und die Unterschrifts- und Ratifizierungsregelungen in den §§ 111, 119 und 120, abrufbar unter http://www.lwl.org/westfaelische-geschichte/portal/Internet/finde/langDatensatz.php?urlID=741&url_tabelle=tab_quelle [Stand: 6.11.2013].

[7] Charta der Vereinten Nationen – Amtliche Fassung der Bundesrepublik Deutschland, BGBl. II 1973, S. 431 ff.

[8] Declaration on Principles of International Law concerning Friendly Relations and Co-operation among States in accordance with the Charter of the United Nations vom 24.10.1970 (abgedruckt in *Tomuschat*, Völkerrecht, Ordnungsnummer 6), die selbst keine formelle Quelle des Völkerrecht ist, sondern in der die Mitgliedstaaten der UNO geltendes Völkerrecht festhalten wollten; siehe zu Letzterem *Verdross/Simma*, Universelles Völkerrecht, § 453.

[9] *Graf Vitzthum*, in: Graf Vitzthum/Bothe, Völkerrecht, 1. Abschnitt, Rn. 45; *Meessen*, Völkerrechtliche Grundsätze des internationalen Kartellrechts, S. 92; *Verdross/Simma*, Universelles Völkerrecht, § 454.

[10] *Graf Vitzthum*, in: Graf Vitzthum/Bothe, Völkerrecht, 1. Abschnitt, Rn. 46; *Ipsen*, Völkerrecht, § 5, Rn. 7.

[11] Council of Europe, Extraterritorial criminal jurisdiction, S. 18; *Doehring*, Völkerrecht, Rn. 88 f.; *Geiger*, Grundgesetz und Völkerrecht mit Europarecht, S. 247 f., 312; *Ipsen*, Völkerrecht, § 23, Rn. 67, 69; *Proelß*, in: Graf Vitzthum/Bothe, Völkerrecht, 5. Abschnitt, Rn. 16; *Rehbinder*, Extraterritoriale Wirkungen des deutschen Kartellrechts, S. 394; *Schwörer*, wistra 2009, 452, 453; *Siegrist*, Hoheitsakte auf fremdem Staatsgebiet, S. 10 f.; *Spang-Hanssen*, Cyberspace & International Law, S. 209, 439; *Stein/v. Buttlar*, Völkerrecht, Rn. 537.

sionen) Natur ist, und ob sie heimlich oder offen geschieht.[12] Demgegenüber schützt das Einmischungs- und Interventionsverbot das sich aus dem Gebot der Achtung der souveränen Staatengleichheit ergebende Recht auf Selbstbestimmung.[13] Der konkrete Inhalt des Prinzips ist jedoch umstritten. Unter „Intervention" soll im Weiteren die Freiheit eines Staates in seiner autonomen Willensbildung sowohl gegenüber militärischem Zwang als auch gegenüber unzulässiger Druckausübung mit politischen und wirtschaftlichen Mitteln[14] und unter „Einmischung" die Anmaßung eigener Regelungs- und Mitsprachekompetenz in Angelegenheiten, für deren Regelung ein anderer Staat ausschließlich zuständig ist, verstanden werden.[15] Gemeinsames Ziel der Verbote ist die Verhinderung der Fremdbestimmung eines Staates.[16] Das letzte hier zu erwähnende Gebot der Achtung fremder Hoheitsakte beinhaltet die Pflicht, die bereits eingetretene Feststellungs-, Befehls- oder Gestaltungswirkung, die fremde Hoheitsakte sich nach eigenem Recht beimessen, grundsätzlich zu respektieren.[17] Aus diesem Gebot ergibt sich aber nicht etwa per se die Pflicht zur Vollziehung fremder Hoheitsakte oder zur Hinnahme einer Beeinträchtigung eigener Regelungsbefugnisse. Eine völkerrechtliche Pflicht zur Respektierung fremder Hoheitsakte besteht insbesondere dann nicht, wenn der jeweilige Hoheitsakt von vornherein (auch) im Ausland seine Wirkungen entfalten sollte und keinen sinnvollen Anknüpfungspunkt an den geregelten Sachverhalt aufweist.[18]

---

[12] *Dahm/Delbrück/Wolfrum*, Völkerrecht, Bd. I/3, S. 792 f.; *Ipsen*, Völkerrecht, § 23, Rn. 69–72; *Verdross/Simma*, Universelles Völkerrecht, § 456.

[13] *Bertele*, Souveränität und Verfahrensrecht, S. 176; Council of Europe, Extraterritorial criminal jurisdiction, S. 21 f.; *Dahm/Delbrück/Wolfrum*, Völkerrecht, Bd. I/3, S. 797; *Pappas*, Stellvertretende Strafrechtspflege, S. 77; *Verdross/Simma*, Universelles Völkerrecht, § 490; *Ziegenhain*, Extraterritoriale Rechtsanwendung, S. 31.

[14] *Geiger*, Grundgesetz und Völkerrecht mit Europarecht, S. 313; *Pappas*, Stellvertretende Strafrechtspflege, S. 77; *Verdross/Simma*, Universelles Völkerrecht, § 491; *Ziegenhain*, Extraterritoriale Rechtsanwendung, S. 31 f.

[15] *Geiger*, Grundgesetz und Völkerrecht mit Europarecht, S. 312; *Pappas*, Stellvertretende Strafrechtspflege, S. 77; *Ziegenhain*, Extraterritoriale Rechtsanwendung, S. 32.

[16] Siehe hierzu den dritten Programmsatz (The principle concerning the duty not to intervene in matters within the domestic jurisdiction of any State, in accordance with the Charter) in der Declaration on Principles of International Law concerning Friendly Relations and Co-operation among States in accordance with the Charter of the United Nations vom 24.10.1970 (abgedruckt in *Tomuschat*, Völkerrecht, Ordnungsnummer 6).

[17] *Verdross/Simma*, Universelles Völkerrecht, § 1021.

[18] Ebenda.

II. Das Gebot der Achtung der Gebietshoheit im Internet

Soweit das Völkerrecht die Ausübung der Hoheitsgewalt auf das eigene Staatsgebiet begrenzt, ist fraglich, ob das der Beschränkung zugrunde liegende Gebot der Achtung der Gebietshoheit fremder Staaten überhaupt für Handlungen im Internet gilt oder ob dieser Grundsatz auf das globale Computernetzwerk aufgrund dessen Grenzen ignorierender Infrastruktur unanwendbar ist, weil die Staaten ihre Gebietshoheit gar nicht ausüben könnten.[19] Die hiermit angesprochene Problematik ist nicht unbekannt, denn mit ähnlichen Fragestellungen waren bereits Völkerrechtler bei früheren technischen Entwicklungen, wie beispielsweise dem Aussenden von Funkwellen und den darauf folgenden Diskussionen um eine sogenannte Ätherfreiheit, konfrontiert.[20] Auch die Funkwellen überschritten technikbedingt Staatsgrenzen, ohne dass solche Grenzüberschreitungen – abgesehen vom Verzicht auf die Technik selbst – immer unterbunden werden konnten bzw. beherrschbar waren. Dessen ungeachtet hat sich bisher jedoch noch keine endgültige Rechtsauffassung gebildet, wie solche Phänomene des scheinbar faktischen Verlusts der Souveränität völkerrechtlich zu behandeln sind.[21] Nur für das Verbringen körperlicher Gegenstände über die Grenze eines Staates bzw. die Leitung unkörperlicher Objekte (z.B. von Telekommunikation) über leitungsgebundene Netze besteht Einigkeit, dass es hierzu einer Einwilligung des betroffenen Staates bedarf, um eine rechtswidrige Verletzung seiner Gebietshoheit auszuschließen.

Auf die Frage der Geltung der Gebietshoheit auch im Internet hat die Literatur noch keine einhellige Antwort gefunden. Einige Autoren ziehen für das globale Computernetzwerk Parallelen zu internationalen Räumen wie dem Weltall[22] und sehen das Internet damit als hoheitsneutrale Sphäre an.[23] Andere Autoren sind der Auffassung, dass der Cyberspace jenseits aller geographischen Grenzen existiere

---

[19] Für eine Anwendbarkeit: wohl *Bär*, Der Zugriff auf Computerdaten im Strafverfahren, S. 234 f., der auf die Territorialhoheit abstellt; *Determann*, Kommunikationsfreiheit im Internet, S. 172; *Germann*, Gefahrenabwehr und Strafverfolgung im Internet, S. 641 ff., widersprüchlich allerdings auf S. 650, wo er vom Internet als hoheitsneutraler Sphäre spricht; im Ergebnis auch *Putnam/Elliott*, in: Sofaer/Goodman, The Transnational Dimension of Cyber Crime and Terrorism, S. 35, 61; *Sahlfeld*, Die Veränderung der Ausübung der Staatsgewalt, S. 59; *Valerius*, Ermittlungen der Strafverfolgungsbehörden, S. 146; gegen eine Anwendbarkeit: *Graham*, JurPC, Web-Dok. 35/1999, Abs. 23, 46; *Jofer*, Strafverfolgung im Internet, S. 195; *Johnson/Post*, Stanford Law Review, vol. 48 (1996), 1367, 1379 f.

[20] *Engel*, RabelsZ 49 (1985), 90, 95 f.; *Verdross/Simma*, Universelles Völkerrecht, §§ 1051 ff.

[21] So haben sich gegen die sog. Ätherfreiheit insbesondere die damals noch zahlreichen sozialistischen Staaten gewandt, siehe hierzu *Simma*, in: BerDGesVölkR 19, S. 39, 46 ff.; *Verdross/Simma*, Universelles Völkerrecht, § 1053.

[22] *Grahman*, JurPC, Web-Dok. 35/1999, Abs. 42, 46.

[23] *Germann*, Gefahrenabwehr und Strafverfolgung im Internet, S. 650.

und nur punktuell einer staatlichen Gewalt zugänglich sei.[24] Gegen diese Tendenzen einer Abgrenzung des Internet von der realen Welt spricht sich jedoch zutreffend eine andere Ansicht aus, die dem Internet die Eigenschaft eines solchen abgrenzbaren und eigenständigen Raums schon deshalb nicht zuschreiben will, weil mit dem „Eintritt" in die virtuelle Welt die sogenannte „Offline"-Welt nicht verlassen wird, sondern derart enge Schnittstellen zwischen den verschiedenen Sphären bestehen, dass letztlich jede Aktivität im Netz auf eine in der realen Welt zurückführbar und deshalb die Anknüpfung an die Gebietshoheit weiterhin möglich ist.[25]

Zwar gibt es einige Besonderheiten, die eine gewisse Eigenständigkeit des Internet belegen. So verfügt das Netz über eine eigene nicht-hierarchische Struktur, die keiner territorialen Einheit folgt, und die Übertragung der Daten richtet sich im Wesentlichen allein nach der Verfügbarkeit von effizienten Übertragungswegen. Das Internet untersteht zudem mit der ICANN[26] einer Art „Regierung", die über einige Organisationsmaßnahmen für die Nutzung des Internet bestimmt. Gleichwohl üben aber in der Praxis die einzelnen Nationalstaaten die tatsächliche Kontrolle über die Internetnutzer aus, indem sie deren Aktivitäten reglementieren und ggf. ahnden oder unterbinden.

Abseits dieser gelebten Staatenpraxis gibt es auch völkerrechtstheoretische Gründe, die der Annahme eines eigenständigen Raums Internet widersprechen. Ein Blick auf die bisher im Völkerrecht tatsächlich existierenden, der Hoheitsgewalt von Staaten nur beschränkt unterliegenden Gebiete offenbart nämlich wesentliche Unterschiede, die eine Gleichbehandlung ausschließen. Als staatenlos gelten neben der Antarktis der Weltraum, Teile des Luftraums[27] sowie die Hohe See. Die Behandlung von Sachverhalten, die sich dort ereignen, regeln verschiedene völkerrechtliche Verträge.[28] Die Ausübung staatlicher Gewalt bleibt in diesen genuin hoheitsfreien Gebieten gerade dort möglich, wo sich Menschen mithilfe von Fahrzeugen (Schiffen, Flugzeugen, Raumfähren etc.) oder durch von ihnen entsendete

---

[24] *Spang-Hanssen*, Cyberspace & International Law, S. 313 ff. m.w.N.

[25] *Determann*, Kommunikationsfreiheit im Internet, S. 166 ff.; *Valerius*, Ermittlungen der Strafverfolgungsbehörden, S. 145 f.

[26] Siehe auch http://www.icann.org [Stand: 6.11.2013].

[27] Siehe zu den Schwierigkeiten der Abgrenzung der Souveränität einzelner Staaten im Luftraum *Doehring*, Völkerrecht, Rn. 544 ff.

[28] Für den Weltraum: Vertrag vom 27.1.1967 über die Grundsätze zur Regelung der Tätigkeiten von Staaten bei der Erforschung und Nutzung des Weltraums einschließlich des Mondes und anderer Himmelskörper, BGBl. II 1969, S. 1967; für den Luftraum: Das bis heute noch wesentlichste Abkommen ist die Chicago Convention on International Civil Aviation vom 7.12.1944, UNTS, Bd. 171, S. 387 ff.; zu weiteren Abkommen siehe *Doehring*, Völkerrecht, Rn. 551 ff.; für die Hohe See: Übereinkommen über die Hohe See vom 29.4.1958, BGBl. II 1972, S. 1091, 1094 mit Ausführungsgesetz vom 21.9.1972 (BGBl. II 1972, S. 1089), daran sich anschließend das Seerechtsübereinkommen der Vereinten Nationen vom 10.12.1982, BGBl. II 1994, S. 1798, ergänzt um ein Übereinkommen vom 28.7.1994 zur Durchführung der Regelungen zum Meeresbergbau (Ausführungsgesetz vom 15.6.1995, BGBl. I 1994, S. 778).

Objekte (Satelliten etc.) befinden. Solche Objekte werden praktisch wie bewegliches Territorium im rechtlichen Niemandsland behandelt, unterliegen also der Gewalt eines bestimmten Staates. Anknüpfungspunkt für diese Staatsgewalt (und damit die Staatenverantwortung) ist dabei regelmäßig ein formeller Akt, nämlich die Registrierung des Objekts. Für den Bereich des Internet ist eine vergleichbare Erfassung indes nirgends vorgesehen und auch nicht zweckmäßig. Aufgrund ihrer Flüchtigkeit und der unbeschränkten Möglichkeit ihrer Vervielfältigung scheidet eine Anknüpfung an Daten als registrierbare Objekte aus.

Die Erfassung von Rechnern kommt ebenfalls nicht in Betracht, weil dies einer Anknüpfung an die Gebietshoheit des Registerstaates gleichkäme und damit bereits ein eigenständiger, vom herkömmlichen Territorium unterscheidbarer Raum entfiele. Daneben zeichnen sich die Kommunikationsabläufe im Internet immer noch im Wesentlichen durch eine konstante Verbindung zu den Territorien von Staaten aus,[29] weil sie zumeist über Computersysteme auf der Erdoberfläche[30] abgewickelt werden, sodass die Geltung der Gebietshoheit auch für das Internet naheliegt.[31] Ein dem Internet entsprechender virtueller Raum ließe sich also gar nicht von der herkömmlichen Offline-Nutzung von Computern abtrennen;[32] diese Nutzung soll daher auch nach den Vertretern einer eigenständigen Behandlung des Cyberspace nicht der Gebietshoheit der Staaten entzogen werden. Personen können ihre Computersysteme nämlich sowohl off- als auch online verwenden, insbesondere sind zahlreiche Rechner nicht fortwährend an das Internet durch eine Standleitung angeschlossen. Selbst eine Differenzierung nach permanenten Speicherinhalten und Zwischenspeicherungen ist praktisch kaum realisierbar,[33] weil selbst Letztere nicht von vornherein zwingend zeitlich eng begrenzt sein müssen, sondern beispielsweise in Form von Nachrichten in E-Mail-Postfächern teilweise Tage oder Wochen andauern, bevor der Empfänger die Daten abruft. Gleiches gilt für die Fixierung von Daten in sogenannten Cache-Speichern, die auf eine schnelle und kurze Spei-

---

[29] *Determann*, Kommunikationsfreiheit im Internet, S. 168.

[30] Soweit Computersysteme auf Schiffen oder Flugzeugen verwendet werden, bietet sich wiederum das Flaggenprinzip als besondere Ausformung des Territorialitätsprinzips als Anknüpfungspunkt an.

[31] Siehe auch Tz. 234 des Erläuternden Berichts zur Convention on Cybercrime (in deutscher Übersetzung in BT-Drucks. 16/7218, S. 85), in dem die Verfasser darlegen, dass sie in der Konvention bewusst von einer Bestimmung absahen, welche die Vertragsparteien verpflichten sollte, eine Gerichtsbarkeit für Straftaten zu begründen, die auf ihren Namen eingetragene Satelliten betreffen. Nach Ansicht der Verfasser war eine solche Bestimmung nämlich überflüssig, „weil rechtswidrige Datenübertragungen mit Satelliten zwangsläufig von der Erde ausgehen und/oder empfangen werden. […] Schließlich haben die Verfasser sich auch die Frage gestellt, ob eine Strafgerichtsbarkeit durch die Eintragung territorial angemessen begründet werden kann, weil in vielen Fällen kein sinnvoller Zusammenhang zwischen der begangenen Straftat und dem Staat der Registrierung hergestellt werden könne, da ein Satellit lediglich als Übertragungsmittel funktioniert."

[32] *Determann*, Kommunikationsfreiheit im Internet, S. 169.

[33] Ebenda.

cherung ausgelegt sind, da in der Praxis der Cache nicht nur für eine Zwischenspeicherung von Daten während des Transports, sondern ebenfalls für deren originären Abruf genutzt werden kann, insbesondere wenn eine häufig angefragte Information nur über große Entfernungen abrufbar ist.

Das Internet ist folglich nicht sinnvoll als ein eigenständiger Raum abgrenz- und regelbar. Das Gebot der Achtung der Gebietshoheit gilt auch für das „Netz der Netze". Die sich aus dem Gebietsgrundsatz ableitende Hoheitsgewalt obliegt grundsätzlich dem Staat, in dem die Daten gespeichert sind.

III. Extraterritoriale Hoheitsakte

Ob und inwieweit ein Staat in die dargestellten völkerrechtlichen Gebote im Einzelnen eingreift, ist häufig schwer zu beurteilen. Zum einen ist bereits umstritten, wann überhaupt ein hoheitliches Handeln vorliegt (nachfolgend unter A.), und zum anderen hängt die Beurteilung der Voraussetzungen der Zulässigkeit eines Hoheitsaktes mit Bezug zum Ausland davon ab, wo er vollzogen wird bzw. wo seine Auswirkungen eintreten (unter B.).

A. Hoheitliches Handeln

Die Antwort auf die Frage nach den Voraussetzungen des Vorliegens hoheitlichen Handelns ist nicht umfassend eindeutig beantwortbar, da sich der Grenzbereich zwischen hoheitlichem und nichthoheitlichem Handeln stetig verschiebt.[34]

Unbestritten ist ein Hoheitsakt jedenfalls dann gegeben, wenn staatliche Organe in Ausübung hoheitlicher Gewalt, also in der Regel mit öffentlich-rechtlich begründeter Befehls- und Zwangsgewalt, handeln.[35] Strittig ist hingegen, ob darüber hinaus auch zwangsfreie Maßnahmen zum hoheitlichen Handeln zählen können. Während beispielsweise insbesondere die in der Tradition des Common Law stehenden Länder in zwangsfreien Handlungen regelmäßig keinen Hoheitsakt und damit keine Verletzung des Völkerrechts sehen,[36] beschränkt das Bundesverfas-

---

[34] *v. Münch*, Das völkerrechtliche Delikt, S. 138 f.

[35] *Okresek*, ÖZöRV 35 (1985), 325, 325; *Schlochauer*, Die extraterritoriale Wirkung von Hoheitsakten, S. 9; *Tiedemann*, FS Bockelmann, S. 819, 821 ff.

[36] Siehe hierzu die Darstellungen bei *Nagel*, Beweisaufnahme im Ausland, S. 21, 29 ff.; *Nordmann*, Die Beschaffung von Beweismitteln aus dem Ausland, S. 57 ff.; *Schädel*, Die Bewilligung internationaler Rechtshilfe, S. 41 f.; *Tiedemann*, FS Bockelmann, S. 819, 819 ff.; vgl. hierzu auch die Vorschläge vom American Law Institute, vol. 1 Restatement Foreign Rel. Law 3rd, § 431, comment e (i).

sungsgericht[37] Hoheitsakte zutreffend nicht auf Zwangsmaßnahmen.[38] Die Differenzierung nach Handlungen mit oder ohne Zwangscharakter stellt nämlich letztlich auf die Einwilligung des Betroffenen ab,[39] da der Vollzug von Zwang grundsätzlich mit dessen Zustimmung zur Maßnahme entfällt. Vom Vorliegen einer Einwilligung durch den Betroffenen, der regelmäßig Privatperson oder juristische Person des Privatrechts ist, in die Handlungen eines Staates auf fremdem Staatsgebiet oder in Maßnahmen mit extraterritorialer Wirkung kann jedoch ein Verstoß gegen völkerrechtliche Gebote nicht abhängen. Die völkerrechtlichen Gebote stehen nämlich nicht zur Disposition von Privatpersonen oder juristischen Personen des Privatrechts, sondern sollen wie beispielsweise die Gebietshoheit ausschließlich die Souveränität des einzelnen Staates schützen.[40]

B. Hoheitsakte auf fremdem Staatsgebiet vs. extraterritoriale Hoheitsakte

Liegt ein Hoheitsakt im jeweiligen Einzelfall vor, so ist bei Sachverhalten mit Bezug zum Ausland im Folgenden zu unterscheiden, ob es sich um einen Hoheitsakt auf fremdem Staatsgebiet oder einen sogenannten extraterritorialen Hoheitsakt handelt.[41] Nicht jedes Handeln eines staatlichen Organs mit Bezug zum Ausland

---

[37] BVerfGE 63, 343, 372; in diesem Sinne auch das schweizerische Bundesgericht SchwBGE 65 I, 39, 44.

[38] So auch *Bertele*, Souveränität und Verfahrensrecht, S. 84 f.; *Geck*, in: Strupp/Schlochauer, Wörterbuch des Völkerrechts, S. 795; *Germann*, Gefahrenabwehr und Strafverfolgung im Internet, S. 642; *Jofer*, Strafverfolgung im Internet, S. 192; *Okresek*, ÖZöRV 35 (1985), 325, 339 ff., 343 mit praktischen Beispielsfällen u.a. aus Österreich und Deutschland; *Schmidt*, Gefahrenabwehrmaßnahmen im Internet, S. 264; *Siegrist*, Hoheitsakte auf fremdem Staatsgebiet, S. 11; *Spatscheck*, Steuern im Internet, Rn. 304; *Tiedemann*, FS Bockelmann, S. 819, 822 ff.; *Valerius*, Ermittlungen der Strafverfolgungsbehörden, S. 147.

[39] *Nordmann*, Die Beschaffung von Beweismitteln aus dem Ausland, S. 59; *Siegrist*, Hoheitsakte auf fremdem Staatsgebiet, S. 12; *Valerius*, Ermittlungen der Strafverfolgungsbehörden, S. 147.

[40] *Bertele*, Souveränität und Verfahrensrecht, S. 86 f.; *Gruhl*, in: Welp, kriminalität@net, S. 49, 67, 73, allerdings ohne Begründung; *Nordmann*, Die Beschaffung von Beweismitteln aus dem Ausland, S. 59; *Okresek*, ÖZöRV 35 (1985), 325, 342 f.; *Siegrist*, Hoheitsakte auf fremdem Staatsgebiet, S. 12; *Spatscheck*, Steuern im Internet, Rn. 307 jeweils m.w.N.; *Spatscheck/Alvermann*, wistra 1999, 333, 334; anders hingegen die Auffassung in Ländern des Common Law, vgl. dazu beispielhaft den Fall *Aboujdid vs. Singapore Airlines* in American Law Institute, Case Citation Restatement Foreign Rel. Law 1993-1994, S. 170.

[41] Siehe zur Differenzierung zwischen extraterritorialen Hoheitsakten und Hoheitsakten auf fremdem Staatsgebiet *Beitzke*, in: Strupp/Schloachauer, Wörterbuch des Völkerrechts, Bd. 1, S. 504; *Geck*, in: Strupp/Schlochauer, Wörterbuch des Völkerrechts, S. 795 f.; *Schlochauer*, Die extraterritoriale Wirkung von Hoheitsakten, S. 10 f.; *v. Münch*, Das völkerrechtliche Delikt, S. 65.

erfolgt nämlich per se völkerrechtswidrig. Um eine rechtswidrige Anmaßung von Hoheitsgewalt handelt es sich nur dann, wenn die Maßnahmen der staatlichen Organe in Konkurrenz zum Verhalten staatlicher Behörden auf fremdem Staatsgebiet treten.[42]

Völkerrechtlich generell unzulässig sind daher Hoheitsakte, die ohne Einwilligung durch auf fremdem Staatsgebiet physisch befindliche staatliche oder staatlich gelenkte Organe vorgenommen werden.[43] Mit ihnen greift der handelnde Staat in die Souveränität des betroffenen Drittstaates ein, soweit keine speziellen Befugnisnormen vorliegen.[44] Hiervon zu unterscheiden sind die Hoheitsakte, bei denen staatliche Organe auf dem eigenen Staatsgebiet hoheitlich handeln, ihr Handeln jedoch in fremdes Staatsgebiet hineinwirkt.[45] Eine solche Anwendung des nationalen Rechts auf Sachverhalte mit Auslandsbezug wird, obwohl die unmittelbare Ausübung der Hoheitsgewalt selbst auf das eigene Staatsgebiet begrenzt ist, missverständlich als „extraterritoriale Hoheitsausübung" bezeichnet.[46] Die hoheitliche Handlung ist jedoch nur insoweit (mittelbar) extraterritorial, als sie sich auf dem Territorium eines weiteren Staates auswirkt.[47] Sowohl die Ausdehnung des nationalen Strafrechts auf Sachverhalte mit Auslandsbezug als auch die überwiegenden Maßnahmen der Strafverfolgungsbehörden im Internet zählen zu dieser letzten Gruppe. Die Beamten verbleiben nämlich physisch auf dem Territorium des eigenen Staatsgebiets und nur bestimmte Wirkungen ihrer Handlungen treten auf fremdem Gebiet ein, z.B. ein Normbefehl an Personen, die sich auf fremdem Territorium befinden, oder der Zugriff auf Computersysteme im Ausland.

---

[42] *Germann*, Gefahrenabwehr und Strafverfolgung im Internet, S. 642.

[43] *Geck*, in: Strupp/Schlochauer, Wörterbuch des Völkerrechts, S. 795 f.; *Schlochauer*, Die extraterritoriale Wirkung von Hoheitsakten, S. 10 f.; *v. Münch*, Das völkerrechtliche Delikt, S. 65.

[44] *Bertele*, Souveränität und Verfahrensrecht, S. 78 ff., 89, 93; Council of Europe, Extraterritorial criminal jurisdiction, S. 18; *Jescheck/Weigend*, Strafrecht AT, § 18 I 4 (S. 166); *Rudolf*, in: BerDGesVölkR 11, S. 7, 33 f.; *Stein/v. Buttlar*, Völkerrecht, Rn. 537; *Ziegenhain*, Extraterritoriale Rechtsanwendung, S. 2.

[45] *Beitzke*, in: Strupp/Schlochauer, Wörterbuch des Völkerrechts, Bd. 1, S. 504; *Schlochauer*, Die extraterritoriale Wirkung von Hoheitsakten, S. 10 f.; *v. Münch*, Das völkerrechtliche Delikt, S. 65.

[46] *Meng*, ZaöRV 44 (1984), 675, 727 f.; *Schlochauer*, Die extraterritoriale Wirkung von Hoheitsakten, S. 10 f.; *Ziegenhain*, Extraterritoriale Rechtsanwendung, S. 1.

[47] *Schlochauer*, Die extraterritoriale Wirkung von Hoheitsakten, S. 10 f.; *Ziegenhain*, Extraterritoriale Rechtsanwendung, S. 1 f.

IV. Völkerrechtliche Befugnis zur extraterritorialen Hoheitsausübung

Unter welchen Voraussetzungen Nationalstaaten zur Ausübung extraterritorialer Hoheitsakte befugt sind, hängt ganz wesentlich von der konkreten Ausgestaltung der Akte ab. Hoheitsakte auf dem eigenen Staatsgebiet unterliegen, auch soweit sie in fremdes Staatsgebiet hineinwirken, folglich nicht generell dem Verdikt der Völkerrechtswidrigkeit. Vielmehr sind sie nur dann unzulässig, wenn sie den Tatbestand eines völkerrechtlichen Delikts verwirklichen.[48] Ein solches liegt vor, wenn ein Völkerrechtssubjekt eine ihm obliegende völkerrechtliche Pflicht verletzt und einem anderen Völkerrechtssubjekt einen Schaden materieller oder immaterieller Art zufügt,[49] wobei letztere Voraussetzung nach einer im Vordringen befindlichen Meinung kein konstitutives Element mehr sein soll, weil bereits in der bloßen Verletzung der Rechte eines Völkerrechtssubjekts ein Schaden zu sehen sei.[50] Ob darüber hinaus der Unrechtstatbestand eine schuldhafte Herbeiführung erfordert oder allein eine objektive Erfolgsbegründung ausreicht, ist nach wie vor umstritten. In der Rechtsprechung, im Schrifttum sowie in der gelebten Staatenpraxis konnten sich weder das Verschuldens- noch das Erfolgsprinzip endgültig durchsetzen,[51] allerdings ist zu Recht eine Tendenz hin zum Erfolgsprinzip zu verzeichnen.[52] Für das Erfolgsprinzip sprechen nicht nur die geringeren Beweisschwierigkeiten, sondern auch das fehlende negative Werturteil, welches mit einem Verschuldensnachweis verbunden wäre.[53] Darüber hinaus bedingt das Erfolgsprinzip eine strengere Inpflichtnahme und hiermit verbunden eine größere Sorgfalt der Staaten, völkerrechtliche Delikte zu vermeiden. Schlussendlich lassen sich die Risiken des Gebrauchs neuer Techniken mit dem Erfolgsprinzip besser regeln.[54]

Ein extraterritorialer Hoheitsakt ist danach insbesondere dann grundsätzlich völkerrechtswidrig, wenn er die Gebietshoheit des fremden Staates unmittelbar verletzt, der Hoheitsakt in seinen Wirkungen einem Hoheitsakt auf fremdem Staats-

---

[48] *Schlochauer*, Die extraterritoriale Wirkung von Hoheitsakten, S. 41; *v. Münch*, Das völkerrechtliche Delikt, S. 65.

[49] Zum Begriff des völkerrechtlichen Delikts *Daum*, Grenzverletzungen und Völkerrecht, S. 27 ff.; *Schüle*, in: Strupp/Schlochauer, Wörterbuch des Völkerrechts, S. 326; *v. Münch*, Das völkerrechtliche Delikt, S. 134, 140.

[50] *Daum*, Grenzverletzungen und Völkerrecht, S. 41 m.w.N.

[51] Ebenda, S. 38; *Schüle*, in: Strupp/Schlochauer, Wörterbuch des Völkerrechts, S. 336; *Sieber*, Straftaten und Strafverfolgung im Internet, C147; *Siegrist*, Hoheitsakte auf fremdem Staatsgebiet, S. 87 ff.; *Strupp*, Das völkerrechtliche Delikt, S. 45 ff.; *v. Münch*, Das völkerrechtliche Delikt, S. 152 ff.; *Wilske*, Die völkerrechtswidrige Entführung, S. 105 f. jeweils m.w.N.

[52] *Daum*, Grenzverletzungen und Völkerrecht, S. 38 ff.; *Siegrist*, Hoheitsakte auf fremdem Staatsgebiet, S. 90; *v. Münch*, Das völkerrechtliche Delikt, S. 163 f.

[53] *v. Münch*, Das völkerrechtliche Delikt, S. 164.

[54] Ebenda, S. 164 f.

gebiet gleichkommt oder die Sicherheit und Ordnung des fremden Staates beeinträchtigt.[55] Eine über diese abstrakten Umschreibungen hinausgehende Aufstellung aller potentiell deliktischen Verhaltensweisen, die für Ermittlungen im Internet in Betracht kommen könnten, würde allerdings auf die Nacherzählung des gesamten Völkerrechts hinauslaufen. Da es insbesondere konkrete Einzeltatbestände nicht gibt,[56] scheidet ein solches Vorgehen aus.[57]

Um die Grenzen des Spielraums nationaler Gesetzgeber und Rechtsanwender bei der Vornahme extraterritorialer Hoheitsakte gleichwohl in Teilbereichen zu verdeutlichen, sollen im Folgenden die Anwendung des deutschen Rechts auf Internetsachverhalte mit Auslandsbezug (nachfolgend unter Teil 2) und die territoriale Reichweite der Befugnisse deutscher Strafverfolgungsbehörden bei der Ermittlungsarbeit im Internet (unter Teil 3) näher untersucht werden.

---

[55] Ebenda, S. 65.

[56] *Schüle*, in: Strupp/Schlochauer, Wörterbuch des Völkerrechts, S. 329.

[57] *v. Münch*, Das völkerrechtliche Delikt, S. 135.

Teil 2

Anwendbarkeit des deutschen Strafrechts auf Auslandssachverhalte

Die nicht zuletzt dem technischen Aufbau des Internet geschuldete Transnationalität der Begehung von Straftaten im „Netz der Netze" führt zu der Frage, ob und inwieweit ein Staat für diese Taten nach nationalem Recht die Strafgewalt reklamieren kann. Soll unter Berücksichtigung der faktisch fehlenden Durchsetzungsmöglichkeiten von Hoheitsgewalt gegenüber Tätern im Ausland die Befugnis zur Regelung grenzüberschreitender Sachverhalte in der Praxis nicht zur leeren Hülle verkommen, kann auch mit Blick auf zu erwartende zwischenstaatliche Spannungen das Recht zur Anwendung nationalen Rechts auf globale Kriminalitätsphänomene nicht grenzenlos sein.

Ausgangspunkte der Untersuchung, inwieweit eine Kompetenz zur Anwendung des Strafrechts auf Sachverhalte mit Auslandsbezug besteht, sind die Grundsätze des internationalen Strafrechts (nachfolgend unter I.). Die Bestimmung des Tatorts bei grenzüberschreitenden Kriminalitätsformen erfolgt zuvorderst anhand des Territorialitätsprinzips als Haupt- und Ausgangsprinzip der meisten Rechtsordnungen der Welt, da es für die Ausübung von Strafgewalt weltweit anerkannt ist[1] (unter II.). Aufgrund der unterschiedlichen Auslegung der Reichweite dieses Prinzips in den verschiedenen Staaten kann sich allerdings eine Vielzahl von positiven Kompetenzkonflikten ergeben, denen nur durch restriktive Handhabung dieser Anwendungsregel begegnet werden kann.[2]

Nach der Analyse des völkerrechtlichen Konfliktpotentials, welches mit einer extraterritorialen Hoheitsausübung verbunden sein kann, zeigt die Arbeit daher die Grenzen der völkerrechtlichen Befugnis zur Anwendung des nationalen Strafrechts auf Sachverhalte mit Auslandsbezug auf. Hierbei wird herausgearbeitet, dass eine hinreichende Konfliktlösung in grenzüberschreitenden Sachverhaltskonstellationen,

---

[1] Siehe hierzu nur American Society of International Law, AJIL 29 (1935), 480 ff.; Council of Europe, Extraterritorial criminal jurisdiction, S. 8; OECD, Computer-related Crime: Analysis of Legal Policy, S. 66; *O'Connor* et al., Model Codes for Post-Conflict Criminal Justice, S. 42; *Oehler*, Internationales Strafrecht, Rn. 153 f. – mit Nachweisen für das Territorialitätsprinzip, das sich in allen Rechtsordnungen weltweit wiederfindet; United Nations, Manual on the prevention and control of computer-related crime, Tz. 249.

[2] Council of Europe, Extraterritorial criminal jurisdiction, S. 8 f.; *Jennings*, BYIL 33 (1957), 146, 159; United Nations, Manual on the prevention and control of computer-related crime, Tz. 247 ff.; *Vander Beken* et al., Finding the Best Place for Prosecution, S. 11, Rn. 20 f.; S. 12, Rn. 23; zum historischen Wandel der Auslegung des Territorialitätsprinzip siehe *Bertele*, Souveränität und Verfahrensrecht, S. 65 ff.

in denen keine festgeschriebenen Regelungsinstrumente greifen, nur durch eine Abwägung der relevanten Staateninteressen möglich ist. Für die Ermittlung des Handlungsorts kommt die Untersuchung zu dem Ergebnis, dass dieser nur dort sein kann, wo der Täter körperlich anwesend ist (nachfolgend unter C.1. und 2.). Der Erfolgstatort ist unter Berücksichtigung der völkerrechtlichen Gesichtspunkte begründet, wo tatbestandsmäßige Verletzungen und konkrete Gefährdungen – nicht jedoch abstrakte Gefahren – eintreten (unter C.3. und 4.).

Für Anbieter von Informations- und Kommunikationsdiensten aus dem EU-Ausland hat das Gemeinschaftsrecht mit dem sogenannten Herkunftslandprinzip der E-Commerce-Richtlinie den Mitgliedstaaten und ihren Strafverfolgungsbehörden auf dem Gebiet des Straf- und Strafverfahrensrechts überdies spezielle Grenzen gesetzt (unter III.). Dem primären und sekundären Gemeinschaftsrecht ist zu entnehmen, dass und inwieweit dieses dort verankerte Prinzip auch im Strafrecht gilt. Aufgrund seines bereits durch die Richtlinie selbst beschränkten Geltungsbereichs und der zahlreichen Umgehungsmöglichkeiten mangels Harmonisierung des materiellen Rechts zeigt sich zwar die geringe Tauglichkeit des Herkunftslandprinzips für das Strafrecht. Soweit es anwendbar ist, kommt ihm in Konstellationen eines Normwiderspruchs aber Vorrang vor den Regelungen des deutschen internationalen Strafrechts zu.

I. Internationale Strafanwendungsregelungen nach nationalem Recht

Zwingende Voraussetzung für die Aufnahme von Ermittlungen in Fällen von im Internet begangenen Straftaten durch deutsche Strafverfolgungsbehörden ist die Anwendbarkeit des deutschen Strafrechts. Die Strafverfolger müssen sich also beispielsweise in Konstellationen, in denen Straftäter bewusst dazu übergehen, nach deutschem Recht strafbare Inhalte über Server im Ausland ins Internet einzuspeisen, um so – zum Teil vermeintlich – der deutschen Strafgewalt zu entgehen,[3] zunächst die Frage nach ihrer Zuständigkeit beantworten. Vor allem für den Deliktstypus des abstrakten Gefährdungsdelikts ist strittig, inwieweit das deutsche Recht auf einen solchen Sachverhalt überhaupt anwendbar ist, wenn der Täter zumindest körperlich im Ausland gehandelt hat. Aufgrund der Struktur des globalen Computernetzwerks können sich Internetnutzer die zum Abruf zur Verfügung gestellten Daten – mangels bisher verlässlicher Methoden einer „Reterritorialisierung des Internet“[4] sowie tatsächlich und rechtlich sicherer Sperrmöglichkeiten[5] – an jedem

---

[3] BMI/BMJ, Zweiter Periodischer Sicherheitsbericht, S. 149; *Fromm*, in: Welp, kriminalität@web, S. 41, 42.

[4] *Hoeren*, MMR 2007, 3, 5 f.; *Lessig/Resnik*, Michigan Law Review, vol. 98, 1999, 395, 399.

Ort der Welt herunterladen, mit der Folge, dass bei strafbaren Handlungen potentiell zu allen Staaten Anknüpfungspunkte bestehen können. Diese Konfliktsituation ist deshalb völkerrechtlich aufzulösen.

Mangels ausschließlicher spezialgesetzlicher Regelungen[6] für die Anwendbarkeit des deutschen Strafrechts auf Internetfälle mit Bezug zum Ausland[7] müssen die Strafverfolgungsbehörden auf die allgemeinen Regelungen des internationalen Strafrechts – §§ 3–7, 9 StGB – zurückgreifen, die nicht in einem Exklusivitätsverhältnis zueinander stehen, sondern sich gegenseitig ergänzen.[8] Normen über die Anwendbarkeit des eigenen Strafrechts können die Staaten unter Beachtung der tragenden Prinzipien des Völkerrechts freiverantwortlich schaffen;[9] die *jurisdiction to prescribe* besteht grundsätzlich territorial uneingeschränkt.[10] Bei der Anwendung der §§ 3–7, 9 StGB müssen die Rechtsanwender jedoch berücksichtigen, dass diese Vorschriften keine mit den Kollisionsnormen des internationalen Privatrechts – Art. 3 ff. EGBGB – vergleichbaren Regelungen beinhalten, sondern einseitige, allein die Anwendbarkeit deutschen Strafrechts regelnde Vorschriften sind.[11] Ausländische (Straf-)Vorschriften bleiben folglich grundsätzlich außer Betracht. Der Begriff „internationales Strafrecht" ist daher missverständlich, weil lediglich die Anwendbarkeit deutschen Rechts auf Straftaten mit Auslandsbezug Regelungsgegenstand ist.[12]

Nach dem in § 3 StGB geregelten Territorialitätsprinzip[13] als Haupt- und Ausgangsprinzip des internationalen Strafrechts unterfallen alle Taten, die innerhalb des Staatsgebiets der Bundesrepublik begangen werden, deren Strafgewalt, gleichgültig von wem sie begangen werden oder wer das Opfer der Tat ist. Der Gebietsgrundsatz ist zum einen Ausdruck der Territorialhoheit und des Selbstschutzinteresses des Staates, zum anderen ermöglicht er eine gerechte Beurteilung der Tat aufgrund ihrer Nähe zu deren sozialen, kulturellen und wirtschaftlichen Hinter-

---

[5] *Sieber/Nolde*, Sperrverfügungen im Internet, S. 228 ff.

[6] Zu Inlandstaten von im EU-Ausland niedergelassenen Diensteanbietern siehe aber auch § 3 TMG und die nachfolgenden Ausführungen in Teil 2, III.

[7] *Barton*, Multimedia-Strafrecht, Rn. 215; *Lehle*, Der Erfolgsbegriff und die deutsche Strafrechtszuständigkeit im Internet, S. 47.

[8] *Lehle*, Der Erfolgsbegriff und die deutsche Strafrechtszuständigkeit im Internet, S. 40.

[9] *Oehler*, Internationales Strafrecht, Rn. 111, Rn. 121; *Römer*, Verbreitungs- und Äußerungsdelikte im Internet, S. 99.

[10] *Bertele*, Souveränität und Verfahrensrecht, S. 102; *Schmidt*, Gefahrenabwehrmaßnahmen im Internet, S. 251.

[11] *Fischer*, StGB, Vor §§ 3–7, Rn. 1; *Lackner/Kühl*, StGB, Vor §§ 3–7, Rn. 1; *Satzger*, Internationales und Europäisches Strafrecht, § 3, Rn. 4.

[12] MünchKommStGB-*Ambos*, Vor §§ 3–7, Rn. 1 f.; S/S-*Eser*, Vorbem. §§ 3–9, Rn. 1, 2, 6.

[13] American Society of International Law, AJIL 29 (1935), 480 ff.; *O'Connor* et al., Model Codes for Post-Conflict Criminal Justice, S. 42; *Oehler*, Internationales Strafrecht, Rn. 153 f. jeweils mit Nachweisen, dass sich das Territorialitätsprinzip in allen Rechtsordnungen weltweit wiederfindet.

gründen.[14] Für die Ermittlung des Tatorts selbst ist § 9 StGB (sog. Ubiquitätsgrundsatz) heranzuziehen. Gemäß §§ 9 Abs. 1, 3 StGB liegt eine Inlandstat vor, wenn entweder der Täter im Inland gehandelt hat oder hätte handeln müssen oder der zum Tatbestand gehörende Erfolg im Inland eingetreten ist oder nach der Vorstellung des Täters dort eintreten sollte.

Aufgrund des in § 5 und § 7 StGB niedergelegten und in das Staats- sowie das Individualschutzprinzip unterteilten Schutz- oder auch Realprinzips ist das deutsche Strafrecht zudem auf im Ausland begangene Taten anwendbar, wenn bestimmte inländische Rechtsgüter gefährdet oder verletzt werden. Das Staatsschutzprinzip (§ 5 Nr. 1, 2, 3b, 4, 5a, 10, 11a StGB) schützt den Staat in seinem Bestand und seiner Handlungsfähigkeit – jene Interessen eines Staates, die fremde Strafrechtsordnungen i.d.R. nicht abdecken. Das sogenannte passive Personalitätsprinzip (Individualschutzprinzip) garantiert indes den eigenen Staatsangehörigen Strafrechtsschutz bei gegen sie gerichteten Auslandstaten, soweit diese auch nach dem Recht des Tatorts strafbar sind (doppelte Strafbarkeit in concreto), § 7 Abs. 1 StGB.

Das aktive Personalitätsprinzip, welches gegenüber der Zeit des Nationalsozialismus seit dem 2. StrRG[15] nur noch in eingeschränkter Form[16] gilt, knüpft in § 7 Abs. 2 Nr. 1, 1. Var. und § 5 Nr. 3a, 5b, 6, 6a, 7, 8, 9, 11, 12, 13, 14, 14a, 15 StGB dagegen an die deutsche Staatsangehörigkeit des Täters an und unterwirft ihn dem deutschen Strafrecht für Taten im Ausland. Soweit die Geltung deutschen Strafrechts von der Strafbarkeit der Tat am Tatort abhängig ist (§ 7 StGB), kommt darin die internationale Solidarität mit der Völkergemeinschaft zum Ausdruck. Wo das Gesetz auf das Erfordernis der lex loci verzichtet (§ 5 StGB), steht das besondere Treueverhältnis zwischen Staat und Bürger im Vordergrund.[17]

In § 6 StGB (Weltrechtsprinzip) legt der deutsche Gesetzgeber sodann fest, welche Rechtsgüter er global schützen will. Die Bestimmung der Rechtsgüter, an deren weltweitem Schutz ein gemeinschaftliches Interesse besteht, ist allerdings nicht immer einfach.[18] Nur selten sind sie in völkerrechtlichen Verträgen eindeutig bezeichnet. Regelmäßig kann allein aus zwischenstaatlichen Abkommen auf den Willen zur internationalen Zusammenarbeit bei der Verfolgung bestimmter Straftaten

---

[14] *Lehle*, Der Erfolgsbegriff und die deutsche Strafrechtszuständigkeit im Internet, S. 40; *Werle/Jeßberger*, JuS 2001, 35, 37.

[15] Vom 4.7.1969, BGBl. I 1969, S. 717, 718 f., geplantes Inkrafttreten zum 1.10.1973, tatsächlich in Kraft gesetzt zum 1.1.1975.

[16] *Jescheck*, in: BMJ, Niederschriften, Bd. 4, S. 12 ff. – zu den Gründen, die zur weitgehenden Abkehr vom aktiven Personalitätsprinzip führten.

[17] *Lehle*, Der Erfolgsbegriff und die deutsche Strafrechtszuständigkeit im Internet, S. 42; *Schmitt*, FS 600 Jahre Würzburger Juristenfakultät, S. 357, 359.

[18] *Hilgendorf*, FS 600 Jahre Würzburger Juristenfakultät, S. 333, 346 ff.; *Kunig*, JuS 1978, 594, 595 f.

geschlossen werden.[19] Da aber der nationale Gesetzgeber weder nach dem kodifizierten Völkerrecht noch nach dem Völkergewohnheitsrecht grundsätzlich an der Regelung seines Strafanwendungsrechts gehindert ist, kann er kraft eigener Entscheidungsgewalt internationale Delikte seiner Strafgewalt unterstellen, soweit er diese Kompetenz nicht willkürlich nutzt.[20] Die Anwendbarkeit des deutschen Strafrechts nach dem Universalprinzip hängt daher nach überwiegender Meinung auch von zwei weiteren ungeschriebenen Voraussetzungen ab:[21] Der Staat darf im konkreten Anwendungsfall nicht gegen ein völkerrechtliches Verbot verstoßen und er muss eine besondere Beziehung zum Regelungsobjekt/-subjekt als sinnvollen Anknüpfungspunkt aufweisen können.

Mit dem letzten Prinzip, dem der stellvertretenden Strafrechtspflege nach § 7 Abs. 2 StGB, stellt der Gesetzgeber sicher, dass bei Verhinderung einer ausländischen Strafjustiz aus tatsächlichen oder rechtlichen Gründen hilfsweise das deutsche Strafrecht – unter näher bestimmten Umständen – eingreift. Der Täter soll nicht straflos bleiben, nur weil eine Strafverfolgung im Ausland nicht stattfindet. Begeht z.B. jemand im Ausland eine Straftat und wird er nach der Tat Deutscher, so unterliegt er dem deutschen Strafrecht, wenn die Tat am Tatort mit Strafe bedroht ist oder der Tatort keiner Strafgewalt unterliegt. Gleiches gilt, wenn ein ausländischer Täter zwar in Deutschland gefasst wurde, aber mangels entsprechenden Antrags nicht ausgeliefert wird.

II. Anwendung der Prinzipien des internationalen Strafrechts auf Internetsachverhalte

Die vorgenannten, in den §§ 3–7, 9 StGB normierten Prinzipien sind auch auf im Internet begangene Taten anwendbar. Jedoch ergeben sich aus der technischen Besonderheit „des Netzes der Netze“, nämlich dass der Täter nur an einem Ort körperlich anwesend ist, sein Handeln aber an unterschiedlichen Orten Auswirkungen haben kann, Probleme bei deren Handhabung, wenn die Anwendbarkeit deutschen Strafrechts vom Territorialitätsprinzip abhängt.

---

[19] *Bremer*, Strafbare Internet-Inhalte in internationaler Hinsicht, S. 226; *Hilgendorf*, FS 600 Jahre Würzburger Juristenfakultät, S. 333, 346 ff.; *Sahlfeld*, Die Veränderung der Ausübung von Staatsgewalt, S. 64.

[20] BGHSt 27, 30, 32 f.

[21] BGHSt 34, 334, 336; *ders.*, NStZ 1994, 232, 233; JR 2000, 202; offen gelassen hingegen vom BVerfG, NStZ 2001, 240, 243; *dass.*, NJW 2001, 1848, 1853; gegen weitere Voraussetzungen: *Ambos*, NStZ 1999, 404, 405; *Eser*, Festgabe 50 Jahre BGH, S. 3, 27 f.; *Werle*, JZ 1999, 1181, 1183; *Werle/Jeßberger*, JuS 2001, 141, 142. Zur Sonderkonstellation der Zuständigkeit nach § 1 VStGB vgl. auch *Ambos*, NStZ 2006, 343, 343 f.

Liegen reine Auslandstaten vor, also wenn sowohl der Handlungs- als auch der Erfolgsort sich nicht im Inland befinden, greifen die §§ 5, 6 und 7 StGB ein. Besondere – mit der Verfolgung von im Internet begangenen Straftaten verbundene – Schwierigkeiten bestehen in diesen Fällen nicht (nachfolgend unter A.). Gleichfalls unproblematisch sind jene Inlandstaten mit Bezug zum Ausland – d.h., entweder der Handlungs- oder der Erfolgsort liegt im Ausland –, in denen der Täter im Inland körperlich handelte bzw. hätte handeln müssen oder im Inland ein tatbestandlich geschütztes Rechtsgut verletzt oder konkret gefährdet (nachfolgend unter B.). Anders verhält es sich dagegen mit den übrigen Inlandstaten, die einen Bezug zum Ausland aufweisen, also wenn der Täter bei der Tatbegehung körperlich im Ausland weilt und im Inland lediglich eine abstrakte Gefahr eintritt (nachfolgend unter C.). Hier wirken sich nicht nur die unterschiedlichen Ansatzpunkte der Auslegung von Handlungs- und Erfolgsort aus (C.1. und 2. sowie 3. und 4.), sondern auch die verschiedenen Standpunkte zur Begrenzung der *jurisdiction to prescribe*, auf welche jeweils später (C.4.a) sowie b)) genauer einzugehen sein wird. Bei Handlungen von im Ausland niedergelassenen Diensteanbietern im Internet müssen die Strafverfolger zudem prüfen, ob für deren strafrechtliche Verfolgung Besonderheiten gelten. Einschlägig kann in diesen Konstellationen das auf der E(lectronic)-Commerce-Richtlinie (ECRL)[22] basierende[23] und in § 3 Abs. 2 Satz 1 TMG[24] umgesetzte sogenannte Herkunftslandprinzip sein (näher unter III.).

A. Reine Auslandstaten

Wie bereits angedeutet, bestehen bei reinen Auslandstaten grundsätzlich keine internetspezifischen Besonderheiten. Liegt weder ein inländischer Handlungs- noch ein inländischer Erfolgstatort nach §§ 3, 9 StGB vor, ist das deutsche Strafrecht nur in den Fällen der §§ 5, 6 und 7 StGB anwendbar.

Beispielhaft für im Internet begangene Straftaten, die unter das Schutzprinzip (§ 5 StGB) fallen, sind die Staatsgefährdungsdelikte i.S.v. §§ 90a, 90b StGB (§ 5 Nr. 3a und b StGB)[25] sowie die Vermittlung des Organhandels i.S.v. § 18 Transplantationsgesetz (§ 5 Nr. 15 StGB)[26] zu nennen. Unter dem Blickwinkel des Welt-

---

[22] Richtlinie über bestimmte rechtliche Aspekte der Dienste der Informationsgesellschaft, insbesondere des elektronischen Geschäftsverkehrs, im Binnenmarkt – Richtlinie 2000/31/EG vom 17.7.2000, ABl. EG 2000, Nr. L 178, S. 1 ff.

[23] Siehe zur Umsetzung der E-Commerce-Richtlinie durch die betroffenen Mitgliedstaaten ins nationale Recht, KOM(2003) 702 vom 21.11.2003, S. 7 ff.

[24] Telemediengesetz vom 26.2.2007, BGBl. I 2007, S. 179 ff., in Kraft getreten am 1.3.2007, zuletzt geändert durch Art. 1 des Gesetzes vom 31.5.2010, BGBl. I 2010, S. 692 ff.

[25] *Römer*, Verbreitungs- und Äußerungsdelikte im Internet, S. 133 f.

[26] S/S-*Eser*, § 9, Rn. 7; *N.N.*, Die Welt, 23.11.2001, „Urteil gegen Nierenanbieter“, 32.

rechtsprinzips (§ 6 StGB) sind insbesondere die Verbreitung von Kinderpornografie gemäß § 6 Nr. 6, § 184b StGB[27] und das Vorbereiten eines Explosions- und Strahlungsverbrechens gemäß § 6 Nr. 2, § 310 StGB von Relevanz.

Greift bei Auslandstaten das Stellvertretungsprinzip (§ 7 StGB) ein, müssen die Strafverfolgungsbehörden auch das Recht des (ausländischen) Tatorts bzw. des dortigen internationalen Strafrechts im Blick haben. Einerseits haben deutsche Gerichte grundsätzlich nur deutsches Recht anzuwenden.[28] Andererseits muss das ausländische Recht bei § 7 StGB berücksichtigt werden, da die Anwendung deutschen Strafrechts davon abhängig sein soll, dass die Tat auch am Tatort mit Strafe bedroht ist. Zunächst ist daher nach deutschem Recht (nach § 9 StGB) zu ermitteln, wo ein Tatort begründet ist. Liegt dieser ausschließlich im Ausland, ist in einem weiteren Schritt zu prüfen, ob die Tat tatsächlich an diesem Ort mit Strafe bedroht ist. Dies wiederum ist nur der Fall, wenn auch nach den Normen des ausländischen internationalen Strafrechts dort ein Tatort begründet und im Übrigen die Tat strafbar ist. In der Praxis kann daher die Bestimmung der Voraussetzungen des § 7 StGB – sowohl wegen der Ermittlung des Tatorts als auch der Eruierung des dortigen Rechts – Schwierigkeiten bereiten, welche aber nicht spezifisch für die Verfolgung von im Internet begangenen Straftaten sind.

B. Inlandstaten mit Auslandsbezug ohne beachtliches völkerrechtliches Konfliktpotenzial

Bei Inlandstaten mit Auslandsbezug ist das deutsche Strafrecht ohne Weiteres anwendbar, wenn der Täter körperlich in Deutschland handelte bzw. im Inland körperlich hätte handeln müssen (§ 3 i.V.m. § 9 Abs. 1, 1. und 2. Var. StGB). Deutsche Strafverfolgungsbehörden sind folglich beispielsweise zuständig, wenn von deutschem Boden Webseiten mit rechtsradikalem Gedankengut ins Internet eingestellt werden und die Inhalte die Straftatbestände der §§ 86, 86a, 130 StGB erfüllen,[29] die Täter Webseiten hochladen, auf denen Anleitungen zum Bombenbau[30] oder anderer Tatwerkzeuge[31] enthalten sind, sodass die Tatbestände der §§ 111, 130a StGB verwirklicht werden können, oder aber Täter sexuelle Handlun-

---

[27] *Kudlich*, in: Merx/Tandler/Hahn, Multimedia-Recht für die Praxis, S. 252; *Ritlewski*, K&R 2008, 94, 96; *Schreibauer*, Das Pornographieverbot des § 184 StGB, S. 95; *Sieber*, JZ 1996, 429, 430 (Fn. 10).

[28] *Werle/Jeßberger*, JuS 2001, 35, 36; *Wessels/Beulke*, Strafrecht AT, Rn. 62.

[29] OLG Frankfurt NStZ 1999, 356 ff.; für einen weiteren Fall siehe http://www.theregister.co.uk/2004/05/10/hate_websites_flourish/ [Stand: 6.11.2013].

[30] Dafür, dass diese Anleitungen verwendet werden siehe: http://www.welt.de/print-welt/article416122/Motiv_des_finnischen_Attentaeters_raetselhaft.html [Stand: 6.11.2013] und http://www.welt.de/print-wams/article109945/Bauchladen_des_Allerschrecklichsten.html [Stand: 6.11.2013].

[31] BayObLG NJW 1998, 1087, 1087 f. (Anleitung zum Bau eines Molotow-Cocktails).

gen im Inland an sich vornehmen und Kinder im Ausland dazu veranlassen, sich diese gleichzeitig über Webcams anzusehen (§ 176 Abs. 4 Nr. 1 StGB).[32]

Darüber hinaus besteht im Wesentlichen Einigkeit über die Anwendbarkeit des deutschen Strafrechts in Fällen, in denen der Täter ein Erfolgsdelikt im Ausland begeht und der tatbestandsmäßige Erfolg (die Rechtsgutverletzung) im Inland[33] eintritt, da dann ein Erfolgsort nach § 9 Abs. 1, 3. Var. StGB im Inland (§ 3 StGB) gegeben ist.[34] Ein solcher liegt etwa vor, wenn durch einen im Ausland ins Netz eingespeisten Computervirus in Deutschland Daten zerstört werden[35] (§ 303a Abs. 1 StGB)[36] oder die Datenverarbeitung, die für einen anderen von wesentlicher Bedeutung ist, durch rechtswidrige Veränderung der Daten erheblich gestört wird[37] (§ 303b Abs. 1 StGB).[38]

Bei konkreten Gefährdungsdelikten, die ebenso zu den Erfolgsdelikten zählen,[39] ist das deutsche Strafrecht nach nahezu einhelliger Ansicht desgleichen anwendbar, wenn ein Erfolgsort im Inland gegeben ist. Dieser ist dort zu finden, wo sich die Gefahr konkretisiert, also wo die vom Handeln abgrenzbare Wirkung nach außen durch das Eintreten der hinreichenden Gefahr entsteht.[40] Deutsche Strafverfolgungsbehörden sind danach z.B. zuständig, wenn Staatsgeheimnisse (etwa Geheimdokumente wie Notfallpläne) im Internet veröffentlicht werden und dadurch die Gefahr eines schweren Nachteils für die äußere Sicherheit der Bundesrepublik Deutschland herbeigeführt wird (§ 95 StGB).

---

[32] BGH MMR 2009, 533, 534.

[33] Zum Umfang des Inlandsgebiets siehe *Fischer*, StGB, Vor §§ 3 bis 7, Rn. 12–19.

[34] MünchKommStGB-*Ambos*, § 9, Rn. 19.

[35] Zum „I love You"-Virus, der Daten auf Computern weltweit veränderte, siehe http://www.welt.de/print-welt/article513159/Computer-Virus_verursacht_Milliarden-Schaeden.html [Stand: 6.11.2013].

[36] Zur materiell-rechtlichen Beurteilung noch nach der alten Fassung des § 303a Abs. 1 StGB *Heghmanns*, in: Achenbach/Ransiek, HWSt^{2}, VI 1, Rn. 137; *Preuße*, Informationsdelikte im Internet, S. 76 ff., 84, 104, 113; zur neuen Fassung vgl. *Gröseling/Höfinger*, MMR 2007, 626 ff.

[37] Zum Zusammenbruch von Computersystemen durch die Versendung eines Wurms, der in Weihnachtsgrüßen mit einem Weihnachtsbaum per E-Mail enthalten war, siehe *Claas Wolter/Holger Pinnow*, WWWeihnachten im World Wide Web, Berliner Morgenpost, 24.12.2000.

[38] Zur materiell-rechtlichen Beurteilung noch nach der alten Fassung des § 303b Abs. 1 StGB *Heghmanns*, in: Achenbach/Ransiek, HWSt^{2}, VI 1, Rn. 172; *Preuße*, Informationsdelikte im Internet, S. 105 ff., 113, 133 f.; zur neuen Fassung vgl. *Gröseling/Höfinger*, MMR 2007, 626 ff.

[39] So die ganz h.M.: *Graul*, Abstrakte Gefährdungsdelikte und Präsumtionen im Strafrecht, S. 24, Fn. 32 m.w.N.; *Roxin*, Strafrecht AT I, § 10, Rn. 124, § 11, Rn. 147 ff.; a.A. *Koriath*, GA 2001, 51, 60 mit dem nicht überzeugenden Argument, dass eine konkrete Gefahr noch kein Erfolg im Wortsinn ist.

[40] MünchKommStGB-*Ambos*, § 9, Rn. 19, 27; *Fischer*, StGB, § 9, Rn. 4c f.; LK-StGB^{12}-*Werle/Jeßberger*, § 9, Rn. 27.

C. Inlandstaten mit Auslandsbezug mit erheblichem völkerrechtlichem Konfliktpotenzial

Schwierigkeiten bei der Bestimmung eines Tatorts in Deutschland ergeben sich jedoch bei abstrakten Gefährdungsdelikten, wenn der Täter körperlich im Ausland handelt. Zum einen liegt in diesen Fällen jedenfalls kein körperliches Handeln im Inland vor und zum anderen ist umstritten, inwieweit abstrakte Gefährdungsdelikte überhaupt einen tatbestandlichen Erfolg i.S.d. § 9 Abs. 1, 3. Var. StGB aufweisen. Die Untersuchung der Anwendbarkeit des deutschen Strafrechts auf diese Fallkonstellationen ist praktisch besonders bedeutsam, da über das Internet begangene Straftaten häufig abstrakte Gefährdungsdelikte sind. Relevant wird dieses Problem beispielsweise, wenn rechtsradikale Inhalte über Server in den USA ins Internet eingestellt werden.[41] Durch das First Amendment zur US-amerikanischen Verfassung als Meinungsfreiheit geschützte,[42] in Deutschland aber regelmäßig strafbare Inhalte – etwa die Billigung, Leugnung oder Verharmlosung von NS-Gewalttaten – können auch in Deutschland abgerufen werden. So ist die Homepage des Deutschen *Ernst Zündel*, eines der führenden Revisionisten, – auch nachdem das Canadian Human Rights Tribunal den Betrieb der Webseite über kanadische Server untersagte[43] – über die USA weiterhin in Deutschland abrufbar.[44] Einen anderen praktischen Fall für die Begehung abstrakter Gefährdungsdelikte[45] im Internet stellen die vom Ausland – insbesondere aus Karibikstaaten – unter Umgehung der strengeren Regelungen des deutschen Rechts ins Internet gestellten Glücksspiele dar.[46] Vom heimischen Computer kann der Nutzer in Deutschland nach dem Herunterladen der Software und Angabe der Kreditkartendaten am Glücksspiel teilnehmen.

---

[41] *Bremer*, Strafbare Internet-Inhalte in internationaler Hinsicht, S. 162; *N.N.*, Die Welt, 11.4.2001, „Schily erwägt Attacken gegen Nazi-Sites“, WW1; *N.N.*, Die Welt, 30.3.2001, „Zahl rechtsextremer Straftaten steigt weiter an“, 4.

[42] *N.N.*, Die Welt, 4.4.2001, „Abtreibungsgegner in den USA dürfen weiter online hetzen“, WW2 – zu einem weiteren Fall, der die Reichweite des Schutzes der Meinungsfreiheit durch das First Amendment beschreibt; siehe dazu ebenfalls die amerikanischen Rechtsprechungsnachweise bei *Holznagel*, AfP 2002, 128, 129 f.; *Mayer*, NJW 1996, 1782, 1788, Fn. 80.

[43] Canadian Human Rights Tribunal in Sachen *Sabina Citron and Toronto Mayor's Committee on Community and Race Relations vs. Ernst Zündel*, Urteil vom 18.1.2002, Az. T.D. 1/02, S. 101, abrufbar unter: http://www.chrt-tcdp.gc.ca/search/files/t460_1596de.pdf [Stand: 6.11.2013].

[44] BfV, Rechtsextremistische Bestrebungen im Internet, S. 34; *N.N.*, Der Spiegel, 13/1996, „Angst vor der Anarchie“, 132, 136.

[45] Zur Einordnung des Veranstaltens eines Glücksspiels als abstraktes Gefährdungsdelikt nach der h. M. siehe S/S-*Eser/Heine*, § 284, Rn. 2c m.w.N.

[46] BGH MMR 2004, 529 ff.; *Klam*, Die rechtliche Problematik von Glücksspielen im Internet, S. 123 ff.; *Klengel/Heckler*, CR 2001, 243 ff.; *Leupold/Bachmann/Pelz*, MMR 2000, 648 ff.; *Volk*, Glücksspiel im Internet, S. 186 ff.

Die Frage nach der Anwendbarkeit des deutschen Strafrechts und damit der Zuständigkeit deutscher Strafverfolgungsbehörden bei der Verwirklichung abstrakter Gefährdungsdelikte durch extraterritoriales Handeln des Täters wird unterschiedlich beantwortet. Eine Meinungsgruppe versucht, über die Bestimmung eines Handlungsorts i.S.d. § 9 Abs. 1, 1. Var. StGB jenseits der körperlichen Anwesenheit des Täters einen inländischen Tatort zu begründen (nachfolgend unter 1. und 2.). Demgegenüber prüft eine zweite Meinungsgruppe, ob über die Regelung des § 9 Abs. 1, 3. Var. StGB durch Bestimmung eines Erfolgsorts eine Antwort auf die aufgeworfene Frage zu finden ist (unter 3. und 4.).

1. Handlungsort im Inland trotz physischer Abwesenheit

Die Teile der Literatur[47] und der Rechtsprechung,[48] welche die Frage nach der Anwendbarkeit des deutschen Strafrechts auf im Internet begangene Taten, in denen der Täter körperlich im Ausland handelte, durch Anknüpfung an den Handlungsort beantworten wollen, sprechen sich für eine Erweiterung des Handlungsorts i.S.d. § 9 Abs. 1, 1. Var. StGB aus.

Sie nehmen einen Handlungsort i.S.d. § 9 Abs. 1, 1. Var. StGB unter bestimmten Bedingungen in Deutschland auch dann an, wenn der Täter rein körperlich tatsächlich nur im Ausland handelte. Überträgt der Täter bewusst vom Ausland Daten auf einen in Deutschland installierten Server, soll er auch in Deutschland tätig sein.[49] Der Computer wäre nach dieser Ansicht also der „technisch verlängerte Arm“ des Täters, durch den er am Standort des Computers handelt. Zum gleichen Ergebnis

---

[47] *Cornils*, JZ 1999, 394, 396 f.; *dies.*, in: Hohloch, Recht und Internet, S. 71, 79 ff.; S/S-*Eser*, § 9, Rn. 4; *ders.*, Festgabe 50 Jahre BGH, S. 3, 23 f.; *Götting*, Kriminalistik 2007, 615, 618; *Graf*, in: Heermann/Ohly, Verantwortlichkeit im Netz, S. 85, 95; *Klam*, Die rechtliche Problematik von Glücksspielen im Internet, S. 52; *Leidenmühler/Plöckinger*, in: Plöckinger/Duursma/Helm, Aktuelle Entwicklungen im Internet-Recht, S. 101, 110 (für Österreich); *dies.*, in: Plöckinger/Duursma/Mayrhofer, Internet-Recht, S. 363, 373 (für Österreich), die zusätzlich zwischen Pull- und Push-Technologien differenzieren; *Marberth-Kubicki*, Computer- und Internetstrafrecht, S. 25, Rn. 47; *Plöckinger*, ÖJZ 2001, 798, 802 (für Österreich); *Schmitt*, in: Eberle/Rudolf/Wasserburg, Mainzer Rechtshandbuch der Neuen Medien, Kapitel XI, Rn. 7; *ders.*, FS 600 Jahre Würzburger Juristenfakultät, S. 357, 366; *Werle/Jeßberger*, JuS 2001, 35, 39.

[48] KG NJW 1999, 3500, 3502.

[49] *Cornils*, JZ 1999, 394, 397; *dies.*, in: Hohloch, Recht und Internet, S. 71, 80; zustimmend S/S-*Eser*, § 9, Rn. 4; *ders.*, Festgabe 50 Jahre BGH, S. 3, 24 und Fn. 93; *Götting*, Kriminalistik 2007, 615, 618 f.; *Graf*, in: Heermann/Ohly, Verantwortlichkeit im Netz, S. 85, 95; *Klam*, Die rechtliche Problematik von Glücksspielen im Internet, S. 52, 207 f.; siehe außerdem *Kioupis*, in: Anagnostopoulos, Internationalisierung des Strafrechts, S. 93, 110 f. (für Griechenland); *Leidenmühler/Plöckinger*, in: Plöckinger/Duursma/Helm, Aktuelle Entwicklungen im Internet-Recht, S. 101, 110 f.; *dies.*, in: Plöckinger/Duursma/Mayrhofer, Internet-Recht, S. 363, 373 (für Österreich); *Marberth-Kubicki*, Computer- und Internetstrafrecht, S. 25, Rn. 47; *Plöckinger*, ÖJZ 2001, 798, 802 (für Österreich); *Schmitt*, in: Eberle/Rudolf/Wasserburg, Mainzer Rechtshandbuch der Neuen Medien, Kapitel XI, Rn. 7; *ders.*, FS 600 Jahre Würzburger Juristenfakultät, S. 357, 366.

kommt eine Literaturansicht, die bei der Abgrenzung zwischen positivem Tun und Unterlassen das Tun zulasten des Unterlassens weit auslegt und zur Handlung des Täters auch den „maschinellen Energieeinsatz“ rechnet.[50] Wenn danach eine Handlung über die unmittelbare Körperbewegung hinaus auch den aktuell vom Täter beherrschten maschinellen Energieeinsatz erfassen soll, also beispielsweise die vom Täter durch Computereingaben initiierten Aktivitäten, müsste konsequenterweise ebenso dort ein Handlungsort liegen, wo der genannte Energieeinsatz sich auswirkte.

Ähnlich geht ein Teil der Rechtsprechung – allerdings in einem anderen Zusammenhang – vor, wenn er von einer teilweisen Verwirklichung einer Handlung im Inland bei körperlicher Anwesenheit im Ausland spricht, soweit die Wirkungen des Täterverhaltens, die nach der tatbestandlichen Handlungsbeschreibung als deren Bestandteil zu betrachten sind, im Inland eintreten.[51] Die höchstrichterliche Rechtsprechung ließ die Frage nach der Begründung eines inländischen Handlungsorts für den Inhalteanbieter, wenn ein Nutzer im Inland Inhalte von einem ausländischen Server abruft und damit Dateien nach Deutschland „herunterlädt“, bei einer Entscheidung aus dem Jahr 2001 unter Anmeldung von Bedenken dagegen offen.[52]

Konsequenz dieser Gruppe von Meinungen ist immer, dass das deutsche Strafrecht auf Straftaten im Internet – auch wenn diese als abstrakte Gefährdungsdelikte ausgestaltet sind – schon aufgrund eines Handlungsorts in Deutschland unter den dargestellten Voraussetzungen anwendbar wäre.

2. Physische Anwesenheit als Voraussetzung der Handlung

Die Begründung eines Handlungsorts unabhängig von der körperlichen Anwesenheit des Täters im oben dargestellten Sinne ist jedoch aus den nachfolgenden Gründen abzulehnen. Der Handlungsort i.S.d. § 9 Abs. 1, 1. Var. StGB ist allein der Ort, an dem der Täter handelte und körperlich anwesend war.[53]

a) Grammatische Auslegung

Der Begriff der Handlung leitet sich von dem Verb „handeln“ ab. Ursprünglich hatte „handeln“ die Bedeutung von „greifen“, „ergreifen“ oder „befühlen“. Später

---

[50] *Altenhain*, CR 1997, 485, 488 ff.

[51] KG NJW 1999, 3500, 3502 – für das Zeigen des Hitlergrußes bei einem Fußballspiel im Ausland, das im Fernsehen auch nach Deutschland übertragen wurde.

[52] BGHSt 46, 212, 224 f. = BGH NJW 2001, 624, 628.

[53] *Fischer*, StGB, § 9, Rn. 3; *Germann*, Gefahrenabwehr und Strafverfolgung im Internet, S. 230; *Poenig*, Die strafrechtliche Haftung des Linkanbieters, S. 134, 135, 174; *Schmidt*, Gefahrenabwehrmaßnahmen im Internet, S. 253; *Sieber*, NJW 1999, 2065, 2067 i.V.m. 2070.

fand das Wort Verwendung als Synonym für „übertragen“ oder „behandeln“. Schlussendlich wurde im Deutschen von einem Handeln gesprochen, wenn etwas verrichtet oder getan wurde.[54] Im allgemeinen Sprachgebrauch wird der Begriff der Handlung heute benutzt, um eine Tätigkeit zu beschreiben.[55] Unter einer Handlung ist daher eine bewusste menschliche Betätigung zu verstehen, die eine Wirkung auf die Umwelt ausübt. Die in der Umwelt zu verzeichnende Wirkung ist dagegen nicht mehr allein dem menschlichen Willen unterworfen, sondern durch Naturgesetze bestimmt und damit zumindest als Teilerfolg und Anfang einer Kausalkette zu begreifen. Das vorgestellte Handlungsziel sowie der eingetretene Handlungserfolg sind von der Tätigkeit „Handeln“ abgrenzbar.

Mit dieser Differenzierung von Handlung und Erfolg ist regelmäßig die Anknüpfung der Handlung an den körperlichen Standort des Täters verbunden. Der Ort, an dem der Täter gehandelt hat, wird grundsätzlich von dem Ort, an dem die durch das Handeln hervorgerufenen Wirkungen eingetreten sind, unterschieden. Die Ansicht, dass der Handlungsort in den Fällen der Nutzung des Internet im Einzelfall auch dort liege, wo der Täter durch seine Handlung eine Wirkung hervorruft, ohne an diesem Ort körperlich anwesend zu sein,[56] entspricht folglich grundsätzlich nicht dem allgemeinen Sprachgebrauch. Ein anderes Verständnis des Handlungsbegriffs durch eine Legaldefinition im Strafgesetzbuch hat der Gesetzgeber nicht vorgegeben.

Eine weitergehende Auslegung des Handlungsbegriffs im Sinne der oben dargestellten Ansicht sprengt gleichwohl noch nicht den Wortsinn des Begriffs der Handlung, sodass die aus Art. 103 Abs. 2 GG folgende unumstößliche Auslegungsgrenze[57] nicht überschritten wäre. Eine scharfe Trennung zwischen Handlung und Erfolg wird in der Alltagssprache nämlich nicht immer vorgenommen. Der Wortsinn des Begriffs der Handlung kann in der Umgangssprache auch über den körperlichen Standort des Täters hinausgehen und das Ergebnis eines menschlichen Handelns beschreiben.[58] Zündet der Täter beispielsweise eine Bombe fern, wird üblicherweise davon gesprochen, dass er „etwas in die Luft sprengte“. Der Erfolg,

---

[54] *Kluge*, Etymologisches Wörterbuch der deutschen Sprache, S. 391, Stichwort handeln.

[55] Duden, Das große Wörterbuch der deutschen Sprache, Bd. 3, S. 1467, Stichwort Handlung.

[56] *Cornils*, JZ 1999, 394, 396 f.; *dies.*, in: Hohloch, Recht und Internet, S. 71, 79 ff.; S/S-*Eser*, § 9, Rn. 4; *ders.*, Festgabe 50 Jahre BGH, S. 3, 23 f.; *Götting*, Kriminalistik 2007, 615, 618; *Klam*, Die rechtliche Problematik von Glücksspielen im Internet, S. 52; *Schmitt*, in: Eberle/Rudolf/Wasserburg, Mainzer Rechtshandbuch der Neuen Medien, Kapitel XI, Rn. 7; *ders.*, FS 600 Jahre Würzburger Juristenfakultät, S. 357, 366; *Werle/Jeßberger*, JuS 2001, 35, 39.

[57] BVerfGE 47, 109, 121, 124.

[58] Duden, Das große Wörterbuch der deutschen Sprache, Bd. 3, S. 1467, Stichwort Handlung.

die Sprengung selbst, wird als eine Tätigkeit beschrieben, obwohl zwischen dem Drücken des Auslösers und der Zündung sogar eine kurze Zeitverzögerung liegt.

Der Beispielsfall der Fernzündung einer Bombe ist in seinen zeitlichen Abläufen vergleichbar mit der Speicherung von Daten auf einen fernen Server. Der Täter bedient seinen Rechner, an dem er die Befehle eingibt, und den Rechner, auf welchem er aufgrund der Befehlseingaben Veränderungen hervorruft, nicht gleichzeitig. Erst nach einer (praktisch vielleicht kaum wahrnehmbaren) zeitlichen Abfolge von Befehlseingabe, Datenübertragung und -empfang tritt eine Wirkung am Zielrechner ein.[59] Wenn auch in der Praxis nicht immer wahrnehmbar, so erfolgen technisch betrachtet die Ereignisse also nicht gleichzeitig. Soweit die vorstehend beschriebene umgangssprachliche Ausdehnung der Handlung auf den Erfolg auf einen zeitlichen Gleichlauf der Ereignisse gestützt wird,[60] widerspricht dies also zumindest den technischen Gegebenheiten.

b) Historische Auslegung

Das Gesetz selbst unterscheidet in der geltenden Fassung des § 9 Abs. 1 StGB, der auf das zweite Gesetz zur Reform des Strafrechts zurückgeht,[61] ausdrücklich zwischen Handlungs- und Erfolgsort. Im Reichsstrafgesetzbuch fand sich demgegenüber in § 3 RStGB lediglich die Regelung:

> „Die Strafgesetze des Deutschen Reiches finden Anwendung auf alle im Gebiete desselben begangenen strafbaren Handlungen […].“[62]

Infolge der gesetzlichen Beschränkung durch die ausschließliche Anknüpfung an strafbare Handlungen in § 3 RStGB waren die Rechtsprechung[63] und Teile der damaligen Literatur[64] ebenfalls bestrebt, den Begriff der Handlung weit zu fassen, um eine umfängliche Bestrafung nach deutschem Recht zu gewährleisten.[65] Nach Ansicht des Reichsgerichts schloss die Handlung deshalb nicht mit der persönlichen Tätigkeit ab. Zum Tatbestand der strafbaren Handlung sei vielmehr sowohl die Tätigkeit als auch die beabsichtigte Wirkung zu rechnen.[66] Bilde nicht nur das formelle Tun den Gegenstand eines Strafgesetzes, so gehöre auch die Wirkung der Tätigkeit zur Handlung im strafrechtlichen Sinne. Daher ziehe sich die Handlung

---

[59] *Bremer*, Strafbare Internet-Inhalte in internationaler Hinsicht, S. 113; *Freund*, Die Strafbarkeit von Internetdelikten, S. 74 f. (für Österreich).

[60] So *Cornils*, JZ 1999, 394, 396; *dies.*, in: Hohloch, Recht und Internet, S. 71, 79.

[61] 2. StrRG vom 4.7.1969, BGBl. I 1969, S. 717, 719 in Kraft getreten am 1.1.1975, BGBl. I 1973, S. 909.

[62] RGBl. I 1871, S. 127, 128.

[63] RGSt 1, 274, 276; 3, 316, 318; 11, 20, 22; 48, 138, 141.

[64] Zur Darstellung der damaligen Meinungsvertreter LK-StGB[1]-*Ebermayer* et al., § 3, Nr. 7; *Kitzinger*, Ort und Zeit der Handlung im Strafrecht, S. 41 f.

[65] RGSt 11, 20, 22; LK-StGB[1]-*Ebermayer* et al., § 3, Nr. 7; zur Problematik im Vergleich zu anderen Staaten American Society of International Law, AJIL 29 (1935), 494 ff.

[66] RGSt 1, 274, 276.

so lange hin, wie ihre Wirksamkeit andaure.[67] Im Fall des Eintritts der beabsichtigten Wirkung an einem anderen Ort als dem, an dem der Täter persönlich tätig geworden ist, lasse sich die zum Tatbestand der Handlung gehörende Wirkung nicht ausscheiden, um den Ort der begangenen Handlung allein nach dem Ort zu bestimmen, an welchem der Täter seine persönliche Tätigkeit entwickelt habe.[68] Das Reichsgericht räumte sodann zwar auch ein, dass der Begriff „Handlung" zweideutig sein könne. Bei enger Auslegung falle unter die Handlung nur die durch den Willen verursachte körperliche Bewegung. Bei weiter Auslegung umfasse aber die Handlung neben der Tätigkeit auch deren Erfolg.[69] Die Richtigkeit letzterer Auslegung ergäbe sich jedoch schließlich „zur vollen Evidenz aus dem Beiwort ‚strafbare'".[70] Strafbar sei die Handlung nämlich erst durch ihre rechtsverletzende Wirkung, sodass der Erfolg zur strafbaren Handlung zähle und damit der Ort des Eintritts des Erfolgs ebenfalls Anknüpfungspunkt für die Anwendung deutschen Strafrechts sein könne.[71]

Der vom Reichsgericht und Teilen der damaligen Literatur vorgenommenen weiten Auslegung des Handlungsbegriffs traten jedoch andere Literaturvertreter dieser Zeit bereits entgegen. Nach ihrer Ansicht umfasste der Handlungsbegriff nur die rein körperliche Tätigkeit und nicht den durch diese hervorgerufenen Erfolg.[72] Da eine ausschließliche Anknüpfung der Anwendbarkeit des deutschen Strafrechts an den Ort der körperlichen Handlung aber zu unbefriedigenden Ergebnissen führen konnte, forderten manche Vertreter einen Zusatz zur Regelung des § 3 RStGB.[73] Unter anderem schlugen sie vor, den Zusatz wie folgt zu fassen:

> „Begangen ist die Handlung an jedem Ort, an dem der Täter gehandelt hat oder zu handeln versucht hat oder an dem Wirkungen seiner Handlung eingetreten sind (eventuell: oder nach seinem Vorsatz eintreten sollten), es sei denn, das diese Wirkungen im Inland befindliche Rechtsgüter weder verletzt noch gefährdet haben. […]."[74]

Unter dem Eindruck vorgenannter Streitigkeiten fasste der Gesetzgeber im Jahr 1940 § 3 RStGB deshalb neu, indem er in Abs. 3 die Regelung aufnahm:

> „Eine Tat ist an jedem Ort begangen, an dem der Täter gehandelt hat oder im Falle des Unterlassens hätte handeln sollen oder an dem der Erfolg eingetreten ist oder eintreten sollte."[75]

---

67 RGSt 3, 316, 318.

68 RGSt 1, 274, 276.

69 RGSt 11, 20, 21.

70 Ebenda, 22.

71 Ebenda.

72 Zur Darstellung damaliger Meinungsvertreter *Kitzinger*, Ort und Zeit der Handlung im Strafrecht, S. 38 ff.

73 *Köhler*, in: Zusammenstellung der gutachterlichen Äußerungen über den Vorentwurf zu einem Deutschen Strafgesetzbuch, S. 5.

74 *Kantorowicz*, in: Zusammenstellung der gutachterlichen Äußerungen über den Vorentwurf zu einem Deutschen Strafgesetzbuch, S. 5.

75 Neufassung des § 3 StGB durch die GeltungsbereichsVO vom 6.5.1940, RGBl. I 1940, S. 754.

Mit dieser Änderung stellte der Gesetzgeber, der damals überwiegend vertretenen Einheitstheorie folgend, den Erfolgseintritt und die Handlung auf eine Stufe.[76] Die Gleichstellung von Handlungs- und Erfolgsort als Tatorte übernahm im Folgenden auch die Regelung des § 9 StGB, die nach den Begründungen zu den Entwürfen eines Strafgesetzbuches E 1960[77] und E 1962[78] zu § 8 StGB-Entwurf die Ergebnisse der Rechtsprechung „verdeutlichen" sollte.

Die historische Auslegung spricht im Ergebnis also für eine enge Auslegung des Begriffs der Handlung. Der Gesetzgeber selbst sah sich veranlasst, den Gesetzestext für die Bestimmung des Tatorts neu zu fassen. Einerseits wollte er an der Rechtsprechung des Reichsgerichts festhalten; andererseits fand er die Auslegung der Rechtsprechung nicht im Gesetzestext des § 3 RStGB verankert. Das geltende Gesetz spricht daher in § 9 StGB auch nicht mehr wie in § 3 RStGB von einer „strafbaren Handlung", sondern von „der Tat". Mit der Anknüpfung an den Begriff der Tat sowie parallel hierzu der Gleichstellung der Orte der Handlung und des Erfolgs als Tatorte in § 9 StGB folgt der Gesetzgeber einer engen Auslegung des Handlungsbegriffs. Bei Loslösung des Handlungsorts von der körperlichen Anwesenheit des Täters und der Bejahung eines Handlungsorts im Inland auch dort, wo der Täter vom Ausland Daten auf einen inländischen Server speichert, bestünde mangels eines konkreten Abgrenzungskriteriums ebenso wie schon zu Zeiten des Reichsstrafgesetzbuchs die Gefahr einer uferlosen Weite des Handlungsbegriffs. Da nunmehr aber die Trennung zwischen Handlung und Erfolg gesetzlich vollzogen ist, besteht kein Bedarf mehr, den Erfolg gleichfalls unter den Begriff der strafbaren Handlung zu subsumieren.

c) Systematische Auslegung

Gegen die Annahme eines Handlungsorts am Serverstandort spricht des Weiteren die systematische Auslegung, die aufzeigt, dass sowohl unter Berücksichtigung der Systematik des § 9 StGB (nachfolgend unter aa)) als auch der Regeln des Versuchs und des Rücktritts (unter bb)) sowie der mehraktigen Deliktstatbestände (unter cc)) eine enge Auslegung des Handlungsorts vorzunehmen ist. Bestätigung findet dieses Ergebnis in europäischen und internationalen Lösungsansätzen für das Problem positiver Kompetenzkonflikte, die ebenfalls primär an dem physischen Standort des Täters im Tatzeitpunkt ansetzen (unter dd)).

---

[76] LK-StGB[6]-*Nagler/Schinnerer*, § 3, Nr. 11.

[77] BT-Drucks. III/2150, S. 107.

[78] BT-Drucks. IV/650, S. 113.

aa) Sonderregelungen für Teilnahme- und Täterschaftsformen

In den Fällen der Tatbeteiligung mehrerer sieht das Gesetz einen vom Ort der Anwesenheit abweichenden Handlungsort nur in einzelnen gesetzlich bestimmten Konstellationen vor. Eine ausdrückliche Regelung für eine solche Zurechnung von Handlungsorten findet sich in § 9 Abs. 2 StGB. Danach ist u.a. die Teilnahme sowohl an dem Ort begangen, an dem die Tat begangen ist, als auch an jedem Ort, an dem ein Teilnehmer gehandelt hat. Jeder Beteiligte trägt die Verantwortung für jede in den Rahmen des gewollten Zusammenwirkens fallende Tätigkeit des bzw. der jeweils anderen.[79] Die Norm gilt jedoch nur für die Teilnahmeformen Anstiftung und Beihilfe.

Für die Beteiligungsformen der Täterschaft (mittelbare Täterschaft und Mittäterschaft) sieht das Gesetz zwar keine vergleichbare (ausdrückliche) Regelung vor. Die Zurechnung des Handlungsorts ergibt sich hier aber bereits aus § 25 Abs. 1, 2. Var. bzw. Abs. 2 StGB. Bei mittäterschaftlicher Begehung werden die durch die einzelnen Mittäter begründeten Handlungsorte den jeweils anderen nach § 25 Abs. 2 StGB zugerechnet,[80] wobei selbst dort ein Tatort begründet wird, wo sich das Handeln eines Mittäters auf Tatbeiträge beschränkt, die für sich gesehen nur Vorbereitungshandlungen sind.[81] Im Fall der mittelbaren Täterschaft, also wenn der Täter z.B. – statt eines Computers – einen Menschen als Werkzeug für seine Tat nutzt, ist der Handlungsort des menschlichen Werkzeugs ebenfalls Handlungsort des mittelbaren Täters im rechtlichen Sinne.[82] Das Gesetz bestimmt in § 25 Abs. 1, 2. Var. StGB eine Zurechnung (zumindest) der Werkzeughandlung und damit auch eine Zurechnung des Handlungsorts des Tatmittlers.

Überträgt der Täter Daten auf einen Server, so bedient er sich im Gegensatz zu den vorstehenden Konstellationen keines weiteren Menschens, insbesondere keines menschlichen Werkzeugs i.S.d. § 25 Abs. 1, 2. Var. StGB. Die Auffassung, dass bei der Speicherung von Inhalten auf einem inländischen Server der (Host-) Provider als Tatmittler anzusehen sei und daher ein inländischer Handlungsort begründet werde,[83] trifft nicht zu, da durch den mit den Tastatureingaben des Täters angesprochenen Server nur die technischen Grundlagen zur Speicherung und Weiterleitung der Daten zur Verfügung gestellt werden.[84] Zu durch einen Dritten veran-

---

[79] RGSt 11, 20, 23.

[80] BGHSt 39, 88, 90; MünchKommStGB-*Ambos*, § 9, Rn. 10; *Hombrecher*, JA 2010, 637, 639.

[81] BGH NStZ-RR 2009, 197, 197.

[82] RGSt 11, 20, 23; 67, 130, 138; BGH wistra 1991, 135; OLG Schleswig wistra 1998, 30, 31; MünchKommStGB-*Ambos*, § 9, Rn. 10; NK-StGB-*Böse*, § 9, Rn. 5; LK-StGB[12]-*Werle/Jeßberger*, § 9, Rn. 14; a.A. SK-StGB-*Hoyer*, § 9, Rn. 5, der allein auf den Ort der Entlassung des Werkzeugs aus dem Einflussbereich des mittelbaren Täters abstellt.

[83] *Heghmanns*, in: Achenbach/Ransiek, HWSt[3], Rn. 7.

[84] *Germann*, Gefahrenabwehr und Strafverfolgung im Internet, S. 230.

lassten Handlungen des Providers als dessen Werkzeug kommt es nicht. Es fehlt an einem vom Täter zur Steuerung des Providers eingesetzten Instrument, das für eine Tatbegehung „durch" einen anderen i.S.d. § 25 Abs. 1, 2. Var. StGB unverzichtbar ist. Denkbar ist allenfalls die Zurechnung eines Tatorts nach § 9 Abs. 2 StGB aufgrund einer Strafbarkeit des Providers wegen Beihilfe. Aber selbst wenn eine solche auch bei neutralen Verhaltensweisen in Betracht käme,[85] wären die §§ 7 ff. TMG[86] (vormals §§ 8 ff. TDG[87] und §§ 6 ff. MDStV[88]) zu beachten, die gesetzliche Sonderregelungen für die Haftung von Providern enthalten, die regelmäßig zu einer Privilegierung der allein beruflich veranlassten und nicht an deliktischen Zwecken ausgerichteten Handlungen führen.[89] Unabhängig von der Einordnung dieser Regelungen als Vorfilter,[90] Tatbestandsmerkmal[91] bzw. „neue[r] Kategorie

---

[85] Die Strafbarkeit bejahen – wegen ihrer generellen Ablehnung einer Sonderstellung neutraler Beihilfehandlungen – z.B. *Beckemper*, Jura 2001, 163, 163 ff.; *Niedermair*, ZStW 107 (1995), 507, 543 f.; zur strafrechtlichen Behandlung neutraler Beihilfehandlungen im Allgemeinen siehe zusammenfassend jeweils m.w.N. S/S-*Heine*, § 27, Rn. 10a ff.; *Kudlich*, Die Unterstützung fremder Straftaten durch berufsbedingtes Verhalten, S. 68 ff.; *Roxin*, Strafrecht AT II, § 26, Rn. 218 ff.; im Besonderen bei der Verantwortlichkeit von Providern *Derksen*, NJW 1997, 1878, 1882 f.; *Heß*, Die Verantwortlichkeit von Diensteanbietern, S. 76 ff.; *Kudlich*, JA 2002, 798, 800 ff.; *Paul*, Primärrechtliche Regelungen zur Verantwortlichkeit von Internetprovidern, S. 99 ff.; *Popp*, Die strafrechtliche Verantwortung von Internetprovidern, S. 89 ff.

[86] Diese gelten auch, wenn die Taten lediglich Bezug zu Drittländern, also zu Nicht-EU-Ländern aufweisen.

[87] Gesetz über die Nutzung von Telediensten (TDG vom 22.7.1997, BGBl. I 1997, S. 1870 f., zuletzt geändert durch Art. 12 Abs. 5 des Gesetzes vom 10.11.2006, BGBl. I 2006, 2553), trat mit Wirksamwerden des Elektronischer-Geschäftsverkehr-Vereinheitlichungsgesetzes (EIGVG) am 1.3.2007 (BGBl. I 2007, S. 251) gemäß Art. 5 Satz 2 außer Kraft.

[88] Staatsvertrag über Mediendienste (Mediendienste-Staatsvertrag – MDStV) vom 20.1. bis 12.2.1997 (GBl. BW 1997, S. 181 ff.) zuletzt geändert durch Art. 8 des Achten Staatsvertrages zur Änderung rundfunkrechtlicher Staatsverträge vom 8. bis 15.10.2004 (GBl. BW 2005, S. 197 ff.), trat mit Wirksamwerden des Neunten Rundfunkänderungsstaatsvertrages am 1.3.2007 (Art. 9 Abs. 2 des Neunten Rundfunkänderungsstaatsvertrages) außer Kraft.

[89] *Heß*, Die Verantwortlichkeit von Diensteanbietern, S. 76 ff., 207, 231 ff.; *Kessler*, Zur strafrechtlichen Verantwortlichkeit von Zugangsprovidern, S. 62 f.; *Kudlich*, Die Unterstützung fremder Straftaten durch berufsbedingtes Verhalten, S. 501 ff.; *ders.*, JA 2002, 798, 800 ff.; *Paul*, Primärrechtliche Regelungen zur Verantwortlichkeit von Internetprovidern, S. 99 ff.; *Popp*, Die strafrechtliche Verantwortung von Internetprovidern, S. 89 ff.

[90] BT-Drucks. 14/6098, S. 23, Vorbemerkung zu den §§ 8 bis 11 – §§ 9 ff. TDG Wirkungsweise eines Filters; *Bleisteiner*, Rechtliche Verantwortlichkeit im Internet, S. 157; *Malek*, Strafsachen im Internet, Rn. 72; *Moritz*, CR 2000, 119, 120; *Park*, GA 2001, 23, 29; *Schmitt*, in: Eberle/Rudolf/Wasserburg, Mainzer Rechtshandbuch der Neuen Medien, Kapitel XI, Rn. 23; *Tettenborn* et al., Beilage Nr. 10 zu BB 2001, 1, 27 – Art. 12 ff. ECRL als Vorfilter für strafrechtlich relevantes Verhalten.

[91] *Haft/Eisele*, JuS 2001, 112, 117 f.; *Hörnle*, NJW 2002, 1008, 1011; *Preuße*, Informationsdelikte im Internet, S. 168, Fn. 471; *Sieber/Höfinger*, in: Hoeren/Sieber, Handbuch Multimedia-Recht, Kap. 18.1, Rn. 21, 27; *Spindler*, NJW 2002, 921, 922.

von Tatbestandsrestriktion“,[92] Rechtfertigungsgrund,[93] Umstand der Schuld[94] oder Strafausschließungsgrund[95] ist die Strafbarkeit des Providers daher bereits aufgrund besonderer gesetzlicher Entscheidung, die auf dem übergeordneten wirtschaftlichen Interesse der Schaffung eines Gemeinsamen Binnenmarkts beruht,[96] ausgeschlossen. So kann der Host-Provider nach dem Gesetz die Speicherung der Daten regelmäßig in dem Bewusstsein vornehmen, sich um deren eventuell rechtswidrigen Inhalt nicht aktiv kümmern zu müssen (§ 10 TMG); eine strafrechtliche Haftung kommt erst bei Kenntnis von der rechtswidrigen Handlung oder Information in Betracht (§ 10 Satz 1 Nr. 1 TMG).

Der Täter handelt also lediglich durch ein nicht-menschliches Werkzeug, seinen Computer. Er nutzt den Computer zwar als seinen „technisch verlängerten Arm“ und verwendet ihn bei der Eingabe von Befehlen über die Tastatur, indem er ihn beeinflusst. Die durch die Beeinflussung hervorgerufenen Wirkungen stellen aber von der Handlung zu unterscheidende Teilerfolge dar, denn der Computer führt lediglich „sklavisch“ die Befehle des Täters aus. Soweit in der Literatur vereinzelt vertreten wird, dass auch der „vom Menschen aktuell beherrschte maschinelle Energieeinsatz“ ein Tun sein könne,[97] kann dem nicht gefolgt werden. Es ist bereits nicht ersichtlich, wo der Unterschied zwischen einem herkömmlichen vom Täter angestoßenen Kausalverlauf und einem vom Täter beherrschten maschinellen Energieeinsatz liegen soll bzw. wie der maschinelle Energieeinsatz vom „natürlichen“ (nicht-maschinellen) Kausalverlauf abzugrenzen ist. Darüber hinaus lassen sich maschinelle Abläufe ebenso wenig wie nicht-maschinelle beherrschen. Insbesondere an Computern angestoßene maschinelle Energieeinsätze sind nur eingeschränkt beherrschbar, weil die Daten mit Lichtgeschwindigkeit transportiert und innerhalb von Millisekunden verarbeitet und gespeichert werden. Der einzig beherrschbare Ablauf ist dort vielmehr die Handlung des den Computer bedienenden Menschen; eine Korrektur der Folgen von dessen Tätigkeit ist nur durch eine gegenläufige Aktivität (Löschen statt Speichern etc.) oder überhaupt nicht möglich.

Nutzt der Täter zur Tatausführung einen Computer, so begründet er nicht automatisch weitere ihm zurechenbare Handlungsorte durch die Verwendung eines solchen nicht-menschlichen Werkzeugs. Für nicht-menschliche Werkzeuge enthält das Gesetz nämlich weder eine für die Bestimmung des Tatorts bei der Teilnahme

---

92 *Hilgendorf*, NStZ 2000, 518, 519.

93 *Popp*, Die strafrechtliche Verantwortung von Internetprovidern, S. 94.

94 LG München I NJW 2000, 1051, 1052; *Hoeren*, in: Hoeren/Sieber, Handbuch Multimedia-Recht, Kap. 18.2, Rn. 61; *Vassilaki*, MMR 1998, 630, 634 f.

95 *Heghmanns*, in: Achenbach/Ransiek, HWSt[3], Rn. 54; *ders.*, ZUM 2000, 463, 465; *ders.*, JA 2001, 71, 78; ihm folgend *Busse-Muskala*, Strafrechtliche Verantwortlichkeit der Informationsvermittler im Netz, S. 243.

96 Erwägungsgrund 40 der Richtlinie 2000/31/EG vom 17.7.2000 (E-Commerce-Richtlinie), ABl. EG 2000, Nr. L 178, S. 6.

97 *Altenhain*, CR 1997, 485, 489.

entsprechende Vorschrift (§ 9 Abs. 2 StGB) noch eine den Täterschaftsformen in § 25 StGB vergleichbare Regelung zur Zurechnung von Tatorten. Das nicht-menschliche Werkzeug ist insbesondere kein „anderer" i.S.v. § 25 Abs. 1, 2. Var. StGB. Tatmittler muss vielmehr eine vom Täter verschiedene Person sein, der Täter muss durch einen anderen Menschen handeln. Eine juristische Ich-Spaltung etwa im Sinne einer virtuellen[98] und körperlichen Anwesenheit, bei der sich der Täter selbst als Werkzeug benutzt, ist abzulehnen.[99] Nicht-menschliche Werkzeuge, z.B. Computer, sind grundsätzlich nicht zur eigenständigen Willensbildung fähig. Darin unterscheiden sie sich erheblich von menschlichen Werkzeugen, sodass sie ohne eine gesonderte Regelung im Gesetz nicht mit solchen gleichgestellt werden können. Der Gesetzgeber hat die Regelungslücke bisher auch nicht geschlossen. Die unterschiedliche Behandlung ist folglich gerechtfertigt; bei der Verwendung eines nicht-menschlichen Werkzeuges handelt der Täter nur dort, wo er körperlich auf das nicht-menschliche Werkzeug einwirkt, beispielsweise auf den Knopf für die Zündung einer Bombe drückt oder über die Tastatur des Computers Befehle weitergibt.

bb) Keine sinnvolle Versuchs- und Rücktrittslösung bei erweitertem Handlungsort

Dieses Ergebnis wird durch die Anwendung der Versuchs- und Rücktrittsregeln auf unsere Konstellation bestätigt. Eine Zwischenspeicherung als Handlung des Täters zu betrachten, erscheint danach nicht sinnvoll.

Der Täter setzt nach seiner Vorstellung von der Tat (§ 22 StGB i.V.m. dem jeweiligen Straftatbestand) regelmäßig nicht erst mit dem Speichern auf einem bestimmten Server, sondern schon zu einem früheren Zeitpunkt an, nämlich mit dem Beginn des Ingangsetzens des Übertragungsvorgangs (Tastendruck, Mausklick o.Ä.). Nach dem Start des Übertragungsvorgangs sind nach der Tätervorstellung keine wesentlichen Zwischenschritte hin zur vollständigen Verwirklichung des Tatbestands mehr notwendig[100] bzw. ist eine unmittelbare Gefährdung des betroffenen Rechtsguts bereits eingetreten.[101] Der im Einzelfall erforderlichen Zwischenspeicherung ist sich der Täter u.U. auch gar nicht bewusst, sodass sie selbst kein wesentlicher Zwischenschritt sein kann. Unter dem Gesichtspunkt der Versuchsstrafbarkeit ist daher bereits der automatisierte Speichervorgang ein (Zwischen-)Erfolg.

---

[98] *Kuner*, CR 1996, 453, 454 – für eine virtuelle Anwesenheit in jedem Land, das ans Internet angeschlossen ist.

[99] So schon aus allgemeinen Erwägungen im Rahmen der Untersuchungen zur a.l.i.c. LK-StGB[11]-*Jähnke*, § 20, Rn. 77 (nicht mehr so deutlich LK-StGB[12]-*Schöch*, § 20, Rn. 198); S/S-*Perron*, § 20, Rn. 35.

[100] BGH NStZ 2004, 38, 38 f.; S/S-*Eser*, § 22, Rn. 36 ff.; *Fischer*, StGB, § 22, Rn. 10.

[101] S/S-*Eser*, § 22, Rn. 42; *Fischer*, StGB, § 22, Rn. 10.

Zum gleichen Ergebnis führt der Blick auf die Rechtsfigur des Rücktritts. Lädt ein Täter beispielsweise über das Internet rechtsradikale Äußerungen auf einen Server und stellte das Speichern noch einen zur Handlung gehörigen Akt dar, so wäre aus Tätersicht die Tat nach dem letzten Tastendruck nicht beendet (§ 24 Abs. 1, 1. Var. StGB – Rücktritt vom unbeendeten Versuch). Wollte der Täter von seiner Tat zurücktreten, so bräuchte er nach dieser Auffassung zur Erlangung der Straffreiheit lediglich während des Uploads den Vorsatz zur vollendeten Tatbegehung aufzugeben. Tatsächlich liegt die Speicherung ohne Eingreifen des Täters jedoch nicht mehr in seiner Hand, sodass ein Rücktritt – wie beim beendeten Versuch (§ 24 Abs. 1, 2. Var. StGB) – nur durch einen aktiven Abbruch der Datenübertragung möglich sein kann. Ein solcher beendeter Versuch kann jedoch nur vorliegen, wenn die Speicherung nicht als Handlung, sondern als Zwischenerfolg begriffen wird, denn nur dann ist durch den letzten Tastendruck aus der Sicht des Täters der Versuch bereits beendet worden.

cc) Untauglichkeit mehraktiger Delikte als Vergleichsgröße

Die Bestimmung eines virtuellen Handlungsorts an einem fernen Serverstandort lässt sich überdies nicht aus einem Vergleich mit der Ermittlung der Handlungsorte bei mehraktigen Delikten herleiten,[102] bei denen die einzelnen Tathandlungen an verschiedenen Orten begehbar sind und trotzdem als Einheit betrachtet werden.[103] Richtig ist, dass bei mehraktigen Delikten mehrere Handlungsorte begründet werden können, z.B. dadurch, dass die Teiltathandlungen auf verschiedenen Staatsgebieten vorgenommen werden. Nimmt A dem B dessen Brieftasche während einer Zugfahrt in Straßburg weg, nachdem er B zuvor in Freiburg ein Schlafmittel in den Kaffee gegeben hatte, so sind Handlungsorte sowohl in Straßburg als auch in Freiburg gegeben. Für die Anwendbarkeit deutschen Strafrechts ist bereits nach dem Gesetz ein Begehungsort im Inland ausreichend.

Die Vielzahl von Handlungsorten bei mehraktigen Delikten ergibt sich jedoch nicht aus einem weiten Verständnis des Handlungsbegriffs, sondern aus der den mehraktigen Delikten immanenten Tatbestandsstruktur. Diese ist dadurch gekennzeichnet, dass eine Geschehensabfolge aus mehreren aufeinander bezogenen verselbstständigten Teiltathandlungen erst die Gesamttathandlung bildet. Letztlich können bei mehraktigen Delikten die einzelnen Teiltathandlungen aber auch nur an einem einzigen Ort erbracht werden.[104] Im Beispielsfall etwa, wenn A dem B dessen Brieftasche in Freiburg gewaltsam entreißt.

---

[102] *Gercke*, Rechtswidrige Inhalte im Internet, S. 21; *Volk*, Glücksspiel im Internet, S. 203.

[103] So *Cornils*, JZ 1999, 394, 397; *dies.*, in: Hohloch, Recht und Internet, S. 71, 79; *Götting*, Kriminalistik 2007, 615, 618.

[104] *Gercke*, Rechtswidrige Inhalte im Internet, S. 21.

dd) Anknüpfen an körperlichem Standort bei staatenübergreifenden Regelungen

Auch soweit staatenübergreifende Regelungen zur Lösung positiver Kompetenzkonflikte ausgearbeitet wurden, erfolgte häufig eine strenge Differenzierung zwischen Handlung und Erfolg. Als Beispiel für derartige Regelungen lassen sich sowohl Vereinbarungen auf EU-Ebene als auch auf das Common Law-Prinzip rückführbare Entwürfe für internationale Konventionen finden.

Soweit sich die Europäische Kommission mit der Lösung positiver Kompetenzkonflikte und damit einhergehend mit der Befugnis eines nationalen Staates, ein bestimmtes Verhalten als verboten aufzufassen und Verstöße dagegen durch nationales Strafrecht mit Sanktionen zu belegen, beschäftigte und an die Handlung einer Person anknüpfte, stellte sie allein auf den Ort der persönlichen Anwesenheit ab.[105] So sprach sich die Kommission bei Vorarbeiten zu einer allgemeinen Harmonisierung des jeweiligen internationalen Strafrechts der Mitgliedstaaten[106] für eine gemeinsame Definition des Handlungsorts im Sinne des Orts der persönlichen Anwesenheit – auch in Kenntnis der Schwierigkeiten bei Straftaten mittels Computernetzwerken – aus.[107]

Die Anknüpfung des Handlungsorts ausschließlich an den Ort der physischen Anwesenheit des Täters wird des Weiteren in Rahmenbeschlüssen des Rates der Europäischen Union deutlich. Nach Art. 10 Abs. 2 des Rahmenbeschlusses des Rates der Europäischen Union über Angriffe auf Informationssysteme vom 24.2.2005[108] erfolgt beispielsweise eine klare Differenzierung zwischen Handlungs- und Erfolgsort, wobei für den Handlungsort auf die physische Anwesenheit des Täters abgestellt wird. Jeder Mitgliedstaat hat sicherzustellen, dass sich seine gerichtliche Zuständigkeit auf Fälle erstreckt, „in denen a) der Täter die Straftat begeht, während er sich physisch im Hoheitsgebiet dieses Staates aufhält […], oder b) sich die Straftat gegen ein Informationssystem in seinem Hoheitsgebiet richtet, unabhängig davon, ob der Täter die Straftat begeht, während er sich physisch im

---

[105] Vgl. aber zum Spannungsverhältnis zwischen Handlungsort und Firmensitz nach dem Herkunftslandprinzip die Ausführungen unter Teil 2, III.A.5.c).

[106] Kommission der Europäischen Gemeinschaften, KOM(2000) 495 endg.; Maßnahmenprogramm zur Umsetzung des Grundsatzes der gegenseitigen Anerkennung gerichtlicher Entscheidungen in Strafsachen, ABl. EG 2001, Nr. C 12, S. 15 f.; nachfolgend siehe auch Kommission der Europäischen Gemeinschaften, KOM(2005) 195 endg. sowie Kommission der Europäischen Gemeinschaften, KOM(2005) 696 endg.; hierzu ebenfalls Arbeitsdokument der Kommissionsdienststellen, Anhang zum Grünbuch über Kompetenzkonflikte und den Grundsatz ne bis in idem in Strafverfahren, SEK(2005), 1767.

[107] Diskussionspapier der Kommission (Generaldirektion Justiz und Inneres, Referat B/3 Justizielle Zusammenarbeit in Strafsachen) über die Anerkennung von Entscheidungen in Strafsachen zwischen den EU-Mitgliedstaaten und Gerichtsbarkeit, S. 15; bis März 2011 erreichbar unter http://web.archive.org/web/20030709005635/http://www.europa.eu.int-/comm/justice_home/unit/penal/discussion_paper_de.doc.

[108] Rahmenbeschluss 2005/222/JI des Rates vom 24.2.2005 über Angriffe auf Informationssysteme, ABl. EU 2005, Nr. L 69, S. 67.

Hoheitsgebiet dieses Staates aufhält". Noch klarer ist die Unterscheidung zwischen dem Ort der physischen Anwesenheit und dem Ort, an dem rechtswidrige Inhalte auf einem Server gehostet werden, in Art. 9 des Rahmenbeschlusses des Rates der Europäischen Union zur strafrechtlichen Bekämpfung bestimmter Formen und Ausdrucksweisen von Rassismus und Fremdenfeindlichkeit vom 28.11.2008.[109] Nach Art. 9 Abs. 2 des Rahmenbeschlusses hat jeder Mitgliedstaat bei Begründung der gerichtlichen Zuständigkeit sicherzustellen, „dass seine gerichtliche Zuständigkeit auch für Fälle gilt, in denen die Handlungen im Rahmen eines Informationssystems begangen werden und a) der Täter bei der Begehung der Handlungen in seinem Hoheitsgebiet physisch anwesend ist, unabhängig davon, ob die Handlungen rassistische Inhalte betreffen, die sich in einem in seinem Hoheitsgebiet betriebenen Informationssystem befinden; b) die Handlungen Inhalte betreffen, die sich in einem in seinem Hoheitsgebiet betriebenen Informationssystem befinden, unabhängig davon, ob der Täter bei der Begehung der Handlungen in seinem Hoheitsgebiet physisch anwesend ist".

Auch auf internationaler Ebene findet sich ein Beispiel für den Ausschluss der Anknüpfung an die virtuelle Anwesenheit bei der Lösung von positiven Kompetenzkonflikten. So stellt z.B. der Stanford Draft für eine Internationale Konvention zur Verbesserung des Schutzes vor Internetkriminalität und Terrorismus[110] in Art. 5 Abs. 4[111] ebenfalls ausdrücklich auf die physische Anwesenheit des Täters zum Tatzeitpunkt ab und qualifiziert die Strafanwendungsregel der körperlichen Anwesenheit sodann sogar zum primären Anknüpfungspunkt für eine Erstreckung der Jurisdiktion auf den Täter.

d) Teleologische Auslegung

Sinn und Zweck der Regelung der differenzierten Anknüpfung an die Handlung und den Erfolg sprechen ebenfalls gegen eine Erweiterung des Handlungs- zulasten

---

[109] Rahmenbeschluss 2008/913/JI des Rates vom 28.11.2008 zur strafrechtlichen Bekämpfung bestimmter Formen und Ausdrucksweisen von Rassismus und Fremdenfeindlichkeit, ABl. EU 2008, Nr. L 328, S. 55 ff.; zum vormaligen Art. 12 des Vorschlags für einen Rahmenbeschluss des Rates zur Bekämpfung von Rassismus und Fremdenfeindlichkeit, KOM(2001) 664 endg. – 2001/0270 (CNS) von der Kommission vorgelegt am 29.11.2001, vgl. ABl. EG 2002, Nr. C 75 E/17, S. 269 ff.

[110] Abgedruckt in *Sofaer/Goodman*, The Transnational Dimension of Cyber Crime and Terrorism, S. 249 ff.

[111] Art. 5 Abs. 4 Stanford Draft lautet: "Each State Party will exercise its rights and fulfill its obligations under this Convention to the extent practicable in accordance with the following priority of jurisdiction: first, the State Party in which the alleged offender was physically present when the alleged offense was committed; second, the State Party in which substantial harm was suffered as a result of the alleged offense; third, the State Party of the alleged offender's dominant nationality; fourth, any State Party where the alleged offender may be found; and fifth, any other State Party with a reasonable basis for jurisdiction."

des Erfolgsbegriffs. Der Gesetzgeber wollte die Anwendung des deutschen Strafrechts mit der Gleichstellung von Handlung und Erfolg als Anknüpfungspunkte für die Bestimmung von Tatorten im Inland umfassend ermöglichen, indem er die sogenannte Einheitstheorie – die sowohl den Handlungsort als auch den Erfolgsort als Begehungsort einer Straftat erfasst – in Gesetzform goss.[112] Die Strafanwendung ist nur hierdurch bestimmt und vorhersehbar.

Eine Erweiterung des Handlungsbegriffs auf außerhalb des Standorts des Täters hervorgerufene Wirkungen würde zum Verlust der Unterscheidbarkeit zwischen Handlung und der durch sie hervorgerufenen Wirkung, d.h. dem Erfolg, führen.[113] Die Grenzen zwischen der Handlung und dem Erfolg der Tat würden verschwimmen und der Erfolgsbegriff könnte inhaltsleer werden,[114] da jedenfalls Teile des Erfolgs schon Bestandteile der Handlung wären. Wären auch die mit der Handlung hervorgerufenen Wirkungen unter den Handlungsbegriff zu subsumieren, so könnten im Einzelfall über den tatbestandlichen Erfolg hinausgehende Wirkungen als Anknüpfungspunkte für weitere Handlungsorte dienen. Die begrenzende Funktion des Erfolgsbegriffs für die Bestimmung von Tatorten würde also konterkariert, wenn die Handlung nicht mehr auf die rein körperliche Tätigkeit begrenzt wäre.[115] Eine Bestimmung des Handlungsorts über den Ort der körperlichen Anwesenheit hinaus käme damit einer Fiktion gleich.[116]

Gegen eine Anknüpfung an den Speicherort als Handlungsort spricht zudem, dass allenfalls der technisch versierte Täter den Standort des Servers, auf dem er die Daten speichert, in bestimmtem Maße wählen kann. Er wird daher so weit wie möglich strengere Rechtsordnungen meiden,[117] indem er keine Serverstandorte nutzt, die solchen Ordnungen unterliegen. Häufig hat der Täter allerdings keine Kenntnis vom Standort des Servers, auf dem seine Daten gespeichert werden, oder er kann den Server zumindest nicht bewusst auswählen.[118] Kennt der Täter den

---

[112] Siehe *Rietzsch*, Deutsche Justiz 1940, 653, 564 f.; vgl. auch die Begründungen zu den Entwürfen eines Strafgesetzbuches E 1960 (BT-Drucks. III/2150, S. 107) und E 1962 (BT-Drucks. IV/650, S. 113) zu § 8 StGB-Entwurf, in denen es hieß, die Rechtsprechung – die sowohl am Handlungs- als auch am Erfolgsort ansetzt – solle verdeutlicht werden.

[113] *Gercke*, Rechtswidrige Inhalte im Internet, S. 20 f.; *Hilgendorf*, ZStW 113 (2001), 650, 666; *Hörnle*, NStZ 2001, 309, 310; *Körber*, Rechtsradikale Propaganda im Internet, S. 141; *Kudlich*, StV 2001, 397, 398; *Volk*, Glücksspiel im Internet, S. 203.

[114] *Hilgendorf*, ZStW 113 (2001), 650, 666; *Koch*, JuS 2002, 123, 127; *Sieber*, NJW 1999, 2065, 2070; *ders.*, in: Koops/Brenner, Cybercrime and Jurisdiction, S. 183, 197.

[115] *Hilgendorf*, ZStW 113 (2001), 650, 666; *Kudlich*, StV 2001, 397, 398.

[116] *Heimgartner*, in: Schwarzenegger/Arter/Jörg, Internet-Recht und Strafrecht, S. 117, 122 (für die Schweiz); *König*, Kinderpornografie im Internet, Rn. 33; *Schwarzenegger*, sic! 2001, 240, 248 (für die Schweiz).

[117] *Germann*, Gefahrenabwehr und Strafverfolgung im Internet, S. 230 (Fn. 482); *Schwarzenegger*, sic! 2001, 240, 247 (für die Schweiz).

[118] *Hilgendorf*, ZStW 113 (2001), 650, 666; *König*, Kinderpornografie im Internet, Rn. 32 ff.; *Poenig*, Die strafrechtliche Haftung des Linkanbieters, S. 134, 174; *Schwarzenegger*, sic! 2001, 240, 247 (für die Schweiz).

Serverstandort nicht und weiß folglich nicht, wo er im rechtlichen Sinne handelt, entfällt jedoch die verhaltenssteuernde Funktion des Strafrechts,[119] da der Täter u.U. glaubte, sich in den Grenzen des Strafrechts des Landes zu bewegen, in dem er körperlich tätig geworden ist.

e) Zwischenergebnis

Für die Frage nach der Befugnis zur Aufnahme von Ermittlungen durch die Strafverfolgungsbehörden in Fällen von im Internet begangenen Straftaten bedeutet die Eingrenzung des inländischen Handlungsorts auf den Ort der körperlichen Anwesenheit des Täters, dass die Strafverfolger bei Anknüpfen an den Handlungsort nur in den folgenden Fällen zuständig sind: Der Täter handelt selbst körperlich im Inland. Wenn er physisch im Ausland tätig wird, nutzt er entweder einen Tatmittler als Werkzeug für seine Zwecke, der im Inland handelt (§ 25 Abs. 1, 2. Var. StGB) oder er führt die Tat mit einem anderen gemeinschaftlich aus, wobei der andere im Inland handelt (§§ 9 Abs. 2, 2. Var., 25 Abs. 2 StGB).

Bedient der Täter ausschließlich einen Computer im Ausland und schaltet keine weitere Person in seine Tätigkeiten ein, liegt dagegen kein inländischer Handlungsort nach § 9 Abs. 1, 1. Var. i.V.m. § 3 StGB vor, sodass die Strafverfolgungsbehörden in diesen Fällen nur dann ihre Ermittlungen aufnehmen können, wenn die Handlung des Täters im Inland zu einem tatbestandlichen Erfolg geführt und damit einhergehend einen Erfolgsort begründet hat.

3. Bestimmung des Erfolgsorts bei extraterritorialer Handlung

Die Mehrheit in Literatur und Rechtsprechung lehnt die Erweiterung eines Handlungsorts über die körperliche Anwesenheit des Täters hinaus aus den vorgenannten Erwägungen ebenfalls ab und beantwortet die Frage, ob in den Fällen eines extraterritorialen Handelns des Täters das deutsche Strafrecht anwendbar ist, zu Recht durch Bestimmung eines Erfolgsorts nach § 9 Abs. 1, 3. Var. StGB.

a) Höchstrichterliche Rechtsprechung

Nach Auffassung des BGH[120] ist das deutsche Strafrecht nicht nur auf Erfolgs- und konkrete Gefährdungsdelikte, sondern zumindest auch auf das abstrakt-

---

[119] *Von Hinden*, Persönlichkeitsverletzungen im Internet, S. 66; *Valerius*, NStZ 2003, 341, 343.

[120] BGHSt 46, 212 ff. = BGH NJW 2001, 624 ff.; anders noch in der Vorinstanz das LG Mannheim, Urteil vom 10.11.1999, Az.: 5 KLs 503 Js 9551/99, abrufbar unter: http://www.netlaw.de/urteile/lgma_05.htm [Stand: 6.11.2013], das einen Tatort in den Fällen verneinte, in denen die Holocaust-Leugnung auf einer Webseite erfolgte, die auf einem Server in Australien gehostet war. Nunmehr dem BGH in seiner Argumentation

konkrete Gefährdungsdelikt der Volksverhetzung gemäß § 130 StGB anwendbar, wenn der Täter nach § 130 StGB strafbare Inhalte ins Internet stellt.[121] Die zwischen den konkreten und rein abstrakten Gefährdungsdelikten anzusiedelnde Gruppe der abstrakt-konkreten Gefährdungsdelikte sei unter dem Gesichtspunkt des Erfolgsorts mit den konkreten Gefährdungsdelikten vergleichbar, die nach einhelliger Auffassung einen Erfolg i.S.d. § 9 Abs. 1, 3. Var. StGB aufwiesen. Der Gesetzgeber habe bei abstrakt-konkreten Gefährdungsdelikten als Erfolg eine zu vermeidende Gefährdung im Tatbestand der jeweiligen Norm ausdrücklich bezeichnet. Der Erfolg i.S.d. § 9 Abs. 1, 3. Var. StGB trete bei abstrakt-konkreten Gefährdungsdelikten an dem Ort ein, an dem sich die Gefährlichkeit der konkreten Tat für das im Tatbestand umschriebene Rechtsgut entfalte.[122] Ein völkerrechtlich legitimierender Anknüpfungspunkt liege in derartigen Fällen in dem Betroffensein eines gewichtigen inländischen Rechtsguts, welches darüber hinaus objektiv einen besonderen Bezug zum Bundesgebiet aufweise.[123] Ob diese Sicht auch auf rein abstrakte Gefährdungsdelikte übertragbar ist, ließ der BGH indes ausdrücklich offen.[124]

Der technischen Qualifizierung der Übertragungsvorgänge maß der BGH[125] im Übrigen keine Bedeutung für die rechtliche Bewertung bei. Es sei unerheblich, ob der Anbieter die Daten zum Nutzer „schickt", also der Anbieter technisch gesehen aktiv ist, während der Empfänger passiv bleibt – sogenannte Push-Technologie[126] –, oder ob der Nutzer die angebotenen Daten „holt", d.h. die Initiative ergreift und der Anbieter eher passiv ist – sogenannte Pull-Technologie[127] –, da die jeweiligen technischen Abläufe ineinander übergingen und damit nicht praktikabel unterschieden werden könnten.

---

aber in den Fällen der im Ausland gehosteten Webseiten der Revisionisten *Ernst Zündel* und *Germar Rudolf* folgend LG Mannheim, Urteile vom 15.2.2007, Az.: 6 KLs 503 Js 4/96 und 15.3.2007 (unveröffentlicht). Die im „Fall Zündel" eingelegte Revision verwarf der BGH durch Beschluss vom 12.9.2007, Az.: 1 StR 337/07, HRRS 2007, Nr. 832.

[121] BGHSt 46, 212, 220 = BGH NJW 2001, 624, 627; dazu auch *Weingärtner*, AfP 2002, 134.

[122] BGHSt 46, 212, 221 = BGH NJW 2001, 624, 627.

[123] BGHSt 46, 212, 224 = BGH NJW 2001, 624, 628.

[124] BGHSt 46, 212, 222 f. = BGH NJW 2001, 624, 627.

[125] BGH MMR 2001, 676, 677 f. = BGH NStZ 2001, 596, 597; so auch schon BGH NJW 2001, 3558, 3559.

[126] *Klußmann*, Lexikon der Kommunikations- und Informationstechnik, Stichwort Pushdienst; *Mayer*, Das Internet im öffentlichen Recht, S. 44; *Sieber*, NJW 1999, 2065, 2071; *ders.*, in: Koops/Brenner, Cybercrime and Jurisdiction, S. 183, 200; *Sieber/Klimek*, K&R 1999, 305.

[127] *Klußmann*, Lexikon der Kommunikations- und Informationstechnik, Stichwort Pushdienst; *Mayer*, Das Internet im öffentlichen Recht, S. 44; *Sieber*, NJW 1999, 2065, 2071; *ders.*, in: Koops/Brenner, Cybercrime and Jurisdiction, S. 183, 200.

b) Universelle Anwendung deutschen Strafrechts

Im Gegensatz zur zumindest teilweise eingrenzenden Auffassung des BGH halten einige Stimmen in der Literatur das deutsche Strafrecht auf Straftaten im Internet generell für anwendbar, überwiegend ohne auf technische Besonderheiten des Internet oder rechtliche Differenzierungen zwischen Erfolgs- und Gefährdungsdelikten einzugehen.[128] Während einzelne Vertreter die Auswirkungen der universellen Anwendbarkeit des deutschen Strafrechts außer Betracht lassen,[129] problematisiert die Mehrheit allerdings diesen Punkt, indem sie auf die Gefahr entstehender zwischenstaatlicher Spannungen eingeht und insbesondere auf die Möglichkeit verweist, dass Deutschland so in den Ruf eines „Weltpolizisten" geraten könnte. Zur Vermeidung der genannten Folgen verlangen deshalb einige eine Einschränkung des deutschen internationalen Strafrechts auf Taten mit finalem Interesse an einer Wirkung in Deutschland.[130]

Im Ergebnis ebenfalls zur universellen Anwendbarkeit deutschen Strafrechts gelangen auch diejenigen, die an die Tatbestandslehre anknüpfen und das deutsche Strafrecht zwar nicht pauschal auf alle Straftaten im Internet anwenden, aber bei abstrakten Gefährdungsdelikten ebenso einen Erfolg i.S.d. § 9 Abs. 1 3. Var. StGB bejahen.[131] Nach einigen vereinzelt gebliebenen Stimmen[132] sei ein derart bestimmter Anwendungsbereich des deutschen Strafrechts bereits durch die allgemeinen

---

[128] *Von Bonin/Köster*, ZUM 1997, 821, 828 (Fn. 66); *Collardin*, CR 1995, 618, 620; *Conradi/Schlömer*, NStZ 1996, 366, 369; *Ernst*, NJW-CoR 1997, 224, 228; Generalbundesanwalt MMR 1998, 93, 94; *Hinterseh*, JurPC 1996, 460, 462 f.; wohl auch *Kuner*, CR 1996, 453, 453 f.; *Löhnig*, JR 1997, 496; *Loock-Wagner*, Das Internet und sein Recht, S. 68 f.; *Meseke*, Kriminalistik 2000, 245, 249; so wohl auch *Vahrenwald*, Recht in Online und Multimedia, 12.2., S. 2.

[129] So *Ernst*, NJW-CoR 1997, 224, 228; *Löhnig*, JR 1997, 496.

[130] *Collardin*, CR 1995, 618, 621; *Conradi/Schlömer*, NStZ 1996, 366, 369; *Hinterseh*, JurPC 1996, 460, 463; *Loock-Wagner*, Das Internet und sein Recht, S. 69.

[131] Allgemein zur Problematik des Erfolgsorts bei abstrakten Gefährdungsdelikten in diesem Sinne: *Beisel/Heinrich*, JR 1996, 95, 96 (für Satellitenausstrahlung pornografischer Sendungen); *Heinrich*, NStZ 2000, 533, 534; *Martin*, ZRP 1992, 19, 21; *ders.*, Strafbarkeit grenzüberschreitender Umweltbeeinträchtigungen, S. 87, 131 und *Tiedemann/Kindhäuser*, NStZ 1988, 337, 346 (für Umweltdelikte) – Letztere fordern aber eher eine Klarstellung durch den Gesetzgeber.

Konkret zu Straftaten im Internet: *Barton*, Multimedia-Strafrecht, Rn. 221; *Beisel/Heinrich*, CR 1997, 360, 363; wohl auch *Derksen*, NJW 1997, 1878, 1880; *Finke*, Die strafrechtliche Verantwortung von Internet-Providern, S. 51; *Heinrich*, GA 1999, 72, 80, 82; *Jeßberger*, JR 2001, 432, 433 (aber beschränkt auf § 130 StGB); *Jofer*, Strafverfolgung im Internet, S. 109; *Klam*, Die rechtliche Problematik von Glücksspielen im Internet, S. 55 ff.; *Lehle*, Der Erfolgsbegriff und die deutsche Strafrechtszuständigkeit im Internet, S. 104, 165; *Poenig*, Die strafrechtliche Haftung des Linkanbieters, S. 175 ff.; *Schmidt*, Gefahrenabwehrmaßnahmen im Internet, S. 254; *Schwarzenegger*, sic! 2001, 240, 247 ff.; *ders.*, ZStrR Bd. 118 (2000), 109, 125 (für die Schweiz).

[132] *Barton*, Multimedia-Strafrecht, Rn. 224; *Jofer*, Strafverfolgung im Internet, S. 119; *Schwarzenegger*, sic! 2001, 240, 247 ff. (für die Schweiz).

prozessualen und materiell-rechtlichen Einschränkungsmöglichkeiten ausreichend begrenzt. Der Großteil der Vertreter dieser Auffassung hält demgegenüber jedoch eine tatbestandliche Einschränkung des Anwendungsbereichs des deutschen Strafrechts für erforderlich, um den mit der universellen Anwendbarkeit des deutschen Strafrechts auf Straftaten im Internet verbundenen zwischenstaatlichen Spannungen ausreichend Rechnung zu tragen.

Strittig ist unter letzterer Gruppe allerdings, wie eine solche Einschränkung erfolgen soll. Nach einer Ansicht bedarf es einer gesonderten gesetzlichen Regelung für im Internet begangene Straftaten,[133] wonach nur noch auf das Bundesgebiet abzielende Verhaltensweisen den Anwendungsbereich des deutschen Strafrechts eröffnen. Dies könne durch Ergänzung des § 9 Abs. 1 StGB um die Sätze 2 und 3 wie folgt erreicht werden:[134]

> „Der zum Tatbestand gehörende Erfolg begründet bei Taten in weltweiten Datennetzen (Internet) nur dann einen Tatort in Deutschland, wenn die Tat einen sachlichen Bezug zu Deutschland aufweist. Ein solcher sachlicher Bezug ist insbesondere dann gegeben, wenn der Inhalt einer in ein Datennetz eingegebenen Datei in deutscher Sprache verfasst ist, sich speziell auf deutsche Sachverhalte oder Personen bezieht, oder wenn der Täter gerade auf eine Wirkung in Deutschland abzielt."

Nach einer weiteren Ansicht führt dagegen bereits die Auslegung der Strafanwendungsregeln im Wege teleologischer Reduktion zur Einschränkung des Anwendungsbereichs des deutschen Strafrechts. Auf abstrakte Gefährdungsdelikte sei das Strafrecht demgemäß nur anwendbar, wenn die Tat eine besondere territoriale Beziehung zu Deutschland aufweise[135] bzw. der Täter mit dolus directus ersten Grades eine Wirkung im Inland herbeiführen wolle.[136] Für Verletzungsdelikte sei nach letzterer Ansicht dagegen lediglich ein objektiver besonderer Bezug zum Gebiet der Bundesrepublik erforderlich.[137] Eine weitere Auffassung[138] fordert dagegen, dass im konkreten Fall völkerrechtliche Grundsätze einer Bestrafung nicht entgegenstehen dürften und dass der extraterritorial handelnde Täter bei Distanzdelikten zumindest bedingt vorsätzlich einen Erfolgseintritt im Inland herbeiführen wollte oder aber, dass ein solcher für ihn vorhersehbar war. Hiergegen wendet sich schließlich eine letzte Ansicht, die das deutsche Strafrecht auf extraterritorial handelnde Täter nur anwendet, wenn der Täter zielgerichtet in Deutschland handeln will und gleichzeitig das Angebot im Internet objektiv auf die Nutzung in Deutsch-

---

133 *Derksen*, NJW 1997, 1878, 1880 f.; *Lehle*, Der Erfolgsbegriff und die deutsche Strafrechtszuständigkeit im Internet, S. 174 f.

134 *Lehle*, Der Erfolgsbegriff und die deutsche Strafrechtszuständigkeit im Internet, S. 174 f.

135 *Poenig*, Die strafrechtliche Haftung des Linkanbieters, S. 202 f., der zusätzlich noch fordert, dass es für die Tat in dem Land, in dem die Handlung ausgeführt wurde, keinen ähnlich gearteten Bezug gibt; *Schmidt*, Gefahrenabwehrmaßnahmen im Internet, S. 255 f.

136 *Finke*, Die strafrechtliche Verantwortung von Internet-Providern, S. 56.

137 Ebenda, S. 57.

138 *Heinrich*, GA 1999, 72, 82 f.

land z.B. durch Verwendung der deutschen Sprache bezogen ist.[139] Sei ein eindeutiger Bezug zu Deutschland nicht herstellbar, sei auch dass deutsche Strafrecht nicht anwendbar.[140]

c) Nichtanwendung auf abstrakte Gefährdungsdelikte

Der Anwendung des deutschen Strafrechts auf alle Deliktstypen tritt die Ansicht entgegen, die im Fall eines extraterritorialen Handelns des Täters einen Erfolgsort i.S.d. § 9 Abs. 1, 3. Var. StGB in Deutschland für abstrakte Gefährdungsdelikte verneint.[141] Das deutsche Strafrecht wäre nach dieser Ansicht bei Straftaten im Internet, sofern ein extraterritoriales Handeln vorliegt, nur bei Verletzungs- und konkreten Gefährdungsdelikten anwendbar. Überwiegend befürworten die Vertreter dieser Ansicht darüber hinaus auch für Verletzungs- und konkrete Gefährdungsdelikte eine einschränkende Interpretation. Wie eine solche ausgestaltet sein sollte, ist jedoch umstritten.

---

[139] *Klam*, Die rechtliche Problematik von Glücksspielen im Internet, S. 66 ff.

[140] Ebenda, S. 70 ff.

[141] Allgemein zur Problematik des Erfolgsorts bei abstrakten Gefährdungsdelikten in diesem Sinne: KG NJW 1999, 3500, 3502 (aber Ansetzen bei der Handlung); *Oehler*, Internationales Strafrecht, Rn. 257; *Satzger*, NStZ 1998, 112, 115 f.; *ders.*, Internationales und Europäisches Strafrecht, § 5, Rn. 21, 27, siehe auch Rn. 52 (zum Teil aber einen nicht näher definierten tatortbegründenden Zwischenerfolg bei abstrakten Gefährdungsdelikten annehmend); *v. d. Horst*, ZUM 1993, 227, 228 (in Bezug auf die Satellitenausstrahlung pornografischer Sendungen).

Konkret zu Straftaten im Internet: LG Mannheim, Urteil vom 10.11.1999, Az.: 5 KLs 503 Js 9551/99, abrufbar unter: http://www.netlaw.de/urteile/lgma_05. [Stand: 6.11.2013]. Aufgehoben durch BGHSt 46, 212 ff. = BGH NJW 2001, 624 ff. und nunmehr dem BGH in seiner Argumentation in den Fällen der im Ausland gehosteten Webseiten der Revisionisten *Ernst Zündel* und *Germar Rudolf* folgend LG Mannheim, Urteile vom 15.2.2007, Az.: 6 KLs 503 Js 4/96 und 15.3.2007 (unveröffentlicht).; *Boese*, Strafrechtliche Verantwortlichkeit für Verweisungen durch Links im Internet, S. 107 f.; *Breuer*, MMR 1998, 141, 142; *Clauß*, MMR 2001, 232; *Freund*, Die Strafbarkeit von Internetdelikten, S. 75 (für Österreich); *Gercke*, CR 2007, 62, 66 f.; *Heghmanns*, JA 2001, 276, 278 ff. *ders.*, in: Achenbach/Ransiek, HWSt[3], Rn. 9 ff.; *Heimgartner*, in: Schwarzenegger/Arter/Jörg, Internet-Recht und Strafrecht, S. 117, 124 f. (für die Schweiz); *Hilgendorf*, NJW 1997, 1873, 1875 f.; *ders.*, ZStW 113 (2001), 650, 662 f.; *Kienle*, Internationales Strafrecht und Straftaten im Internet, S. 51 f.; *Kioupis*, in: Anagnostopoulos, Internationalisierung des Strafrechts, S. 93, 108 f. – anders aber ab S. 111 – (für Griechenland); *Klengel/Heckler*, CR 2001, 243, 248; *König*, Kinderpornographie im Internet, Rn. 78 f.; *Körber*, Rechtsradikale Propaganda im Internet, S. 147 f.; *Leupold/Bachmann/Pelz*, MMR 2000, 648, 654; *Moritz*, in: Loewenheim/Koch, Praxis des Online-Rechts, S. 473, 479; *Pelz*, ZUM 1998, 530, 531; *Plöckinger*, ÖJZ 2001, 798, 801 f. (für Österreich); *Ringel*, CR 1997, 302, 303; *Römer*, Verbreitungs- und Äußerungsdelikte im Internet, S. 120, 126; *Schmitt*, in: Eberle/Rudolf/Wasserburg, Mainzer Rechtshandbuch der Neuen Medien, Kapitel XI, Rn. 12 f. (der im Ausnahmefall aber auch abstrakten Gefährdungsdelikten einen tatbestandlichen Erfolg zubilligt); *ders.*, FS 600 Jahre Würzburger Juristenfakultät, S. 357, 369; *Werle/Jeßberger*, JuS 2001, 35, 39 (konkret für § 130 StGB – jedoch bei der Handlung ansetzend).

Einige schlagen vor, nur Straftaten, die eine besondere – objektiv zu bestimmende – sogenannte territoriale Spezifizierung zum Inland aufweisen, in den Anwendungsbereich des deutschen Strafrechts einzubeziehen.[142] Eine solche Spezifizierung könne sich z.B. aus der deutschen Sprache, dem inhaltlichen Bezug des Angebots auf deutsche Personen und Sachverhalte etc. ergeben. Nach anderer Auffassung ist dagegen die Spezifizierung nur den allgemeinen Regeln des Völkerrechts entnehmbar[143] bzw. ein völkerrechtlich anerkanntes Anknüpfungsinteresse erforderlich.[144] Andere[145] fordern wiederum eine Eingrenzung in Anlehnung an § 7 StGB, wonach eine Inlandstat bei extraterritorialem Handeln nur dann vorliegt, wenn der „zum Tatbestand gehörende Erfolg" in Deutschland eingetreten ist *und* sich die Tat gegen einen Deutschen richtet (Argument aus § 7 Abs. 1 StGB), der Täter zur Zeit der Tat Deutscher war bzw. es nach der Tat geworden ist (Argument aus § 7 Abs. 2 Nr. 1 StGB) oder der Täter zur Zeit der Tat Ausländer war, im Inland betroffen und nicht ausgeliefert wird (Argument aus § 7 Abs. 2 Nr. 2 StGB). Nach einer weiteren Ansicht[146] ist eine Einschränkung des Anwendungsbereichs sinnvoll hingegen nur dadurch zu erreichen, dass das deutsche Strafrecht lediglich in den Fällen anwendbar ist, in denen auch am Handlungsort eine identische Strafnorm existiert.

d) Bestimmung eines eigenständigen Erfolgsbegriffs

Eine andere Meinungsgruppe bestimmt den Erfolg i.S.d. § 9 Abs. 1, 3. Var. StGB unabhängig von der Differenzierung zwischen Erfolgs- und Gefährdungsdelikten. Der „zum Tatbestand gehörende Erfolg" könne „jede Wirkung, um deren Verhinderung willen das sie verursachende Verhalten mit Strafe bedroht wird", sein.[147] Eingrenzend sei jedoch erforderlich, den Anwendungsbereich bei extraterritorialem Handeln des Täters auf diejenigen Taten zu beschränken, die dem Inhalt nach einen Bezug zum Inland aufweisen, der sich nicht zugleich auch für den Staat des Anbieterstandorts herstellen ließe.[148]

---

[142] *Boese*, Strafrechtliche Verantwortlichkeit für Verweisungen durch Links im Internet, S. 110 f.; *Clauß*, MMR 2001, 232, 233; *Hilgendorf*, NJW 1997, 1873, 1876 f.; *ders.*, ZStW 113 (2001), 650, 668 ff.; *Moritz*, in: Loewenheim/Koch, Praxis des Online-Rechts, S. 473, 479; *Römer*, Verbreitungs- und Äußerungsdelikte im Internet, S. 145; im Ergebnis wohl auch *Leidenmühler/Plöckinger*, in: Plöckinger/Duursma/Helm, Aktuelle Entwicklungen im Internet-Recht, S. 101, 111 (für Österreich); *Schmitt*, in: Eberle/Rudolf/Wasserburg, Mainzer Rechtshandbuch der Neuen Medien, Kapitel XI, Rn. 10; *ders.*, FS 600 Jahre Würzburger Juristenfakultät, S. 357, 373 f.

[143] *Körber*, Rechtsradikale Propaganda im Internet, S. 149 ff. – ohne Konkretisierung der Regelungen.

[144] *Heghmanns*, in: Achenbach/Ransiek, HWSt^3, Rn. 16.

[145] *Breuer*, MMR 1998, 141, 144.

[146] *Kienle*, Internationales Strafrecht und Straftaten im Internet, S. 173, 182.

[147] *Germann*, Gefahrenabwehr und Strafverfolgung im Internet, S. 233 f.

[148] Ebenda, S. 236.

Diesem Ansatz ähnelt eine weitere Sicht, die bei der Tathandlung und deren Wirkung ansetzt und für die Konkretisierung des „zum Tatbestand gehörenden Erfolgs“ auf die vom Gesetz geforderte Rechtsgutbeeinträchtigung abstellt.[149] Bei Gefährdungsdelikten könne jedenfalls dann, wenn das Verhalten zur Beeinträchtigung des geschützten Rechtsguts geeignet sei, ein Erfolgsort begründet werden.[150]

Nach einer weiteren Auffassung soll hierbei allein auf die Formulierung des jeweiligen Tatbestands abzustellen und nur dort ein Erfolg zu bejahen sein, wo ein gedanklich abgrenzbarer Erfolg in der Außenwelt vom Tatbestand vorausgesetzt werde.[151]

Zu einem ähnlichen Ergebnis gelangt ferner die Ansicht, nach der durch die bloße abstrakte Gefährlichkeit einer Handlung ein Erfolg nicht schon überall dort eintrete, wo sich die vom Gesetzgeber befürchtete Folge des strafbaren Handelns realisiere.[152] Maßgebend sei zwar der Wortlaut des konkreten Tatbestands, der aber vom Gesetzgeber in der Regel nicht zielgerichtet unter dem Aspekt der internationalen Erstreckung des Strafrechts gewählt werde. Es sei daher eine eigenständige, im Zusammenhang mit den §§ 3 ff. StGB stehende, klare, international harmonisierte „materienbezogene Regelung für Kommunikationsdelikte“ erforderlich, um die Anwendbarkeit des deutschen Strafrechts auf im Ausland begangene Straftaten im Internet zu regeln.[153]

Ein anderer Vertreter der Literatur[154] unterscheidet zwischen reinen Tätigkeitsdelikten und Delikten, die eine Veränderung der Außenwelt erfordern, und nimmt nur bei Ersteren keinen Erfolgsort i.S.d. § 9 Abs. 1, 3. Var. StGB an. Darüber hinaus sei eine Begrenzung allein durch die Weiterentwicklung technischer Möglichkeiten, insbesondere in der Entwicklung von Sperrmöglichkeiten für bestimmte Länder, sinnvoll umsetzbar.[155]

e) Anwendung unter Berücksichtigung der Technik

Nach einer weiteren Gruppe von Meinungsvertretern ist den technischen Besonderheiten des Internet bei der Bestimmung der Anwendbarkeit des deutschen Strafrechts Rechnung zu tragen. Ein Teil der Vertreter dieser Ansicht versteht den „zum Tatbestand gehörenden Erfolg“ i.S.d. § 9 Abs. 1, 3. Var. StGB als einen sogenann-

---

[149] *Vassilaki*, CR 2001, 262, 263; *dies.*, in: Moritz/Dreier, Rechts-Handbuch zum E-Commerce[2], Teil G, Rn. 7 f.

[150] *Vassilaki*, CR 2001, 262, 264; *dies.*, in: Moritz/Dreier, Rechts-Handbuch zum E-Commerce[2], Teil G, Rn. 9.

[151] *Kudlich*, StV 2001, 397, 398 f.; *ders.*, HRRS 2004, 278, 280.

[152] *Weigend*, in: Hohloch, Recht und Internet, S. 85, 89 f.

[153] Ebenda, S. 85, 90.

[154] *Schreibauer*, Das Pornographieverbot des § 184 StGB, S. 106.

[155] Ebenda, S. 113.

ten Tathandlungserfolg.[156] Das deutsche Strafrecht sei damit grundsätzlich auf alle Deliktsarten anwendbar. Durch die technischen Besonderheiten des Internet, insbesondere die Verwendung von Push-Technologien (aktives Versenden von Daten durch den Anbieter an den Empfänger) und Pull-Technologien (bloßes Bereitstellen von Daten durch den Anbieter für den Empfänger, der sich diese selbst herunterlädt) sei die universelle Anwendbarkeit jedoch eingeschränkt. Nur Datenübermittlungen mittels Push-Technologien würden zur Anwendbarkeit des deutschen Strafrechts auf Straftaten im Internet führen. Lediglich der Internetnutzer, der Daten auf diese Weise versendet, sei aktiv tätig, sodass allein in diesen Konstellationen ein dem Täter als mittelbare Folge der Tathandlung zurechenbarer Erfolg herbeigeführt werde.[157] Die Notwendigkeit einer weitergehenden Einschränkung des Anwendungsbereichs des deutschen Strafrechts – z.B. auf zielgerichtetes Handeln – könne damit überhaupt nur in Teilnahmefällen (§ 9 Abs. 2 StGB) gegeben sein,[158] da für den Teilnehmer eine Begrenzung aufgrund der Technik nicht sinnvoll möglich sei.[159]

Ebenso an den technischen Besonderheiten des Internet bei der Bestimmung der Anwendbarkeit des deutschen Strafrechts, aber ohne Berufung auf einen „Tathandlungserfolg", setzt eine andere Ansicht an.[160] Nur in den seltenen Konstellationen des vom Anbieter in Gang gesetzten unmittelbaren Versendens an den Empfänger sei das deutsche Strafrecht anwendbar, da der Täter durch die Richtung des Angriffs selbst den erforderlichen Bezug zum sanktionierenden Staat herstelle, wodurch sich zugleich eine weitere Einschränkung des Anwendungsbereichs des deutschen Strafrechts erübrige.[161]

Eine von diesem Ansatz abweichende Ansicht macht die Bestimmung der Anwendbarkeit des deutschen Strafrechts wiederum davon abhängig, ob sich die Tat explizit auf einen tatbestandlichen Erfolg in Deutschland bezieht. Eine Inlandstat nach § 9 Abs. 1 StGB scheide in den Fällen eines extraterritorial handelnden Täters aus, wenn aus Gründen der technischen Besonderheiten des Internet eine weltweite Wirkung (etwa im WWW) erzielt werde.[162]

---

[156] *Sieber*, NJW 1999, 2065, 2068; *ders.*, in: Koops/Brenner, Cybercrime and Jurisdiction, S. 183, 196 ff.; sich in diesem Punkt anschließend MünchKommStGB-*Ambos*, § 9, Rn. 34; *Hörnle*, NStZ 2001, 309, 310; *Soiné*, Polizeispiegel 2001, 168, 169; so wohl auch *Vec*, NJW 2002, 1535, 1538; *Volk*, Glücksspiel im Internet, S. 206, 208.

[157] *Sieber*, ZRP 2001, 97, 101; sich in diesem Punkt anschließend *Graf*, in: Heermann/Ohly, Verantwortlichkeit im Netz, S. 85, 95; *ders.*, DRiZ 1999, 281, 282.

[158] *Sieber*, NJW 1999, 2065, 2071 f.; *ders.*, in: Koops/Brenner, Cybercrime and Jurisdiction, S. 183, 201; für eine völkerrechtliche Einschränkung aber *Hörnle*, NStZ 2001, 309, 310 und *Volk*, Glücksspiel im Internet, S. 235 ff., für eine zwischenstaatlich konsentrierte Vorgehensweise.

[159] *Sieber*, NJW 1999, 2065, 2071 f.; *ders.*, in: Koops/Brenner, Cybercrime and Jurisdiction, S. 183, 201.

[160] *Gercke*, Rechtswidrige Inhalte im Internet, S. 26; *ders.*, ZUM 2002, 283, 287.

[161] *Gercke*, Rechtswidrige Inhalte im Internet, S. 30.

[162] *Lenz*, FS Nishihara, S. 467, 476.

f) Ungeeignetheit nationaler Normen

Im Gegensatz zu den vorgenannten Ansichten ist nach einer weiteren Auffassung das Territorialitätsprinzip auf Internet-Inhalte bei extraterritorialem Handeln generell unanwendbar,[163] da der Sinn und Zweck dieses Prinzips bei Straftaten im Internet hinfällig sei. Der Geltungsbereich des deutschen Strafrechts soll aber gleichwohl für Erfolgsdelikte eröffnet sein, weil ansonsten der Wortlaut des § 9 Abs. 1, 3. Var. StGB als Auslegungsgrenze nicht genügend berücksichtigt würde. Zumindest für Erfolgsdelikte sei aber eine gesetzgeberische Klarstellung in dem Sinne erforderlich, dass bei strafbaren Internet-Inhalten allein § 9 Abs. 1, 1. Var. StGB anwendbar sei, indem § 9 Abs. 1 StGB um folgenden Satz 2 ergänzt werden sollte:

> „Eine Tat, die das Bereithalten von Inhalten im Sinne des Teledienstegesetzes[164] zum Gegenstand hat, ist an jedem Ort begangen, an dem der Täter gehandelt hat."[165]

Die aus der Einschränkung des Territorialitätsprinzips entstehenden Strafbarkeitslücken seien durch eine begrenzte Erweiterung des aktiven Personalitätsprinzips, insbesondere auf diejenigen Täter, welche sich gezielt für ihre Veröffentlichungen ins liberalere Ausland absetzen, zu schließen.[166]

Einen ähnlichen Ansatz verfolgt die Ansicht, welche das deutsche Strafrecht – jedenfalls für den Bereich der rechtsextremen Propaganda im Netz – nicht aufgrund nationaler Normen für anwendbar hält. Da nationale Behörden bei der Strafverfolgung von Tätern, die strafbare Inhalte vom Ausland ins Internet stellen, in der Praxis machtlos seien, sei die Zuständigkeit zur Verfolgung solcher Taten sinnvollerweise allein durch internationale Vereinbarungen und die Zusammenarbeit auf internationaler Ebene festschreibbar.[167]

Nach einer weiteren Auffassung ist eine grundlegende gesetzgeberische Reform des Strafanwendungsrechts bei sogenannten deterritorialisierenden Kriminalitätserscheinungen erforderlich. Es bedürfe einer ergänzenden gesetzlichen Vorschrift, welche die Gerichtsbarkeit daran anknüpft, dass die im Ausland begangene Tat geeignet sei, im Inland eine fühlbare deliktsspezifische Beeinträchtigung der durch die jeweilige Strafvorschrift geschützten Interessen zu bewirken.[168]

---

[163] *Bremer*, Strafbare Internet-Inhalte in internationaler Hinsicht, S. 115.

[164] Nunmehr aufgegangen im Telemediengesetz vom 26.2.2007, BGBl. I 2007, S. 179 ff.

[165] *Bremer*, Strafbare Internet-Inhalte in internationaler Hinsicht, S. 174 f.; *ders.*, MMR 2002, 147, 151.

[166] *Bremer*, Strafbare Internet-Inhalte in internationaler Hinsicht, S. 238; *ders.*, MMR 2002, 147, 151.

[167] *Koch*, JuS 2002, 123, 127.

[168] *Von Bubnoff*, in: Zieschang/Hilgendorf/Laubenthal, Strafrecht und Kriminalität in Europa, S. 83, 100.

4. Erfolg nur bei Eintritt tatbestandsmäßiger Verletzungen und konkreter Gefährdungen

Gemeinsam war den vorstehenden am Erfolgsort ansetzenden Ansichten, dass sie den Erfolgsort nahezu ausschließlich mit Blick auf das nationale Recht bestimmen. Hierfür stritt zunächst auch das jedem Nationalstaat gegebene Recht zur Ausgestaltung seines internationalen Strafrechts und seiner damit einhergehenden Kompetenz zur Erstreckung des eigenen Rechts auf Sachverhalte mit Auslandsbezug.[169] Unberücksichtigt blieb hierbei jedoch, dass die nationalen Prinzipien des internationalen Strafrechts allenfalls Beispiele aus der Staatenpraxis darstellen, die völkerrechtlich im Allgemeinen anerkannt sind.[170]

a) Bestimmung des Erfolgsorts unter Berücksichtigung des Völkerrechts

Erforderlich ist also zusätzlich die Auslegung dieser Anwendungsregeln unter Heranziehung völkerrechtlicher Grundsätze.[171] Die Bestimmung des Erfolgsorts kann nicht unabhängig von den Regeln des Völkerrechts geschehen. Die potentiell weltweiten Wirkungen einer jeden im Internet begangenen Straftat verdeutlichen dieses Erfordernis. Bei undifferenzierter Anwendung nationalen Strafrechts durch Staaten, die gleichzeitig eine Zuständigkeitserklärung jedes dieser Staaten zur Verfolgung der im Internet begangenen Straftaten darstellt, würden nämlich unauflösbare Spannungen entstehen. Das Territorialitätsprinzip ist zwar als Ausgangspunkt für die Ausübung von Strafgewalt weltweit anerkannt,[172] gleichwohl ergeben sich aufgrund der unterschiedlichen Auslegung der Reichweite des Prinzips in den verschiedenen Staaten aber sogenannte positive Kompetenzkonflikte, denen nur durch restriktive Handhabung begegnet werden kann.[173]

---

[169] *Oehler*, Internationales Strafrecht, Rn. 111, Rn. 121; *Römer*, Verbreitungs- und Äußerungsdelikte im Internet, S. 99.

[170] So wohl *Holthausen*, NStZ 1992, 268, 268 f.; *Lehle*, Der Erfolgsbegriff und die deutsche Strafrechtszuständigkeit im Internet, S. 132 f.; *Martin*, Strafbarkeit grenzüberschreitender Umweltbeeinträchtigungen, S. 137; *Scholten*, Das Erfordernis der Tatortstrafbarkeit in § 7 StGB, S. 60 f.

[171] MünchKommStGB-*Ambos*, Vor §§ 3–7, Rn. 11; *Hilgendorf*, NJW 1997, 1873, 1877; *Lehle*, Der Erfolgsbegriff und die deutsche Strafrechtszuständigkeit im Internet, S. 133.

[172] Siehe hierzu nur American Society of International Law, AJIL 29 (1935), 480 ff.; Council of Europe, Extraterritorial criminal jurisdiction, S. 8; OECD, Computer-related Crime: Analysis of Legal Policy, S. 66; *O'Connor* et al., Model Codes for Post-Conflict Criminal Justice, S. 42; *Oehler*, Internationales Strafrecht, Rn. 153 f. – mit Nachweisen für das Territorialitätsprinzip, das sich in allen Rechtsordnungen weltweit wiederfindet; United Nations, Manual on the prevention and control of computer-related crime, Tz. 249.

[173] Council of Europe, Extraterritorial criminal jurisdiction, S. 8 f.; *ders.*, Recommendation No. (89) 9, Erläuternder Bericht, S. 84 f.; *Jennings*, BYIL 33 (1957), 146, 159; United Nations, Manual on the prevention and control of computer-related crime, Tz. 247 ff.; *Vander Beken* et al., Finding the Best Place for Prosecution, S. 11, Rn. 20 f.; S. 12, Rn. 23;

Nach den im Folgenden zu ermittelnden völkerrechtlichen Grenzen umfasst der Erfolgsbegriff i.S.d. § 9 Abs. 1, 3. Var. StGB nur Verletzungen und konkrete Gefährdungen des jeweils geschützten Rechtsguts als manifestierte tatbestandliche Erfolge. Mit der Verwirklichung eines abstrakten oder abstrakt-konkreten Gefährdungsdelikts wird hingegen kein den völkerrechtlichen Anforderungen genügender Erfolgstatort und damit keine Zuständigkeit deutscher Strafverfolgungsbehörden begründet.

Immer wenn die Strafverfolger einen Erfolgsort i.S.d. § 9 Abs. 1, 3. Var. StGB bei extraterritorialem Handeln des Täters im Internet annehmen und infolgedessen das deutsche Strafrecht anwenden, wirken sie auf einen Sachverhalt ein, der sich auch auf dem Hoheitsgebiet zumindest eines weiteren anderen Staates ereignete. Eine solche Anwendung des nationalen Rechts auf im Ausland handelnde Personen wird, obwohl die unmittelbare Ausübung der Hoheitsgewalt selbst auf das eigene Staatsgebiet begrenzt ist, missverständlich als „extraterritoriale Hoheitsausübung" bezeichnet.[174] Die hoheitliche Handlung ist jedoch nur insoweit extraterritorial, als sie sich auf dem Territorium eines weiteren Staates auswirkt,[175] etwa indem sie sich als Normbefehl an Personen richtet, die sich auf fremdem Territorium befinden.

aa) Völkerrechtliches Konfliktpotenzial bei Ausdehnung des Strafrechts

Um die Grenzen für eine extraterritoriale Hoheitsausübung bestimmen zu können, ist zunächst zu klären, in welchen Fallkonstellationen durch den normativen Regelungs- und Geltungsanspruch der nationalen Regeln des internationalen Strafrechts auf Taten, die im Ausland begangen wurden und im Inland einen Erfolg i.S.d. § 9 Abs. 1, 3. Var. StGB hervorgerufen haben könnten, positive völkerrechtliche Konflikte entstehen. Ausgangspunkt ist die Überlegung, dass sich der deutsche Staat durch die Ausdehnung seines Strafrechts u.U. in das völkerrechtlich geschützte Recht eines dritten Staates auf Selbstbestimmung einmischen könnte, indem er die innere Ordnung des betroffenen Staates stört bzw. mit dessen Regelungsgewalt in Konkurrenz tritt.

Das Völkerrecht beruht wie bereits erwähnt[176] im Wesentlichen auf dem Gebot der Achtung der souveränen Staatengleichheit, dessen näheren Anwendungsbereich u.a. das Gebot der Achtung der Gebietshoheit (nachfolgend unter (1)), das Einmischungs- und Interventionsverbot (unter (2)) sowie das Gebot der Achtung fremder Hoheitsakte (unter (3)) näher umreißen. Sind diese Grundprinzipien durch die Aus-

---

zum historischen Wandel der Auslegung des Territorialitätsprinzips, siehe *Bertele*, Souveränität und Verfahrensrecht, S. 65 ff.

[174] *Meng*, ZaöRV 44 (1984), 675, 727 f.; *Schlochauer*, Die extraterritoriale Wirkung von Hoheitsakten, S. 10 f.; *Ziegenhain*, Extraterritoriale Rechtsanwendung, S. 1.

[175] *Schlochauer*, Die extraterritoriale Wirkung von Hoheitsakten, S. 10 f.; *Ziegenhain*, Extraterritoriale Rechtsanwendung, S. 1 f.

[176] Siehe hierzu die Ausführungen unter Teil 1, I.

dehnung des Anwendungsbereichs der nationalen Strafrechtsnormen betroffen, so entsteht eine Konfliktsituation.

(1) Gebot der Achtung der Gebietshoheit

Nach dem Gebot der Achtung der Gebietshoheit ist kein Staat – vorbehaltlich einzelner, seltener Ausnahmen – berechtigt, unmittelbar auf fremdes Territorium einzuwirken.[177] Die bloße Ausdehnung der Strafbarkeit auf im Ausland handelnde Personen beinhaltet jedoch grundsätzlich keine Beeinträchtigung der Gebietshoheit des ausländischen Staates, da es an einer unmittelbaren Einwirkung auf dessen Territorium fehlt. Allein die Anwendbarkeitserklärung des deutschen Strafrechts auf einen Sachverhalt führt nur zu mittelbaren rechtlichen oder tatsächlichen Folgen, die sich auf dem Gebiet eines anderen Staates auswirken können. Ein unmittelbarer Eingriff, wie das Tätigwerden im Rahmen der Strafverfolgung auf dem fremden Territorium (Ladung, Verhör oder gar Ergreifung[178] eines Beschuldigten), wird allein durch die Anwendung des deutschen Strafrechts auf einen Sachverhalt noch nicht vorgenommen.[179] Ebenso verhält es sich mit Ermittlungsmaßnahmen der Strafverfolgungsbehörden im Inland, die aber im Einzelfall durchaus extraterritoriale Auswirkungen nach sich ziehen können.[180]

(2) Einmischungs- und Interventionsverbot

Das Einmischungs- und Interventionsverbot schützt das sich aus dem Gebot der Achtung der souveränen Staatengleichheit ergebende Recht auf Selbstbestimmung.[181] Mit der grenzüberschreitenden Regelung und Anwendung nationaler Strafrechtsnormen auf Sachverhalte, bei denen der Täter im Ausland gehandelt hat, ist eine Einmischung oder Intervention in das Recht auf Selbstbestimmung des anderen Staates verbunden, wenn der Rechtsanwender auf die Willensbildung des

---

[177] Council of Europe, Extraterritorial criminal jurisdiction, S. 18; *Doehring*, Völkerrecht, Rn. 88 f.; *Geiger*, Grundgesetz und Völkerrecht mit Europarecht, S. 315; *Ipsen*, Völkerrecht, § 23, Rn. 67, 69; *Proelß*, in: Graf Vitzthum/Bothe, Völkerrecht, 5. Abschnitt, Rn. 16; *Rehbinder*, Extraterritoriale Wirkungen des deutschen Kartellrechts, S. 394; *Schwörer*, wistra 2009, 452, 453; *Siegrist*, Hoheitsakte auf fremdem Staatsgebiet, S. 10 f.; *Spang-Hanssen*, Cyberspace & International Law, S. 209, 439; *Stein/v. Buttlar*, Völkerrecht, Rn. 537.

[178] So z.B. bei der Entführung *Adolf Eichmanns* durch den israelischen Geheimdienst aus Argentinien im Jahr 1960; *Stein/v. Buttlar*, Völkerrecht, Rn. 541.

[179] Vgl. hierzu auch StIGH 5, 73, 90, 104 f.; *Hermanns*, Völkerrechtliche Grenzen, S. 18 m.w.N.; *Rehbinder*, Extraterritoriale Wirkungen des Kartellrechts, S. 338.

[180] Siehe hierzu die Ausführungen unter Teil 3, II.A.–E.

[181] *Bertele*, Souveränität und Verfahrensrecht, S. 176; Council of Europe, Extraterritorial criminal jurisdiction, S. 21 f.; *Dahm/Delbrück/Wolfrum*, Völkerrecht, Bd. I/3, S. 797; *Pappas*, Stellvertretende Strafrechtspflege, S. 77; *Verdross/Simma*, Universelles Völkerrecht, § 490; *Ziegenhain*, Extraterritoriale Rechtsanwendung, S. 31.

jeweils betroffenen Staates einwirkt oder der Gesetzgeber Angelegenheiten regelt, die in die alleinige Regelungskompetenz eines anderen Staates fallen (sog. innere Angelegenheiten).[182] Die Ausübung der Selbstbestimmung des regelnden Staates fällt dagegen grundsätzlich nicht unter die Verbote; selbst soweit hiermit im Einzelfall auch eine extraterritoriale Wirkung verbunden ist, da diese regelmäßig nur einen Reflex darstellt.[183]

Anders verhält es sich allerdings, wenn Ziel der Selbstbestimmung auch die Gestaltung einer fremden Gesellschaft ist. Denkbar ist etwa, dass durch die Ausdehnung des Strafrechts der deutsche Gesetzgeber Einfluss auf die politische Willensbildung eines anderen Staates nimmt, indem er beispielsweise bestimmte Formen oder Inhalte politischer Entscheidungen unter Strafe stellt. Dass solche politischen Entscheidungen einen Erfolgstatort in Deutschland aufweisen, ist etwa in den Fällen staatlicher Aufrufe zum Mord möglich[184] – z.B. im Fall des Mordaufrufs durch eine Fatwa des Ajatollah *Khomeini* gegen *Salman Rushdie* wegen der Veröffentlichung seines Werks „Die Satanischen Verse“. Fühlen sich in Deutschland lebende Personen zur Ausführung des Mordes angesprochen oder soll das potentielle Opfer in Deutschland ermordet werden, liegt ein Erfolgsort auch in Deutschland. Der Anwendungsbereich des Interventionsverbotes ist in solchen Fällen durch die Erstreckung des Strafrechts eröffnet; eine völkerrechtliche Konfliktlage entsteht.

Völkerrechtliche Konfliktlagen ruft die Anwendung des deutschen Strafrechts auf Taten mit Auslandsbezug auch dann hervor, wenn Rechtsverhältnisse im Ausland durch abweichende Regelungen mittels nationaler Ver- und Gebotsnormen infrage gestellt werden.[185] Freiheiten, die ein Staat seinen Bürgern gewährt, sind seine Angelegenheit. Mit der Anwendung des deutschen Strafrechts etwa auf Personen, die im Ausland Inhalte ins Internet einstellen und einen Erfolg i.S.d. § 9 Abs. 1, 3. Var. StGB herbeiführen, wird gleichzeitig die Rechtmäßigkeit der Ausübung der im Ausland gewährten Freiheiten in Zweifel gezogen. Infolge der Beschränkung kommt es zu einem Eingriff in die innere Organisation des betroffenen Staates, sodass eine Einmischung im Sinne des Völkerrechts vorliegt. Besonders deutlich wird dies am Beispiel der nahezu unumschränkten Meinungsäußerungsfreiheit auf der Grundlage des First Amendment zur Verfassung der USA. Danach

---

[182] MünchKommStGB-*Ambos*, Vor §§ 3–7, Rn. 11; *Spang-Hanssen*, Cyberspace & International Law, S. 351.

[183] *Bertele*, Souveränität und Verfahrensrecht, S. 177.

[184] Ebenda, S. 90.

[185] *Jeßberger*, JR 2001, 432, 434; *Pappas*, Stellvertretende Strafrechtspflege, S. 78; siehe auch *Eisele*, JA 2000, 424, 425; *Hilgendorf*, ZStW 113 (2001), 650, 660 ff., die jedoch generell in der grenzüberschreitenden Anwendung nationaler Strafrechtsnormen einen Eingriff in die Souveränität, insbesondere einen Verstoß gegen das Nichteinmischungsprinzip sehen; a.A. *Poenig*, Die strafrechtliche Haftung des Linkanbieters, S. 203, der davon ausgeht, dass das Nichteinmischungsprinzip bei Vorliegen eines objektiven Bezugs der Tat zu Deutschland nicht betroffen ist, wenn am Handlungsort keine gesetzliche Regelung die Handlung als strafbar deklariert.

unterfallen selbst rassistische und nach deutschem Recht volksverhetzende Aussagen einem besonderen, staatstragenden Schutz.[186] Eine Bestrafung wegen solcher Äußerungen auf der Grundlage deutschen Strafrechts konterkariert die Freiheitsgewährung, für die sich die USA gegenüber jeder im Inland handelnden Person entschieden haben. Durch den sogenannten SPEECH Act[187] haben die USA dementsprechend die inländische Durchsetzung ausländischer Urteile, die ihrer Vorstellung von Meinungsäußerungsfreiheit widersprechen, sogar unterbunden.

Keine Einmischung liegt dagegen vor, wenn das deutsche Strafrecht ein Verhalten für strafbar erklärt, das auch am ausländischen Handlungsort strafbar ist (identische Norm). In diesem Fall wird die vom ausländischen Staat aufgestellte und mit den Mitteln des Strafrechts verteidigte Rechts- und Werteordnung nicht beeinträchtigt,[188] sondern bestätigt. Dort, wo eine ausdrückliche Entscheidung des ausländischen Gesetzgebers für oder gegen ein strafbewehrtes Verbot fehlt, ist indes nach dem Zweck des Untätigbleibens zu fragen. Bei einer bloßen unbeabsichtigten Regelungslücke ist durch Auslegung der Wille des ausländischen Gesetzgebers in der Regel feststellbar. In den Fällen, in denen die Lücke bewusst gelassen wurde, um die Ausgestaltung der Rechtslage anderen Mechanismen, insbesondere dem Gewohnheits- oder Richterrecht, zu überlassen, ist diese Gesetzgebungstechnik eine innere Angelegenheit von staatsprägender Natur. Diese Strukturen würden durch die Rechtsetzung eines anderen Staates abgewandelt werden. Deshalb liegt in letzteren Fällen eine Einmischung vor, wenn auch in geringerem Maße als in den Fällen der Ausdehnung des deutschen Strafrechts auf Fälle, die nach dem Recht des Auslands ausdrücklich erlaubt sind.

(3) Gebot der Achtung fremder Hoheitsakte

Das Gebot der Achtung fremder Hoheitsakte beinhaltet die Pflicht, die bereits eingetretene Feststellungs-, Befehls- oder Gestaltungswirkung, die fremde Hoheitsakte sich nach eigenem Recht beimessen, grundsätzlich zu respektieren.[189] In das Gebot der Achtung fremder Hoheitsrechte greift der deutsche Staat ein, wenn der ausländische Staat die Vornahme einer auf seinem Staatsgebiet stattfindenden Handlung erlaubt, der deutsche Staat aber sein Strafrecht für anwendbar erklärt und eben dieses Verhalten wegen seiner Auswirkungen auf dem eigenen Staatsgebiet und fehlender deutscher Erlaubnis unter Strafe stellt. Als Beispielsfall lässt sich das im Staat des Handlungsorts ausdrücklich genehmigte Veranstalten von Glücksspie-

---

[186] *Holznagel*, AfP 2002, 128, 129 f.; *Weingärtner*, AfP 2002, 134, 134 f.

[187] Securing the Protection of our Enduring and Established Heritage Act v. 10.8.2010, abrufbar unter http://www.gpo.gov/fdsys/pkg/PLAW-111publ223/pdf/PLAW-111publ223.pdf [Stand: 6.11.2013].

[188] *Meessen*, Völkerrechtliche Grundsätze des internationalen Kartellrechts, S. 118 f.; *Spang-Hanssen*, Cyberspace & International Law, S. 350.

[189] *Verdross/Simma*, Universelles Völkerrecht, § 1021.

len im Internet anführen.[190] Hier impliziert die Anwendung eigenen Strafrechts auf den ausländischen Sachverhalt, dass die fremde Genehmigung rechtlich nicht existent sei, wenn eine Ausübung des genehmigten Verhaltens ohne Kollision mit dem deutschen Recht praktisch nicht möglich ist. Derzeit gibt es nämlich noch keine verlässlichen und wirtschaftlich vertretbaren technischen Systeme, die den Seitenabruf im Internet zuverlässig auf bestimmte Nationen beschränken.[191]

Die Behandlung einer ausländischen Genehmigung als nicht bestehend stellt grundsätzlich eine Missachtung des fremden Hoheitsakts dar, sodass auch der Anwendungsbereich dieses völkerrechtlichen Prinzips eröffnet ist und eine völkerrechtliche Konfliktlage entsteht.

bb) Völkerrechtliche Befugnis zur Ausdehnung des Strafanwendungsrechts

Liegt nach den obigen Ausführungen eine völkerrechtliche Konfliktlage vor, muss der eingreifende Staat des Weiteren nach dem Völkerrecht befugt sein, sein nationales Recht auf im Ausland handelnde Personen anzuwenden. Hierzu ist er im Grundsatz berechtigt, da das Völkerrecht nicht vorgibt, dass der räumliche Geltungsbereich nationaler Normen an der Staatsgrenze enden muss.[192] Völkerrechtlich grundsätzlich unzulässig ist nur die eigenständige Vornahme einer Hoheitsausübung auf fremdem Territorium, weil der Staat in diesem Fall regelmäßig in die Souveränität des betroffenen Drittstaates eingreift.[193]

Das jedem Nationalstaat aufgrund seiner Souveränität gegebene Recht zur Ausgestaltung seines internationalen Strafrechts und damit einhergehend seiner Kompetenz zur Erstreckung des eigenen Rechts auf Sachverhalte mit Auslandsbezug ist gleichwohl aber nicht unbegrenzt;[194] anderenfalls wäre ein staatenübergreifendes

---

[190] Im Allgemeinen zur Glücksspielproblematik: BGH MMR 2004, 529 ff.; EuGH NJW 2004, 139 ff.; *Klam*, Die rechtliche Problematik von Glücksspielen im Internet, S. 123 ff.; *Klengel/Heckler*, CR 2001, 243 ff.; *Leupold/Bachmann/Pelz*, MMR 2000, 648 ff.

[191] Vgl. zu Betrachtungen der „Reterritorialisierung des Internet" *Hoeren*, MMR 2007, 3, 5 f.; *Lessig/Resnik*, Michigan Law Review, vol. 98, 1999, 395, 399; *Mitsdörffer/Gutfleisch*, MMR 2009, 731, 731 f.; *Sankol*, K&R 2008, 279, 283.

[192] *Determann*, Kommunikationsfreiheit im Internet, S. 164 f.; *Ipsen*, Völkerrecht, § 23, Rn. 87; *Rehbinder*, Extraterritoriale Wirkungen des Kartellrechts, S. 53; *Ziegenhain*, Extraterritoriale Rechtsanwendung, S. 3 f.

[193] *Bertele*, Souveränität und Verfahrensrecht, S. 78 ff., 89, 93; Council of Europe, Extraterritorial criminal jurisdiction, S. 18; *Jescheck/Weigend*, Strafrecht AT, § 18 I 4 (S. 166); *Rudolf*, in: BerDGesVölkR 11, S. 7, 33 f.; *Stein/v. Buttlar*, Völkerrecht, Rn. 537; *Ziegenhain*, Extraterritoriale Rechtsanwendung, S. 2.

[194] MünchKommStGB-*Ambos*, Vor §§ 3–7, Rn. 11; *Germann*, SchwZStR 1954, 237, 237; *Ipsen*, Völkerrecht, § 23, Rn. 87; *Jescheck/Weigend*, Strafrecht AT, § 18 I 2 (S. 164 f.); *Kunig/Uerpmann*, Jura 1994, 186, 192; *Martin*, Strafbarkeit grenzüberschreitender Umweltbeeinträchtigungen, S. 135 f.; *Pappas*, Stellvertretende Strafrechtspflege, S. 76; *Schmitt*, FS 600 Jahre Würzburger Juristenfakultät, S. 357, 359; *Scholten*, Das Er-

friedliches Zusammenleben nämlich unmöglich. Ein Nationalstaat darf Sachverhalte mit Auslandsberührung nur dann regeln, wenn dies nicht willkürlich geschieht. Dem Rechtsanwender ist es korrespondierend mit der Regelungsbefugnis des Nationalstaates nicht gestattet, eine Norm über die Regelungsbefugnis des Gesetzgebers hinaus anzuwenden. Wo die konkreten Grenzen für eine extraterritoriale Hoheitsausübung zu ziehen sind, ist allerdings streitig.

Nach einer Ansicht ist eine konkrete völkerrechtliche Erlaubnisnorm für die extraterritoriale Hoheitsausübung eines Staates notwendig.[195] Die weitaus h.M. verzichtet dagegen auf eine solche Norm und fordert lediglich, dass der Befugnis zur Anwendung des nationalen Strafrechts auf im Ausland handelnde Täter eine völkerrechtliche Verbotsnorm nicht entgegensteht.[196]

Gestützt wird letztere Ansicht durch die sogenannte „Lotus"-Entscheidung[197] des Ständigen Internationalen Gerichtshofs (StIGH). Dieser musste darüber befinden, ob ein Staat einen strafbewehrten Erfolg auf einem Schiff unter seiner Flagge trotz ausländischen Handlungsorts ahnden darf. Hintergrund der Entscheidung war ein Zusammenstoß zweier unter verschiedenen Flaggen fahrender Schiffe auf Hoher See. Ein französischer Wachoffizier hatte einen nach türkischem Recht strafbewehrten Erfolg, den Tod von acht türkischen Staatsangehörigen, auf dem unter türkischer Flagge fahrenden Kohlendampfer „Boz-Kourt" durch die Kollision des von ihm gesteuerten, unter französischer Flagge fahrenden Postdampfers „Lotus" herbeigeführt. Die Türkei wandte daraufhin das türkische Strafrecht auf den Franzosen an.[198] Der StIGH stellte in diesem Fall fest, dass nicht maßgeblich sei, ob für die Ausweitung der Ausübung der nationalen Gerichtsbarkeit ein positives Recht im Völkerrecht bestehe, sondern ob ein solches der Ausdehnung entgegenstehe.[199] Die Ausübung von Hoheitsgewalt sei nicht von der Existenz einer positiven völkerrechtlichen Norm abhängig, sondern ergebe sich aus der Souveränität des Staates selbst. Sie sei nur in Ausnahmefällen durch Verbotsregeln beschränkt.[200] Eine

---

fordernis der Tatortstrafbarkeit in § 7 StGB, S. 56 ff.; *Schroeder*, NJW 1969, 81, 81 ff.; *Stein/v. Buttlar*, Völkerrecht, Rn. 602 i.V.m. 606; *Walter*, JuS 2006, 870, 870 f.; *Weigend*, in: Holoch, Recht des Internet, S. 85, 87.

[195] *Bruns*, ZaöRV 1 Teil 1 (1929), 1, 53 f.; *Loder* im Sondervotum, StIGHE 5, 73, 107 ff.; *Mosler*, ZaöRV 36 (1976), 6, 40 f.; *Schlochauer*, Die extraterritoriale Wirkung von Hoheitsakten, S. 51 ff.; *Weiss* im Sondervotum, StIGHE 5, 73, 119 ff.

[196] *Bertele*, Souveränität und Verfahrensrecht, S. 61 f., 74 f.; *Ipsen*, Völkerrecht, § 23, Rn. 90; *Meng*, ZaöRV 44 (1984), 675, 740; *Pappas*, Stellvertretende Strafrechtspflege, S. 76; *Rehbinder*, Extraterritoriale Wirkungen des Kartellrechts, S. 53 f., 68; *Rudolf*, in: BerDGesVölkR 11, S. 7, 18 ff.; United Nations, Manual on the prevention and control of computer-related crime, Tz. 257; *Verdross/Simma*, Universelles Völkerrecht, § 1022; *Ziegenhain*, Extraterritoriale Rechtsanwendung, S. 3.

[197] PCIJ, Série A, n° 10. = StIGHE 5, 73 ff.

[198] StIGHE 5, 73, 80 ff.

[199] StIGHE 5, 73, 90 f.

[200] StIGHE 5, 73, 90.

Konkretisierung dieser Verbotsregeln nahm der Gerichtshof jedoch nicht vor. Nach seiner Ansicht war die Ausdehnung der Anwendung des nationalen Strafrechts seitens der Türkei zulässig, da im internationalen Recht kein Anhaltspunkt für eine Begrenzung des Geltungsbereichs der Strafnormen bestehe.[201] Die Feststellung des StIGH, dass keine positive Erlaubnisnorm für die extraterritoriale Hoheitsausübung erforderlich ist, ist auch heute noch nicht konventionsrechtlich[202] überholt.[203] Der StIGH beantwortete vielmehr insoweit eine grundsätzliche Frage.[204]

Sein Nachfolger, der IGH, relativierte 1996 durch die Advisory Opinion on the Legality of the Threat or Use of Nuclear Weapons[205] die vorgenannte Aussage allerdings für eine besondere Sachverhaltskonstellation. Er erklärte trotz fehlender Nachweisbarkeit einer ausdrücklichen vertrags- oder gewohnheitsrechtlichen Verbotsnorm die Bedrohung mit oder den Einsatz von Atomwaffen unter ganz besonders extremen Bedingungen entgegen der Linie im „Lotus-Fall“ nicht ausdrücklich für zulässig.[206] Ein generelles Abrücken des IGH von dem Verzicht auf eine positive Erlaubnisnorm ist damit indes nicht verbunden. Vielmehr ist die neuere Entscheidung im Zusammenhang mit der besonderen zu entscheidenden Sachverhaltsproblematik zu sehen.

Die herrschende – auf eine positive Erlaubnisnorm verzichtende – Meinung verdient Zustimmung. Die extraterritoriale Hoheitsausübung ist allerdings nicht schon deshalb ohne positive völkerrechtliche Norm zulässig, weil jede sich auf einen Staat auswirkende strafbare Handlung bereits eine Einmischung in die inneren Angelegenheiten darstellt und die extraterritoriale Hoheitsausübung dadurch herausgefordert würde.[207] Verübt eine (nicht staatlich gelenkte) Privatperson eine strafbare Tat, führt diese nämlich nicht automatisch bereits zu einem Angriff auf die Souveränität des Drittstaates. Das Souveränitätsprinzip dient nur der Abgrenzung der Rechte der Staaten untereinander,[208] nicht aber der Abgrenzung der Rechte zwischen einem Bürger und einem Drittstaat. Für einen Verzicht auf eine positive Er-

---

201 StIGHE 5, 73, 104 f.

202 Art. 11 Übereinkommen über die Hohe See vom 29.4.1958, BGBl. II 1972, S. 1091, 1094 mit Ausführungsgesetz vom 21.9.1972 (BGBl. II 1972, S. 1089) betrifft nicht die Entscheidung, ob eine generelle Erlaubnisnorm erforderlich ist, sondern nur den konkreten Anknüpfungspunkt.

203 *Dahm/Delbrück/Wolfrum*, Völkerrecht, Bd. I/1, S. 320 ff.; *Meng*, ZaöRV 44 (1984), 675, 738; *Verdross/Simma*, Universelles Völkerrecht, S. 778 ff.; a.A. *Kienle*, Internationales Strafrecht und Straftaten im Internet, S. 156.

204 StIGHE 5, 73, 89; *Becker*, in: Menzel et al., Völkerrechtssprechung, S. 294; *Rehbinder*, Extraterritoriale Wirkungen des Kartellrechts, S. 70.

205 ICJ Rep. 1996, 226 ff.

206 Siehe zu diesem Problemfeld *Becker*, in: Menzel et al., Völkerrechtssprechung, S. 297 f., 847 ff. m.w.N.

207 I.d.S. aber *Martin*, Strafbarkeit grenzüberschreitender Umweltbeeinträchtigungen, S. 141.

208 *Ipsen*, Völkerrecht, § 5, Rn. 7 f.

laubnisnorm als Befugnis zur extraterritorialen Hoheitsausübung spricht aber, dass der betroffene Staat anderenfalls so lange Zurückhaltung üben müsste, bis sich eine entsprechende völkerrechtliche Überzeugung herausgebildet hat. In Konfliktsituationen wird sich für gewöhnlich jedoch kein eingriffslegitimierendes völkerrechtliches Gewohnheitsrecht bilden können. Ein effektiver Schutz der Strafverfolgungsinteressen der jeweils betroffenen Staaten durch Anwendung des eigenen Strafrechts auf den konkreten Sachverhalt wäre folglich kaum möglich.[209]

cc) Begrenzung der Befugnis zur Ausdehnung des Strafrechts

Die Begrenzung der Berechtigung zu extraterritorialer Hoheitsausübung über Verbotsnormen ist allerdings schwierig, weil diese Normen nur selten völkervertraglichen Regelungen entnommen werden können. Für die Anwendung des deutschen Strafrechts auf ausländische Aktivitäten im Internet, durch die im Inland Erfolge i.S.d. § 9 Abs. 1, 3. Var. StGB hervorgerufen werden, lassen sich keine abschließenden speziellen völkervertraglichen Regelungen finden. Die am 1.7.2004 in Kraft getretene Convention on Cybercrime (CCC) des Europarates vom 23.11.2001[210] ist zwar ein multilateraler völkerrechtlicher Vertrag, der sich auch mit der Frage der Gerichtsbarkeit beschäftigt und den Deutschland nach und nach umgesetzt hat.[211] Die Konvention regelt in Art. 22 aber lediglich – primär abstellend auf das Territorialitätsprinzip und ergänzend auf das aktive Personalitätsprinzip – einen Mindestanwendungsbereich.[212] Das Vertragswerk enthält also weder Vorschriften über die Bestimmung des Tatorts, an dem die Straftat begangen wurde, noch Normen für die Ermittlung des Verhältnisses von ausländischem und in-

---

[209] *Martin*, Strafbarkeit grenzüberschreitender Umweltbeeinträchtigungen, S. 141 f.; *Meng*, ZaöRV 44 (1984), 675, 740.

[210] Europarat, ETS No. 185.

[211] Siehe beispielsweise das einundvierzigste Strafrechtsänderungsgesetz zur Bekämpfung der Computerkriminalität vom 7.8.2007, BGBl. I 2007, S. 1786 ff.; das Inkrafttreten des Übereinkommens über Computerkriminalität zum 1.7.2009 wurde am 29.4.2010 im BGBl. 2010 II Nr. 9 S. 218–240 verkündet.

[212] Art. 22 CCC lautet in deutscher Übersetzung: „(1) Jede Vertragspartei trifft die erforderlichen gesetzgeberischen und anderen Maßnahmen, um ihre Gerichtsbarkeit über die nach den Artikeln 2 bis 11 umschriebenen Straftaten zu begründen, wenn die Straftat wie folgt begangen wird: (a) ihrem Hoheitsgebiet; […] (d) einem ihrer Staatsangehörigen, wenn die Straftat nach dem am Tatort geltenden Recht strafbar ist oder die Straftat außerhalb des Hoheitsbereichs irgendeines Staates begangen wird. […] (5) die Gerichtsbarkeit für eine mutmaßliche Straftat, die nach diesem Übereinkommen umschrieben ist, von mehr als einer Vertragspartei geltend gemacht, so konsultieren die beteiligten Vertragsparteien einander, soweit angebracht, um die für die Strafverfolgung geeignetste Gerichtsbarkeit zu bestimmen.“

ländischem Strafrecht, sondern lediglich eine auf Freiwilligkeit beruhende Konsultierungsaufforderung im Konfliktfall.[213]

Trotz dieser Schwierigkeiten besteht im Übrigen aber Einigkeit darüber, dass die staatliche Regelungshoheit nicht beliebig ausgeübt werden darf, da anderenfalls ein „anarchistisches Chaos" innerhalb der Staatengemeinschaft eintreten würde. Wodurch und inwieweit die Befugnis zur Regelung der Anwendbarkeit nationalen Strafrechts auf Sachverhalte mit Auslandsbezug begrenzt ist, wird jedoch unterschiedlich beurteilt. Während einige an völkerrechtlichen Verbotsnormen, insbesondere an dem Rechtsmissbrauchsverbot, ansetzen[214] (nachfolgend unter (1)), verlangen andere einen besonderen Anknüpfungspunkt (sog. *genuine link*)[215] (unter (2)) oder fordern eine Interessenabwägung[216] (unter (3)).

(1) Untauglichkeit des Rechtsmissbrauchsverbots als Befugnisbegrenzung

Als eine nicht völkervertragsrechtlich festgelegte[217] Grenze der Befugnis zur extraterritorialen Hoheitsausübung ziehen einige Literaturvertreter das Verbot rechtsmissbräuchlichen Verhaltens heran.[218] Verstoße ein Staat gegen dieses Verbot, sei eine extraterritoriale Hoheitsausübung rechtswidrig.

Der Inhalt des Rechtsmissbrauchsverbots ist allerdings nicht klar bestimmt. Während teilweise nur auf eine nicht rechtmäßige Ausübung eines Rechts durch den jeweiligen Rechtsträger abgestellt wird, fällt nach anderer Auffassung bereits der willkürliche oder unvernünftige Gebrauch absoluter Rechte oder aber erst die absichtliche Schadenszufügung unter das Verbot rechtsmissbräuchlichen Verhal-

---

[213] Zur Freiwilligkeit der Konsultation dritter Staaten im Konfliktfall siehe die deutsche Denkschrift zur Umsetzung der Konvention, BT-Drucks. 16/7218, S. 51; siehe auch Tz. 239 des Erläuternden Berichts zur Konvention.

[214] Nachweise bei *Ipsen*, Völkerrecht, § 39, Rn. 44; *Rudolf*, in: BerDGesVölkR 11, S. 7, 19.

[215] *Dahm/Dehlbrück/Wolfrum*, Völkerrecht, Bd. I/1, S. 215; *Pappas*, Stellvertretende Strafrechtspflege, S. 81; *Ziegenhain*, Extraterritoriale Rechtsanwendung, S. 3.

[216] Siehe nur American Law Institute, Restatement Foreign Rel. Law 2nd, § 40, in dem eine Abwägungspflicht unter nicht abschließender Aufführung bestimmter Faktoren postuliert wird; dass., vol. 1 Restatement Foreign Rel. Law 3rd, § 403, in dem eine ausdrücklich nicht abschließende Liste von abzuwägenden Kriterien aufgeführt ist, sowie § 441, in welchem die Abwägungskriterien präzisiert werden; *Biehler* et al., Freiburg Proposal, S. 7 f., zur Ausgestaltung der einzelnen Stufen siehe S. 9 ff.; Council of Europe, Extraterritorial criminal jurisdiction, S. 31 f.; *Lagodny*, Strafgewaltkonflikte, S. 132 ff.; *Vander Beken* et al., Finding the Best Place for Prosecution, S. 24, Rn. 67, zur Ausgestaltung der einzelnen Phasen siehe S. 31 ff., zusammenfassend S. 46, Rn. 139–141, S. 59 ff.; siehe auch *Vander Beken/Vermeulen/Lagodny*, NStZ 2002, 624, 626 ff.

[217] *Neuhaus*, Das Rechtsmissbrauchsverbot im heutigen Völkerstrafrecht, S. 119 ff.

[218] Nachweise bei *Ipsen*, Völkerrecht, § 39, Rn. 44; *Rehbinder*, Extraterritoriale Wirkungen des Kartellrechts, S. 56 f.; *Rudolf*, in: BerDGesVölkR 11, S. 7, 19; *Spang-Hanssen*, Cyberspace & International Law, S. 240.

tens.[219] Das Verbot ist zudem nicht in allen Rechtsordnungen als Prinzip des innerstaatlichen Rechts anerkannt.[220] Sogar einige hoch entwickelte Rechtsordnungen enthalten kein solches Verbot.[221] Soweit es in anderen Rechtsordnungen normiert ist, lässt sich ein übereinstimmender Inhalt nur schwer bestimmen.[222] In der völkerrechtlichen Rechtsprechung von StIGH und IGH findet das Verbot rechtsmissbräuchlichen Verhaltens ebenfalls keine Anerkennung.[223] Die Gerichtshöfe gingen in ihren Entscheidungen, wenn überhaupt, nur beiläufig auf dieses Verbot ein und nutzten es nicht zur Anspruchsbegründung.

Seine Untauglichkeit zur Bestimmung der Grenzen der extraterritorialen Hoheitsausübung ergibt sich ferner daraus, dass es erst eingreifen soll, wenn das staatliche Handeln an sich auf einer anerkannten rechtlichen Grundlage beruht, dieses Recht aber entgegen seiner Bestimmung genutzt und damit unter dem Deckmantel der grundsätzlich zulässigen Rechtsausübung in Rechte Dritter eingegriffen wird. Das Rechtsmissbrauchsverbot knüpft also an eine spezielle Erlaubnis zur Hoheitsausübung an und kann deshalb keine Grenzen für die allgemeine völkerrechtliche Erlaubnis setzen; es ist für eine andere Fallgruppe konstruiert. Unter diesen Voraussetzungen sind aus dem Rechtsmissbrauchsverbot keine allgemeinen Grenzen für die extraterritoriale Hoheitsausübung herzuleiten.[224]

Infolge der wesentlichen Unterschiede bei der Akzeptanz und bei der Ausfüllung des Rechtsmissbrauchsverbots auf nationaler und internationaler Ebene sowie des Zuschnitts auf andere Fälle kann dieses Verbot im Völkerrecht folglich nicht als maßgebliche Grenze für die Zulässigkeit der Regelung von Sachverhalten mit Auslandsbezügen dienen.[225]

---

[219] *Bertele*, Souveränität und Verfahrensrecht, S. 173 ff.; *Ipsen*, Völkerrecht, § 39, Rn. 44 ff. – jeweils mit einer Darstellung der verschiedenen Ansichten über den Umfang des Rechtsmissbrauchsverbots.

[220] *Ipsen*, Völkerrecht, § 39, Rn. 46; *Neuhaus*, Das Rechtsmissbrauchsverbot im heutigen Völkerrecht, S. 17 ff., 46 ff. – zur Verwendung des Begriffs „Rechtsmissbrauchsverbot" in Literatur und Rechtsprechung.

[221] *Neuhaus*, Das Rechtsmissbrauchsverbot im heutigen Völkerrecht, S. 162 ff.

[222] *Ipsen*, Völkerrecht, § 39, Rn. 46; *Lehle*, Der Erfolgsbegriff und die deutsche Strafrechtszuständigkeit im Internet, S. 126 f.

[223] *Bertele*, Souveränität und Verfahrensrecht, S. 175 f.; *Ipsen*, Völkerrecht, § 39, Rn. 45; *Neuhaus*, Das Rechtsmissbrauchsverbot im heutigen Völkerrecht, S. 127 ff.; *Rudolf*, in: BerDGesVölkR 11, S. 7, 20.

[224] *Bertele*, Souveränität und Verfahrensrecht, S. 176, der im Ergebnis sogar das Rechtsmissbrauchsverbot nicht als einen von der Judikatur formulierten, fest etablierten und konturierten Rechtssatz sieht; *Ipsen*, Völkerrecht, § 39, Rn. 46; *Nordmann*, Die Beschaffung von Beweismitteln, S. 172 f.

[225] *Bertele*, Souveränität und Verfahrensrecht, S. 176; *Rudolf*, in: BerDGesVölkR 11, S. 7, 16, 19 ff.

(2) Keine hinreichende Konfliktlösung durch *genuine link*

Die wohl h.M. sieht das sogenannte *genuine link*-Erfordernis als Regelungsinstrument zur völkerrechtlichen Beschränkung der Befugnis zur extraterritorialen Hoheitsausübung an.[226] Das genannte Erfordernis ist historisch gewachsen. Die Staaten waren schon aus Praktikabilitätsgründen stets bestrebt, ihr nationales Recht auf einen sich im Ausland zutragenden Sachverhalt nur bei einer besonderen Beziehung zu diesem anzuwenden.[227] Nach wohl h.M. bedarf ein Staat bei einer Handlung mit extraterritorialem Bezug folglich einer besonderen Beziehung zum Regelungsobjekt bzw. –subjekt, also eines sinnvollen Anknüpfungspunkts bzw. einer rechtlich relevanten Inlandsbeziehung,[228] einer echten oder substanziell hinreichenden Verknüpfung,[229] eines eigenen legitimen Rechtspflegeinteresses,[230] einer Berührung der genuinen staatlichen Ordnungsaufgabe[231] oder eines legitimierenden Anknüpfungsgrunds oder Anknüpfungspunkts.[232] Allerdings genügt ein beliebiger sinnvoller Anknüpfungspunkt nicht; es ist erforderlich, dass der betreffende Staat die engste Verbindung zwischen dem Sachverhalt und seiner Rechtsordnung aufweist.

Damit reiht sich die wohl h.M. in die Rechtsprechungslinie des StIGH[233] bzw. des IGH[234] ein, die gleichfalls einen sinnvollen Anknüpfungspunkt für die Ausübung extraterritorialer Hoheitsgewalt fordern.

Im bereits erwähnten „Lotus-Fall“[235] sah der StIGH die Befugnis zum Einschreiten der Türkei im Eintritt des Erfolgs der fahrlässigen Tötung auf dem unter ihrer Flagge fahrenden Kohlendampfer „Boz-Kourt“.[236] Die türkische Staatsangehörigkeit der Opfer berücksichtigte der Gerichtshof nicht, sondern ließ offen, ob diese –

---

226 *Geiger*, Grundgesetz und Völkerrecht mit Europarecht, S. 29 f.; *Ipsen*, Völkerrecht, § 23, Rn. 88; *Jescheck/Weigend*, Strafrecht AT, § 18 I 2 (S. 165); *Meng*, ZaöRV 44 (1984), 675, 741; *Pappas*, Stellvertretende Strafrechtspflege, S. 81 f.; *Rudolf*, in: BerDGes VölkR 11, S. 7, 22, 29; *Satzger*, Jura 2010, 108, 109; *Schmidt*, Gefahrenabwehrmaßnahmen im Internet, S. 251 f.; *Walter*, JuS 2006, 870, 871; *Ziegenhain*, Extraterritoriale Rechtsanwendung, S. 4; a.A. *Eser*, Festgabe 50 Jahre BGH, S. 3, 27.

227 *Ipsen*, Völkerrecht, § 23, Rn. 87 ff.; *Meng*, ZaöRV 44 (1984), 675, 740.

228 *Rudolf*, in: BerDGesVölkR 11, S. 7, 44.

229 *Ipsen*, Völkerrecht, § 23, Rn. 90; *Spang-Hanssen*, Cyberspace & International Law, S. 239 f.

230 *Jescheck/Weigend*, Strafrecht AT, § 18 I 2 (S. 165).

231 *Mansdörfer*, HRRS 2009, 252, 253.

232 BVerfGE 27, 30, 32; 34, 334, 336 – für das Weltrechtsprinzip.

233 So klingt das Erfordernis eines sinnvollen Anknüpfungspunkts beispielsweise in der sog. „Lotus“-Entscheidung an, StIGHE 5, 73, 95.

234 Der IGH griff auf das *genuine link*-Erfordernis z.B. im „Nottebohm-Fall“, ICJ Rep. 1955, S. 1, 24 und im „Barcelona-Traction-Fall“, ICJ Rep. 1970, S. 1, 42 zurück.

235 Siehe hierzu die Ausführungen unter Teil 2, II.C.4.a)bb).

236 StIGHE 5, 73, 94 f.

soweit sie als einziger Anknüpfungspunkt in Betracht käme – ausreichend im Sinne einer rechtlich relevanten Inlandsbeziehung sei.[237] Nach Auffassung des StIGH verstieß die alleinige Anknüpfung an den Erfolgsort als Tatort nicht gegen das Völkerrecht, da die Gerichte vieler Länder das nationale Strafrecht bei Vorliegen eines inländischen Erfolgsorts, trotz Handelns des Täters im Ausland, anwenden würden.[238] Der Gerichtshof stellte also darauf ab, dass der strafende Staat durch eine „Wirkung" der Tat spürbar auf seinem „schwimmenden Territorium" betroffen war. Wie im Einzelfall eine solche Wirkung beschaffen sein muss, ließ er jedoch offen. Auch heute ist die „Lotus"-Entscheidung trotz Regelung der Zusammenstöße von Schiffen im Übereinkommen über die Hohe See vom 29.4.1958[239] noch nicht überholt. Zwar regelt Art. 11 Nr. 1 des Übereinkommens die Kollision von Schiffen auf Hoher See anders als noch der StIGH zugunsten des Flaggenstaates, auf dessen Schiff sich der Täter befindet, oder des Staates, dessen Staatsangehörigkeit dieser besitzt, aber das Übereinkommen stellt im Ergebnis desgleichen auf einen sinnvollen Anknüpfungspunkt ab, wenn auch auf einen anderen.

Der Nachfolger des StIGH, der IGH, beschäftigte sich u.a. in der sogenannten „Nottebohm"-Entscheidung ebenfalls mit der Ausdehnung des nationalen Rechts auf einen Sachverhalt, der sich im Ausland zugetragen hat.[240] Die Entscheidung betraf zwar nicht das Strafrecht, die Regelungsansätze sind aber auch darauf anwendbar. Der gebürtige Deutsche *Nottebohm* hatte im Jahr 1905 seinen Wohnsitz nach Guatemala verlegt, wo er sich eine Existenz aufbaute. Nach Ausbruch des Zweiten Weltkriegs stellte er 1939 einen Einbürgerungsantrag in Liechtenstein und wurde trotz Fehlens eines dreijährigen Aufenthalts im Land noch im gleichen Jahr eingebürgert. In den folgenden Monaten lebte er weitherhin in Liechtenstein, kehrte jedoch bereits Anfang 1940 wieder nach Guatemala zurück. Im Jahr 1941 erklärte Guatemala dem Deutschen Reich den Krieg. Zwei Jahre später wurde der „Deutsche" *Nottebohm* in Guatemala verhaftet und später sein Vermögen aufgrund eines Dekretes aus dem Jahr 1949 eingezogen. Nach dem Dekret war die Beschlagnahme des Vermögens von Personen möglich, die am 7.10.1938 oder danach im Besitz der Staatsangehörigkeit eines Staates waren, mit dem Guatemala im Krieg stand. Liechtenstein klagte daraufhin beim IGH gegen Guatemala auf Rückerstattung des Vermögens *Nottebohms*, hilfsweise auf Schadensersatz und berief sich hierbei auf die Ausübung diplomatischen Schutzes. Der IGH versagte in seiner Entscheidung der Einbürgerung jedoch die Anerkennung. *Nottebohm* habe weder durch die Wahl des Wohnsitzes noch durch eine gefühlsmäßige Bindung eine hinreichende Beziehung zu Liechtenstein besessen. Eine durch eine enge Beziehung zum einbürgernden Staat gekennzeichnete „effektive" Staatsangehörigkeit sei aber erforderlich,

---

237 StIGHE 5, 73, 94.

238 StIGHE 5, 73, 95.

239 BGBl. II 1972, S. 1091, 1094 mit Ausführungsgesetz vom 21.9.1972 (BGBl. II 1972, S. 1089).

240 ICJ Rep. 1955, S. 1, 13 ff.

wenn ein Staat (hier Guatemala) die Ausübung diplomatischen Schutzes durch einen anderen Staat (hier Liechtenstein) zu dulden habe.[241] In dieser Entscheidung brachte der IGH das Erfordernis eines sinnvollen Anknüpfungspunktes als maßgeblichen Umstand für die Anwendung des nationalen Rechts auf ausländische Sachverhalte damit deutlicher als noch in der „Lotus"-Entscheidung zum Ausdruck. Soweit die „Nottebohm"-Entscheidung im Folgenden unter Hinweis auf die tatsächliche Staatenpraxis stark angegriffen wurde,[242] da nahezu ausnahmslos alle Staaten einen lockeren Anknüpfungspunkt für die Erteilung der Staatsbürgerschaft ausreichen ließen,[243] betrifft diese Beanstandung nicht das Erfordernis eines Anknüpfungspunkts als solches. Denn auch die Kritiker der Entscheidung stellten dieses nicht in Abrede, sondern richteten sich lediglich gegen dessen Ausgestaltung durch den IGH im konkreten Fall.

Die so verstandene Anknüpfung an einen *genuine link* dient der Eingrenzung der Anwendung nationalen Rechts auf Sachverhalte mit Auslandsbezug, allerdings ist sie nicht geeignet, letztgültig die Grenzen der allgemeinen Befugnis zur extraterritorialen Hoheitsausübung festzulegen. Das *genuine link*-Erfordernis versagt beispielsweise in den Fällen, in denen mehrere Staaten einen sinnvollen Anknüpfungspunkt vorzuweisen haben.[244] Daher beließ es selbst der IGH beispielsweise im sogenannten „Barcelona-Traction-Fall"[245] nicht nur bei der Bestimmung von Anknüpfungspunkten, sondern wog zwischen mehreren ab[246] und entschied sich für den engeren.[247]

---

241 ICJ Rep. 1955, S. 1, 26.

242 *Makarov*, ZaöRV 16 (1955-56), 407, 414 ff.; *Stein/v. Buttlar*, Völkerrecht, Rn. 569.

243 *Hailbronner/Kau*, in: Graf Vitzthum/Bothe, Völkerrecht, 3. Abschnitt, Rn. 116.

244 *Lagodny*, Strafgewaltkonflikte, S. 104; *Meessen*, Völkerrechtliche Grundsätze des internationalen Kartellrechts, S. 120; *Vander Beken/Vermeulen/Lagodny*, NStZ 2002, 624, 625.

245 ICJ Rep. 1970, S. 3 ff.; der IGH musste sich mit der Frage beschäftigen, ob sich die Staatsangehörigkeit juristischer Personen nach der Staatsangehörigkeit der (die Kontrolle über das Unternehmen ausübenden) Gesellschafter mit der Mehrheit der Unternehmensanteile bestimmt (sog. Kontrolltheorie) oder nach dem Staat, in dem die Gesellschaft gegründet wurde (sog. Gründungstheorie). Im zur Entscheidung vorgelegten Fall war Belgien Heimatstaat der in Spanien enteigneten Mehrheit der Gesellschafter der Barcelona Traction Light And Power Company, Ltd. und vertrat die sog. Kontrolltheorie. Obwohl Kanada, der Gründungsstaat der Gesellschaft, die Rechtswidrigkeit der entschädigungslosen Enteignung der Gesellschaft durch das Franco-Regime in Spanien nicht rügte, machte Belgien die Ausübung diplomatischen Schutzes geltend. Der IGH vertrat den Standpunkt, dass die Staatszugehörigkeit der juristischen Person zwecks Ausübung diplomatischen Schutzes nach der Gründungstheorie zu bestimmen sei, d.h. nach dem Staat, in welchem die juristische Person gegründet wurde (hier Kanada). Nach Ansicht des Gerichtshofs wies die Barcelona Traction eine engere Verknüpfung mit Kanada als mit Belgien auf (ICJ Rep. 1970, S. 3, 50, Rn. 101).

246 ICJ Rep. 1970, S. 3, 42, Rn. 70.

247 ICJ Rep. 1970, S. 3, 50, Rn. 101; ebenfalls für eine Abwägung, allerdings mit anderem Ergebnis Richter *Sir Gerald Fitzmaurice* in seinem Sondervotum, ICJ Rep. 1970, S. 3, 81, Fn. 29.

Insbesondere bei der Verfolgung von Straftaten im Internet müssen aufgrund der globalen Auswirkungen dieser Taten (z.B. weltweite Abrufmöglichkeiten von strafbewehrten Inhalten oder globale Schädigungen von Computersystemen durch einen über das Internet verbreiteten Virus) mehrere Staaten einen sinnvollen Anknüpfungspunkt für sich in Anspruch nehmen können. Diese Ansprüche sind nach dem herkömmlichen Verständnis eines *genuine link* als „starke Bindung" zu einer Rechtsordnung jedoch nicht mehr geeignet, positive Kompetenzkonflikte zu lösen, da bei Zuhilfenahme des Internet die Taten im Regel- und nicht nur im Ausnahmefall globale Auswirkungen herbeiführen. Eine konkurrierende Jurisdiktion, die zur gleichzeitigen internationalen Zuständigkeit mehrerer Staaten führt, kommt bei Internetsachverhalten wegen der Zuständigkeit unüberschaubar vieler Staaten zu nicht mehr praktikablen und unangemessenen Ergebnissen.[248]

Das alleinige Abstellen auf einen genuine link versagt aber genau betrachtet auch in den Fällen, in denen nur ein Staat ein nachvollziehbares Eingriffsinteresse aufzuweisen hat. Unberücksichtigt bleiben bei dieser einseitigen Betrachtung nämlich die mit den oben dargestellten Grundsätzen der Souveränität und Nichteinmischung umschriebenen Rechte des abwehrenden Staates, dessen Belange u.U. sogar erheblich schwerer wiegen können, so etwa wenn in Deutschland die Darstellung eines Hakenkreuzes auf der Homepage einer indischen Religionsgemeinschaft verfolgt wird.[249] Das Hakenkreuz gilt in weiten Teilen Asiens, insbesondere in Indien, als Glückssymbol. Es steht vorwiegend für den indischen bzw. vedischen Sonnengott Surya und wird hier als Symbol der Freigiebigkeit geschätzt.[250] Der ursprüngliche Begriff „Swastika" für das Hakenkreuz bedeutet „Glücksbringer".[251] Mit diesen Eigenschaften bildet die Swastika eine zentrale Figur der religiösen Symbolik für hunderte Millionen Menschen. Ein strafbewehrtes Verbot ist also auch bei Berücksichtigung der besonderen Symbolbedeutung in Deutschland in diesen besonderen Fallkonstellationen nicht hinnehmbar.

(3) Völkerrechtliche Konfliktlösung durch Interessenausgleich

Die Ermittlung der Grenzen für die Anwendung des nationalen Rechts auf Sachverhalte mit Auslandsbezug kann nur durch eine Abwägung der relevanten Staateninteressen (Eingriffs- und Abwehrinteressee) erfolgen, da allein auf diesem Wege eine gerechte Konfliktlösung zu finden ist. Innerhalb der Abwägung ist das Erfordernis eines sinnvollen Anknüpfungspunktes allerdings ein wesentlicher Gesichts-

---

[248] Vgl. zur ausufernden Inanspruchnahme britischer Gerichte für Klagen wegen Äußerungen im Internet *McLean*, CRi 2012, 141 ff.

[249] Innerhalb der Europäischen Union gibt es immer wieder Versuche, die Verwendung des Hakenkreuzes als solches (sowie andere Symbole des Nationalsozialismus) in allen Mitgliedstaaten zu verbieten.

[250] Siehe die Darstellung unter http://www.swastika-info.com/ [Stand: 6.11.2013].

[251] Siehe die Darstellung unter http://de.wikipedia.org/wiki/Swastika [Stand: 6.11.2013].

punkt, der das Eingriffsinteresse darstellt (nachfolgend unter (b)), dem im Einzelfall ein Abwehrinteresse gegenübersteht (unter (c)). Die Befugnis der Staaten, ohne positive Erlaubnisnorm Sachverhalte mit Auslandsbezügen zu regeln, ist also beschränkt durch die im konkreten Fall entgegenstehenden Interessen der anderen Staaten, soweit diese überwiegen (unter (d)).

(a) Abwägung als geeignetes Mittel zur Schlichtung von Jurisdiktionskonflikten

Die Idee der Interessenabwägung zur Schlichtung von Jurisdiktionskonflikten ist nicht neu.[252] Wesentliche Ansätze für die Beachtung fremder Staatsinteressen enthält z.B. das Restatement of the Law Second[253] des American Law Institute von 1965 in § 40,[254] das Kriterien nennt, anhand derer sich die im Kompetenzkonflikt stehenden Staaten verständigen sollen. Das Restatement of the Law Third von 1986 verfeinert die Anforderungen an die Abgrenzung von entgegenstehenden Jurisdiktionsinteressen in den §§ 402 f.,[255] nach denen die Zuständigkeit zur Regelung

---

[252] ICJ Rep. 1970, S. 3, 42, Rn. 70; ebenfalls für eine Abwägung allerdings mit anderem Ergebnis als der Gerichtshof selbst Richter *Sir Gerald Fitzmaurice* in seinem Sondervotum, ICJ Rep. 1970, S. 3, 81, Fn. 29; KG RIW 1981, 406, 407; MünchKommStGB-*Ambos*, Vor §§ 3–7, Rn. 15; *Geiger*, Grundgesetz und Völkerrecht mit Europarecht, S. 301; *Pappas*, Stellvertretende Strafrechspflege, S. 79 ff.; *Schmidt*, Gefahrenabwehrmaßnahmen im Internet, S. 252; *Sieber*, Straftaten und Strafverfolgung im Internet, C 141; *Ziegenhain*, Extraterritoriale Rechtsanwendung, S. 41 f., 243 ff.

[253] American Law Institute, Restatement Foreign Rel. Law 2nd, § 40, comment a.

[254] § 40 Restatement Foreign Rel. Law 2nd lautet: "Where two states have jurisdiction to prescribe and enforce rules of law and the rules they may prescribe require inconsistent conduct upon the part of a person, each state is required by international law to consider, in good faith, moderating the exercise of its enforcement jurisdiction, in the light of such factors as (a) vital national interests of each of the states, (b) the extent and the nature of the hardship that inconsistent enforcement actions would impose upon the person, (c) the extent to which the required conduct is to take place in the territory of the other state, (d) the nationality of the person, and (e) the extent to which enforcement by action of either state can reasonably be expected to achieve compliance with the rule prescribed by that state."

[255] American Law Institute, vol. 1 Restatement Foreign Rel. Law 3rd, §§ 402 f.

§ 402 Restatement Foreign Rel. Law 3rd lautet: "Subject to § 403, a state has jurisdiction to prescribe law with respect to (1) (a) conduct that, wholly or in substantial part, takes place within its territory; (b) the status of persons, or interests in things, present within its territory; (c) conduct outside its territory that has or is intended to have substantial effect within its territory; (2) the activities, interests, status, or relations of its nationals outside as well as within its territory; and (3) certain conduct outside its territory by persons not its nationals that is directed against the security of the state or against a limited class of other state interests."

§ 403 Restatement Foreign Rel. Law 3rd lautet: "(1) Even when one of the bases for jurisdiction under § 402 is present, a state may not exercise jurisdiction to prescribe law with respect to a person or activity having connections with respect to a person or activity having connections with another state when the exercise of such jurisdiction is unreasonable. (2) Whether exercise of jurisdiction over a person or activity is unreasonable is determined by evaluating all relevant factors, including, where appropriate: (a) the link of the activity

eines Sachverhalts in einem dreistufigen Verfahren ermittelt werden soll. In einem ersten Schritt sei zu prüfen, ob eines der in § 402 genannten Kriterien als Anknüpfungspunkt vorliegt, anschließend im zweiten Schritt, ob die Kriterien im konkreten Einzelfall vernünftigerweise eine Anknüpfung zulassen (§ 403 Abs. 1 und 2). Im dritten und letzten Schritt soll eine Abwägung der verbliebenen entgegenstehenden Interessen erfolgen (§§ 403 Abs. 3, 441 f.[256]). Unter Verweis auf das Restatement of the Law Third schlugen sodann 2001 auch Wissenschaftler der Princeton University eine Abwägung zwischen verschiedenen Kriterien bei der

---

to the territory of the regulating state, i.e., the extent to which the activity takes place within the territory, or has substantial, direct, and foreseeable effect upon or in the territory; […] (3) When it would not be unreasonable for each of two states to exercise jurisdiction over a person or activity, but the prescriptions by the two states are in conflict, each state has an obligation to evaluate its own as well as the other state's interest in exercising jurisdiction, in light of all the relevant factors, Subsection (2); a state should defer to the other state if that state's interest is clearly greater."

[256] § 441 Restatement Foreign Rel. Law 3rd lautet: "(1) In general, a state may not require a person (a) to do an act in another state that is prohibited by the law of that state or by the law of the state of which he is a national; or (b) to refrain from doing an act in another state that is required by the law of that state or by the law of the state of which he is a national. (2) In general, a state may require a person of foreign nationality (a) to do an act in that state even if it is prohibited by the law of the state of which he is a national; or (b) to refrain from doing an act in that state even if it is required by the law of the state of which he is a national."

§ 442 Restatement Foreign Rel. Law 3rd lautet: "(1) (a) A court or agency in the United States, when authorized by statute or rule of court, may order a person subject to its jurisdiction to produce documents, objects, or other information relevant to an action or investigation, even if the information or the person in possession of the information is outside the United States. (b) Failure to comply with an order to produce information may subject the person to whom the order is directed to sanctions, including finding of contempt, dismissal of claim or defense, or default judgment, or may lead to a determination that the facts to which the order was addressed are as asserted by the opposing party. (c) In deciding whether to issue an order directing production of information located abroad, and in framing such an order, a court or agency in the United States should take into account the importance to the investigation or litigation of the documents or other information requested; whether the information originated in the United States; the availability of alternative means of securing the information; and the extent to which noncompliance with the request would undermine important interests of the United States or compliance with the request would undermine important interests of the state where the information is located. (2) If disclosure of information located outside the United States is prohibited by a law, regulation, or order of a court or other authority of the state in which the information or prospective witness is located, or of the state of which a prospective witness is a national, (a) a court or agency in the United States may require the person to whom the order is directed to make a good faith effort to secure permission from the foreign authorities to make the information available; (b) a court or agency should not ordinarily impose sanctions of contempt, dismissal, or default on a party that has failed to comply with the order for production, expect in cases of deliberate concealment or removal of information or of failure to make a good faith effort in accordance with paragraph (a); (c) a court or agency may, in appropriate cases, make findings of fact adverse to a party that has failed to comply with the order for production, even if that party has made a good faith effort to secure permission from the foreign authorities to make the information available and that effort has been unsuccessful."

Anwendung des Weltrechtsprinzips vor.[257] Zwar nicht in Anlehnung an die vorgenannten Restatements, aber ebenfalls unter Differenzierung verschiedener Anknüpfungspunkte stellten 2000/2001 auch die Verfasser des Stanford Draft für eine International Convention to Enhance Protection from Cyber Crime and Terrorism[258] einen Bewertungskatalog zur Lösung von positiven Kompetenzkonflikten auf.[259]

Stufenmodelle zur Lösung von Zuständigkeitskonflikten befürworteten des Weiteren ausdrücklich[260] oder implizit[261] auch Arbeiten, die ihre Wurzeln im kontinentaleuropäischen Rechtskreis haben. So erarbeiteten z.B. die Verantwortlichen des Projekts „Finding the Best Place for Prosecution" im Jahr 2002[262] im Rahmen des von der EU aufgelegten sogenannten Grotius II – Strafrecht Programms[263] sowie Wissenschaftler am Max-Planck-Institut für ausländisches und internationales Strafrecht in ihrer Untersuchung über konkurrierende Zuständigkeit und das Verbot der Mehrfachverurteilung in der Europäischen Union (2003)[264] Entwürfe, in denen sie zwischen einer vorgerichtlichen Phase, einer erstinstanzlichen Gerichtsphase sowie einer Phase der Überprüfung der gerichtlichen Entscheidung differenzierten und innerhalb der einzelnen Stufen Wert auf die Berücksichtigung der jeweils entgegenstehenden Interessen legten. Zu ähnlichen Ergebnissen – aber ohne eine Unterscheidung zwischen verschiedenen Stufen vorzunehmen – kamen ferner ein Gutachter für das Bundesministerium der Justiz 2001 zu der Frage, ob sich die Normierung einer europäischen Gerichtskompetenz für Strafgewaltskonflikte emp-

---

[257] *Macedo*, The Princeton Principles on Universal Jurisdiction, Principle 8, S. 32; zur Abwägung S. 53.

[258] Abgedruckt in *Sofaer/Goodman*, The Transnational Dimension of Cyber Crime and Terrorism, S. 249 ff.

[259] Siehe Art. 5 Abs. 4 Stanford Draft, der wie folgt lautet: "Each State Party will exercise its rights and fulfill its obligations under this Convention to the extent practicable in accordance with the following priority of jurisdiction: first, the State Party in which the alleged offender was physically present when the alleged offense was committed; second, the State Party in which substantial harm was suffered as a result of the alleged offense; third, the State Party of the alleged offender's dominant nationality; fourth, any State Party where the alleged offender may be found; and fifth, any other State Party with a reasonable basis for jurisdiction." *Sofaer*, in: Sofaer/Goodman, The Transnational Dimension of Cyber Crime and Terrorism, S. 221, 232 f.

[260] *Biehler* et al., Freiburg Proposal, S. 7 f., zur Ausgestaltung der einzelnen Stufen siehe S. 9 ff.; *Vander Beken* et al., Finding the Best Place for Prosecution, S. 24, Rn. 67, zur Ausgestaltung der einzelnen Phasen siehe S. 31 ff., zusammenfassend S. 46, Rn. 139–141, S. 59 ff.; siehe auch *Vander Beken/Vermeulen/Lagodny*, NStZ 2002, 624, 626 ff.

[261] Eurojust, Jahresbericht 2003, Anhang, S. 61 ff.; *Lagodny*, Strafgewaltkonflikte, S. 132 ff.

[262] *Vander Beken* et al., Finding the Best Place for Prosecution, S. 31 ff.; siehe auch *Vander Beken/Vermeulen/Lagodny*, NStZ 2002, 624, 626 ff.

[263] Zum Beschluss des Programms siehe Beschluss des Rates vom 28. Juni 2001 über die Durchführung der zweiten Phase des Programms für die Förderung, den Austausch, die Aus- und Fortbildung sowie die Zusammenarbeit von Angehörigen der Rechtsberufe (Grotius II – Strafrecht), ABl. EG 2001, Nr. L 186, S. 1 ff.

[264] *Biehler* et al., Freiburg Proposal, S. 9 ff.

fiehlt,[265] und Eurojust in einem 2003 zu diesem Themenkomplex durchgeführten Seminar in den Entscheidungsleitlinien „Die Lösung von Kompetenzkonflikten".[266]

Speziell für den Umgang mit Jurisdiktionskonflikten unter dem Blickwinkel von im Internet begangenen Straftaten finden sich Vorschläge im „Manual on the prevention and control of computer-related crime" der United Nations von 1994.[267] Nach Textziffer 254 des vorgeschlagenen Maßnahmenkatalogs sollen sich die Staaten um die Aushandlung von Vereinbarungen bei positiven Kompetenzkonflikten bemühen,[268] indem sie Anknüpfungskriterien für die Jurisdiktion festlegen, Mechanismen für künftige Konsultationen im Streitfall erarbeiten und Grundlagen für die gegenseitige Rechtshilfe und Anerkennung von Entscheidungen entwickeln.

Obwohl die angesprochenen Vorschläge von Institutionen und Wissenschaftlern zur Lösung von Kompetenzkonflikten sich zum Teil auf die Rechtspraxis einzelner Staaten[269] oder völkerrechtliche Grundsätze[270] berufen, entspricht eine Abwägung entgegenstehender Staatsinteressen nicht immer auch der konkreten Staatenpraxis. Diese zeigt vielmehr auf, dass die Staaten die Beilegung von Konflikten unter Berücksichtigung fremder Interessen nicht selten nur so lange vorantreiben, wie sie ihre eigenen Interessen erfolgreich durchsetzen können.[271] Daher ist fraglich, ob die Interessenabwägung gleichwohl als völkerrechtlicher Grundsatz verstanden werden kann, der bereits nach Art. 25 GG ohne Transformationsgesetz von der Legislative, Exekutive und Judikative zu beachten ist.

---

[265] *Lagodny*, Strafgewaltkonflikte, S. 132 ff.

[266] Eurojust, Jahresbericht 2003, Anhang, S. 61 ff.; siehe hierzu auch *Walden*, computer crimes and digital investigations, S. 307 ff., Rn. 5.37 ff., der die Entscheidungsrichtlinien sogar als den einzig existierenden praktikablen Vorschlag im Umgang mit Jurisdiktionskonflikten ansieht, S. 309, Rn. 5.43.

[267] United Nations, Manual on the prevention and control of computer-related crime, Tz. 245 ff.

[268] Tz. 254 lautet: "States should, therefore, endeavour to negotiate agreements on the positive conflicts issue. These agreements should address the following issues: (1) An explicit priority of jurisdictional criteria: for example, of location of act over location of effect, of the place of physical detainment of the suspect over in absentia proceedings or extradition; (2) A mechanism for consultation between the States concerned in order to agree upon either the priority of jurisdiction over the offence or the division of the offence into separate acts; (3) Cooperation in the investigation, prosecution and punishment of international computer offences, including the admissibility of evidence lawfully gathered in the other countries, and the recognition of punishment effectively served in other jurisdictions. This would prevent unreasonable hardship to the accused, otherwise possible by an inflexible interpretation of the territoriality principle."

[269] So das American Law Institute, Restatement Foreign Rel. Law 2nd, § 40; dass., vol. 1 Restatement Foreign Rel. Law 3rd, §§ 402 f., 421 f., 431 ff., 441 ff.

[270] *Macedo*, The Princeton Principles on Universal Jurisdiction, Principle 8, S. 32.

[271] Zur Untersuchung der Staatenpraxis siehe *Bertele*, Souveränität und Verfahrensrecht, S. 145 ff.

Die USA gehen beispielsweise für gewöhnlich von einer im Einzelfall lediglich freiwillig durchzuführenden Berücksichtigung fremder Interessen durch eine nicht verpflichtende Selbstbeschränkung (sog. *comity*)[272] aus. Eine Pflicht zur Interessenabwägung wird daher zum Teil auch als nicht völkerrechtlich zwingend angesehen.[273] Dennoch spricht mehr für die Ansicht, die bereits eine Abwägungspflicht im Völkerrecht verankert sieht.[274]

Eine Rücksichtnahme auf die Interessen anderer Staaten kann zumindest im Sinne eines pragmatischen Gebots der Tagespolitik als Minimalkonsens angesehen werden. Gerade die *comity*-Strategie der USA zeigt, dass selbst diese von einer bedingungslosen Jurisdiktionspolitik absehen. Auch wenn sie nur unter einem generösen Gestus (*comity* kann insoweit mit „freiwilligem Entgegenkommen" übersetzt werden) fremde Interessen berücksichtigen und sich hierzu nicht völkerrechtlich verpflichtet fühlen, zeigt sich doch im Kern die Überzeugung, nicht unbeschränkt agieren zu dürfen.[275] Dies gilt insbesondere in Fällen sogenannter *true conflicts*, also wenn US-amerikanische Gebote mit ausdrücklichen und sanktionierten Verboten eines anderen Staates kollidieren und die Justiz dann eine völkerrechtliche Pflicht zur Zurückhaltung durchaus bejaht.[276] Zwar ist eine derart pragmatische, auf Freiwilligkeit beruhende Rücksichtnahme nicht mit einem verpflichtenden Abwägungsgebot gleichzusetzen. Die Abweichungen beider Ansätze sind aber nur graduell und beruhen eher auf dem unterschiedlich stark ausgeprägten Bestreben, Partikularinteressen durchzusetzen, als auf verschiedenen grundsätzlichen Rechtsauffassungen.

---

[272] Siehe hierzu *Bertele*, Souveränität und Verfahrensrecht, S. 147 ff.; *Meng*, ZaöRV 41 (1981), 469, 478 ff., jeweils mit der Darstellung einzelner US-gerichtlicher Entscheidungen zum Grundsatz der *comity*. Im Ergebnis kritisch zur Anknüpfung an die *comity* OECD, Computer-related Crime: Analysis of Legal Policy, S. 68 unter Bezug auf eine Stellungnahme des Richters *M.D. Kirby* (Australien).

[273] *Bertele*, Souveränität und Verfahrensrecht, S. 189; zur US-amerikanischen Praxis vgl. die Entscheidung des Supreme Court im Verfahren *Hartford Fire Ins. Co. v. California*, 113 S. Ct. S. 2891 ff. und die ausdrücklich hierauf Bezug nehmende Ziffer 3 der Antitrust Enforcement Guidelines for International Operations des US Department of Justice und der Federal Trade Commission (Stand: April 1995), abrufbar unter http://www.usdoj.gov/atr/public/guidelines/internat.htm [Stand: 6.11.2013] sowie die Entscheidung des United States Court of Appeals, 2nd Circuit, 148 F.2d 416 (Alcoa), S. 443 f.; anders hingegen das American Law Institute, vol. 1 Restatement Foreign Rel. Law 3rd, § 403, comment a und Reporters' Note 2 unter Berufung auf die Entscheidung 549 F.2d 597, 613 f. *(Timberlane v. Bank of America)*.

[274] *Meessen*, Völkerrechtliche Grundsätze des internationalen Kartellrechts, S. 202 f.; *Nordmann*, Die Beschaffung von Beweismitteln, S. 165 f.

[275] Council of Europe, Extraterritorial criminal jurisdiction, S. 21; *Hermanns*, Völkerrechtliche Grenzen, S. 49 f.; *Rehbinder*, Extraterritoriale Wirkungen des deutschen Kartellrechts, S. 370.

[276] United States District Court for the District of Delaware, 307 F. Supp. 1291, 1303 ff. m.w.N.; American Law Institute, vol. 1 Restatement Foreign Rel. Law 3rd, § 403 Abs. 3, comment e; American Society of International Law, AJIL 29 (1935), Art. 14, 616 f.

Damit ist jedoch nicht das Bestehen eines Völkerrechtsgrundsatzes im Sinne einer Abwägungspflicht ausgeschlossen, sondern im Einzelfall nur seine effektive Durchsetzung in der Praxis. Beiden Ansätzen liegt denn auch die Einsicht zugrunde, dass Staaten sich in einer komplexen Welt mit mehreren Akteuren bewegen. Während der Gedanke der *comity* aus einer Position der Stärke heraus das in der Praxis bestehende ungleiche Kräfteverhältnis unter den Völkerrechtssubjekten betont, überwindet das Abwägungsgebot dieses Kräfteungleichgewicht durch Anerkennung der rechtlichen Gleichheit aller Staaten. Letztere Sichtweise entspricht dem Völkerrecht, das keine unabhängige rechtsetzende Macht über den Einzelstaaten kennt. Eine Ordnung unter den Staaten kann also nicht aus dem Recht des Stärkeren, sondern immer nur aus der Einsicht in die völkerrechtlich gesicherte souveräne Gleichheit der Staaten[277] und der Abgrenzung der ihnen jeweils zukommenden eigenen Machtbereiche[278] entstehen. Nur ein solches System erfüllt den wichtigsten Zweck jeder zwischenstaatlichen Ordnung, nämlich die Befriedung der Konfliktparteien und die Prävention gleichartiger Konfliktfälle. Allein wenn ein Streit mit vernünftigen und einsichtigen Argumenten gelöst wird, übt er seine über den Einzelfall hinausreichende befriedende Wirkung aus. Dass dieses Streben nach friedlicher Konfliktlösung ein anerkanntes Ziel internationaler Politik ist und folglich als Völkerrecht aufgefasst werden kann, zeigt sich nicht zuletzt in der Präambel und im 6. Kapitel der UN-Charta.[279]

Die Kollision zweier Souveränitätsansprüche lässt sich also nur zufriedenstellend auflösen, wenn beide Seiten ihre im Völkerrecht verankerte grundsätzliche Gleichheit und Souveränität behalten und im Einzelfall die gegenüberstehenden Interessen ausgeglichen werden. Die nur einseitige Bestimmung des völkerrechtlichen Dürfens aus Vernunftsgesichtspunkten (*genuine link*-Ansatz) führt wie oben bereits gezeigt[280] nicht weiter. Notwendig und letztlich dem Gebot der souveränen Staatengleichheit allein genügend ist eine Lösung unter Einbeziehung und Abwägung der beide Seiten bewegenden berechtigten Interessen, *eine Gewichtung ihrer Souveränität im Einzelfall*.[281] Die unbestreitbaren Schwierigkeiten bei der praktischen Umsetzung des Abwägungsgedankens, die insbesondere darin bestehen, dass Gerichte des Forumstaates automatisch dazu neigen, das Gewicht der Interessen ihres Staates besonders hoch einzuschätzen[282] und die Abwägung eine dem Souveränitätsgedanken zum Teil zuwider laufende Bewertung ausländischen Rechts beinhaltet,[283] lassen die Abwägungslösung nicht ungeeignet erscheinen. Diese Probleme

---

277 *Rehbinder*, Extraterritoriale Wirkungen des Kartellrechts, S. 336.

278 *Hermanns*, Völkerrechtliche Grenzen, S. 11 f., 34.

279 Charta der Vereinten Nationen – Amtliche Fassung der Bundesrepublik Deutschland, BGBl. II 1973, S. 431 ff.

280 Siehe die Ausführungen unter Teil 2, II.C.4.a)cc)(2).

281 *Meessen*, Völkerrechtliche Grundsätze des internationalen Kartellrechts, S. 82, 202.

282 *Lowe*, RabelsZ 1988, 157, 202 f.

283 *Mestmäcker*, RabelsZ 1988, 205, 251.

bestehen bereits seit Langem und bei jeder Befassung mit transnationalen Sachverhalten, ohne dass sich dadurch das Klima internationaler Zusammenarbeit verschlechtert hätte. Der negative Effekt dürfte deshalb hinter dem gerechten Interessenausgleich zurücktreten. Dem politischen Charakter einer jeden Entscheidung mit Auslandsberührung kann ohne Weiteres durch die herkömmlichen Mechanismen von diplomatischen Protesten und Konsultationen Rechnung getragen werden, die wertvolle Hinweise auf die relevanten Interessen geben. Die (abschließende) Gewichtung der Interessen durch die nationalen Gerichte bleibt alternativlos, solange eine überstaatliche Gerichtsbarkeit über derartige Konflikte nicht existiert.

(b) Eingriffsinteresse

Der Jurisdiktion beanspruchende Staat hat ein beachtenswertes Eingriffsinteresse, wenn er einen sinnvollen Anknüpfungspunkt zur Tat vorweisen kann.[284] Es sind daher abstrakte Tatbestandsmerkmale herauszuarbeiten, die auf eine Vielzahl von Fällen zugeschnitten und geeignet sind, in konkreten Anwendungsfällen einen sinnvollen Anknüpfungspunkt zu bestimmen. Nicht sinnvoll sind Punkte, die entweder als unvernünftig oder sonst willkürlich erscheinen, aber auch jene, die in keinem denkbaren Fall geeignet sind, das geringstmögliche Abwehrinteresse eines anderen Staates zu überwinden, das bereits durch dessen Souveränität und generelles Interesse an Nichteinmischung entsteht.

Soweit sich die internationale höchstrichterliche Rechtsprechung mit der Problematik beschäftigte, stellte sie keine allgemeingültigen Vorgaben für die Beantwortung der Frage auf, was sinnvoll ist. Die Literatur entwickelte dagegen zum Teil bereits sehr konkrete Ansätze für die nähere Bestimmung des Inhalts sinnvoller Anknüpfungspunkte.

(aa) Strafanwendungsregeln als Regelbeispiele sinnvoller Anknüpfungspunkte

Manche Literaturvertreter setzen die nationalen Prinzipien des internationalen Strafrechts mit den völkerrechtlich sinnvollen Anknüpfungspunkten gleich.[285] Gegen eine solche unterschiedslose Behandlung spricht jedoch, dass sich das Völkerrecht in der Interaktion und dem Ausgleich verschiedener Staaten untereinander herausbildet, während die Regelungen des internationalen Strafrechts Ausdruck der jeweiligen nationalen, von wirtschaftlichen und politischen Interessen geprägten Bedürfnisse sind. Da nationale Regelungen die Aspekte des Abwehrinteresses von

---

[284] Zum sinnvollen Anknüpfungspunkt vgl. auch die Ausführungen Teil 2, II.C.4.a)cc)(2); *Jennings*, BYIL 33 (1957), 146, 153.

[285] *Epping*, RIW 1991, 461, 466; so wohl *Jakobs*, Strafrecht AT, 5. Abschnitt, Rn. 5 ff.; wohl auch *Kienle*, Internationales Strafrecht und Straftaten im Internet, S. 144 f.; *Pottmeyer*, NStZ 1992, 57, 59; *Rath*, JA 2006, 435, 436; *Sahlfeld*, Die Veränderung der Ausübung von Staatsgewalt, S. 61; *Walter*, JuS 2006, 870, 871.

Drittstaaten generell eher vernachlässigen, können sie weder pauschal mit dem jeweiligen völkerrechtlich sinnvollen Anknüpfungspunkt gleichgestellt werden[286] noch als „Wegweiser“[287] dienen.

Die Prinzipien des internationalen Strafrechts sind vielmehr nur Beispielsfälle, die der allgemeinen Staatenpraxis als völkerrechtlich im Allgemeinen anerkannte Ansichten entnommen sind.[288] Es gibt also keine durch nationale Normen des internationalen Strafrechts bestimmte und damit begrenzte Menge sinnvoller Anknüpfungspunkte; letztlich entscheidend bleibt die Betrachtung des jeweiligen Einzelfalls. Die Bestimmung der völkerrechtlich sinnvollen Anknüpfungspunkte ist insofern vergleichbar mit der Technik der Regelbeispiele, wie sie aus dem StGB bekannt ist. Der Gesetzgeber beschreibt eine Situation, die *in der Regel* eine bestimmte strafrechtliche Wirkung nach sich ziehen soll, ausschlaggebend bleibt aber der konkrete Einzelfall. Daher ist es möglich, dass trotz der Subsumierbarkeit eines Sachverhalts unter eines der nationalen Prinzipien des internationalen Strafrechts für diese Sachverhaltskonstellation gleichwohl kein sinnvoller Anknüpfungspunkt vorliegt. Neben der im Umgang mit extraterritorialen Sachverhalten nötigen Flexibilität bietet diese Auffassung auch den Vorteil, dass die Gefahr einer ausufernden und dogmatisch nicht zu begründenden Kasuistik weitgehend gebannt und Rechtssicherheit gewonnen werden kann.

Die Prinzipien des internationalen Strafrechts verkörpern selbst folglich weder die sinnvollen Anknüpfungspunkte, noch liefern sie allein die Kriterien für ihre Bestimmung. Sie müssen vielmehr zunächst unter Heranziehung der völkerrechtlichen Grundsätze gedeutet werden.[289] Ein unter nationalen Gesichtspunkten bestimmter Erfolgsbegriff i.S.d. § 9 Abs. 1, 3. Var. StGB stellt also noch keinen zwingenden sinnvollen Anknüpfungspunkt in völkerrechtlicher Hinsicht dar, weil er allein mittels des national normierten Territorialitäts- und Ubiquitätsprinzips ermittelt wurde.

(bb) Intensität der objektiven Rechtsgutbeeinträchtigung

Speziell bei den hier problematisierten Auswirkungen einer vom Ausland gesteuerten Tat ist umstritten, welche Intensität die geforderte Wirkung haben muss, um überhaupt als Anknüpfungspunkt für eine extraterritoriale Hoheitsausübung in

---

286 MünchKommStGB-*Ambos*, Vor §§ 3–7, Rn. 24.

287 So aber *Henrich*, Das passive Personalitätsprinzip im deutschen Strafrecht, S. 22.

288 So wohl *Holthausen*, NStZ 1992, 268, 268 f.; *Lehle*, Der Erfolgsbegriff und die deutsche Strafrechtszuständigkeit im Internet, S. 132 f.; *Martin*, Strafbarkeit grenzüberschreitender Umweltbeeinträchtigungen, S. 137; *Scholten*, Das Erfordernis der Tatortstrafbarkeit in § 7 StGB, S. 60 f.

289 MünchKommStGB-*Ambos*, Vor §§ 3–7, Rn. 11; *Hilgendorf*, NJW 1997, 1873, 1877; *Lehle*, Der Erfolgsbegriff und die deutsche Strafrechtszuständigkeit im Internet, S. 133.

Betracht zu kommen. Weitgehende Einigkeit besteht lediglich darüber, dass eine bewusste objektive Rechtsgutbeeinträchtigung im Inland als ein sinnvoller Anknüpfungspunkt anzusehen ist[290] und damit ein relevantes Eingriffsinteresse nach sich zieht. Inwieweit der Intensität der Auswirkungen auf den betroffenen Staat darüber hinaus Bedeutung zukommt, indem sie etwa das Eingriffsinteresse abschwächt oder insgesamt entfallen lässt, ist jedoch fraglich.

Da theoretisch jedes Land mit einer Verbindung zum Internet in irgendeiner Weise von einer im Internet begangenen Straftat betroffen sein kann, ist es wenig sinnvoll, jede irgendwie geartete Wirkung der Straftat auf andere Staaten als Anknüpfungspunkt ausreichen zu lassen. Anderenfalls würde sich für diesen Bereich eine universelle Zuständigkeit sämtlicher Staaten zur extraterritorialen Jurisdiktion etablieren, die eine unabsehbare Vielzahl von positiven Kompetenzkonflikten und Streitigkeiten nach sich zöge. Es ist also eine nähere Konkretisierung nötig, welche Wirkungen zur Bildung eines hinreichenden Interesses erforderlich sind. Hierfür ist zu untersuchen, ob die Annahme eines sinnvollen Anknüpfungspunkts von der Unterscheidung zwischen vorsätzlichem und fahrlässigem Handeln (nachfolgend unter (aaa)) oder zwischen Verletzung und Gefährdung eines Rechtsguts (unter (bbb)) durch eine im Ausland begangene Tat auf dem Territorium des eingreifenden Staates abhängig ist.

(aaa) Gleichwertigkeit vorsätzlicher und fahrlässiger Begehung

Knüpfen Staaten die Anwendung ihres Strafrechts an die auf ihrem Staatsgebiet eingetretene Wirkung, so verlangen sie zum Teil, dass der Täter diese vorsätzlich herbeiführen wollte,[291] während andere eine vorhersehbare Wirkung ausreichen lassen.[292] Letztere können sich auf die „Lotus"-Entscheidung des StIGH stützen, in welcher der Gerichtshof der „lediglich" fahrlässigen Tatbegehung keine besondere Bedeutung beimaß.[293]

---

[290] American Law Institute, vol. 1 Restatement Foreign Rel. Law 3rd, § 402, comment d, S. 239, Reporters' Note Nr. 2, S. 243; Council of Europe, Extraterritorial criminal jurisdiction, S. 8 f., 24.

[291] So festgestellt in der Untersuchung des Council of Europe, Extraterritorial criminal jurisdiction, S. 9; *Oehler*, Internationales Strafrecht, S. 264, Rn. 357, der darauf hinweist, dass im angloamerikanischen Rechtskreis die Anknüpfung an den Erfolg im Inland durch eine im Ausland begangene fahrlässige Tat nicht geschieht. Siehe hierzu auch Art. 5 Abs. 2 Buchstabe a des Stanford Draft einer International Convention to Enhance Protection from Cyber Crime and Terrorism, abgedruckt in *Sofaer/Goodman*, The Transnational Dimension of Cyber Crime and Terrorism, S. 249 ff.

[292] So etwa der deutsche Gesetzgeber, der in § 9 StGB nicht zwischen Vorsatz- und Fahrlässigkeitsdelikten differenziert; in diesem Sinne auch American Society of International Law, AJIL 29 (1935), 501; zu Literaturvertretern siehe *Jennings*, BYIL 33 (1957), 146, 161; *Meessen*, Völkerrechtliche Grundsätze des internationalen Kartellrechts, S. 163; *Rehbinder*, Extraterritoriale Wirkungen des Kartellrechts, S. 75.

[293] StIGHE 5, 73, 96.

Nach dem Sondervotum eines bei der Abstimmung zur Entscheidung unterlegenen Richters[294] soll allerdings der Unterscheidung zwischen Vorsatz- und Fahrlässigkeitstat bei Distanzdelikten, d.h. einem Auseinanderfallen von Handlungs- und Erfolgsort, besondere Bedeutung zukommen. Nur wenn der Täter die Absicht habe, „den schädlichen Erfolg an einer anderen Stelle, als wo er sich befindet, herbeizuführen", könne „der Ort des Erfolges mit dem Ort der Handlung gleichzustellen" sein.[295] Handele der Täter hingegen fahrlässig, bestehe keine hinreichende unmittelbare Beziehung zwischen Handlung und Erfolg, die deren Gleichstellung rechtfertigen könne. Ohne weitere Begründung lehnte der Richter sodann für fahrlässiges extraterritoriales Handeln eine Anwendung nationaler Bestimmungen durch den von den Auswirkungen der Tat betroffenen Staat ab.

Vereinzelt nimmt die Literatur letztere Argumentation auf.[296] Der nur unachtsame Täter wisse regelmäßig nicht, wo sich sein Verhalten auswirken werde. Existiere allerdings eine Norm, die sein Verhalten sowohl am Handlungsort als auch am Erfolgsort in gleicher Weise unter Strafe stelle, so komme ebenfalls bei Fahrlässigkeitstaten eine Strafbarkeit am Erfolgsort in Betracht, denn dann treffe den Täter der gleiche Vorwurf wie bei einer Bestrafung am Handlungsort.[297] Weitere Literaturvertreter argumentieren mit den verfassungsrechtlichen Maßstäben des Rechtsstaatsgebots und des Gesetzesvorbehalts. Das Gebot des Gesetzesvorbehalts lasse die Begründung der Strafbarkeit an einem vom Handlungsort verschiedenen Ort des Erfolgs nur zu, wenn die Strafbarkeit am Erfolgsort vorhersehbar eingetreten sei. Bei der Verfolgung und Bestrafung von Distanzdelikten sei zu berücksichtigen, dass der Täter u.U. das Recht des Wirkungsstaates nicht kenne oder nicht kennen konnte, insbesondere wenn er fahrlässig gehandelt habe.[298] Erforderlich sei zumindest das Bewusstsein, strafbar zu handeln,[299] oder eine identische Norm für die Strafbarkeit am Handlungsort.[300]

---

294 *Loder* in StIGHE 5, 73, 107 ff.

295 StIGHE 5, 73, 110.

296 MünchKommStGB-*Ambos*, Vor §§ 3–7, Rn. 22; *Kunig/Uerpmann*, Jura 1994, 186, 193.

297 MünchKommStGB-*Ambos*, Vor §§ 3–7, Rn. 22; *Kunig/Uerpmann*, Jura 1994, 186, 193.

298 So etwa *Germann*, SchwZStR 1954, 237, 243; *Oehler*, Internationales Strafrecht, Rn. 124.

299 *Germann*, SchwZStR 1954, 237, 243; *Oehler*, Internationales Strafrecht, Rn. 124; *Scholten*, Das Erfordernis der Tatortstrafbarkeit in § 7 StGB, S. 69 f. – Unabhängig von vorsätzlicher oder fahrlässiger Begehung und begrenzt auf Ausländer, da von einem sich im Ausland aufhaltenden eigenen Staatsangehörigen die Kenntnis der Normen seines Heimatstaates vorausgesetzt werden könnte.

300 *Doehring*, Der Staat 1965, 259, 269 f. (Betrachtung erfolgte aber nur für Auslandstaten, nicht für Distanzdelikte und unabhängig von vorsätzlicher oder fahrlässiger Begehung); *Kienle*, Internationales Strafrecht und Straftaten im Internet, S. 173, 185 f. (für eine analoge Anwendung des Prinzips der identischen Norm); *Scholten*, Das Erfordernis der

Die Ablehnung der Anknüpfung an den Erfolgsort im Inland bei fahrlässigem Handeln im Ausland überzeugt nicht. Insbesondere ist nicht entscheidend, dass der Täter bei Fahrlässigkeitsdelikten den Erfolgstatort regelmäßig nicht kennt, denn dies ist nicht einmal bei dem vorsätzlich Handelnden erforderlich. Die Anwendbarkeit des nationalen Strafrechts ist nämlich nach zutreffender Ansicht kein Tatbestandsmerkmal.[301] Das fehlende Bewusstsein eines ausländischen Tatorts kann allenfalls im Rahmen der Schuld berücksichtigt werden;[302] der Täter kann im Einzelfall einem unvermeidbaren Verbotsirrtum i.S.d. § 17 StGB unterliegen und daher nicht zu bestrafen sein.[303] Die entsprechenden Strafnormen sind im Übrigen bereits dann vorhersehbar, wenn sie die Voraussetzungen des in Art. 103 Abs. 2 GG niedergelegten Gesetzesvorbehalts und des in Art. 20 Abs. 3 GG beheimateten Rechtsstaatsgebots erfüllen. Es genügt also, wenn sie Inhalt eines formell ordnungsgemäß zustande gekommenen Parlamentsgesetzes sind, welches die Voraussetzungen und Folgen der Beurteilung der Tat als Straftat regelt[304] und die zumutbare Möglichkeit der Kenntnisnahme der Vorschriften bestand.

Der Vorwurf an den fahrlässig handelnden Täter besteht überdies gerade darin, sich nicht ausreichend Gedanken um sein Handeln gemacht zu haben, obwohl er hierzu in der Lage gewesen wäre. Soweit die fahrlässige Begehung nach deutschem Recht mit Strafe bedroht ist, gründet sich die Strafbarkeit, ebenso wie die des Vorsatzdelikts, im Wesentlichen nicht auf den in der Tat zutage getretenen „bösen" Willen des Täters, sondern vor allem auf die eingetretene[305] oder zu befürchtende Rechtsgutbeeinträchtigung.[306] Dass dem angesprochenen Erfolgsunwert beim Fahrlässigkeitsdelikt besondere Bedeutung zukommt, wird in der Nichtstrafbarkeit eines fahrlässigen Versuchs deutlich:[307] Während beim Vorsatzdelikt ggf. auch der Täter, der nach seiner Vorstellung von der Tat zur Verwirklichung des Tatbestands unmittelbar ansetzt, wegen Versuchs bestraft werden kann, hindert beim Fahrlässigkeitsdelikt der ausbleibende Handlungserfolg die Begründung einer Strafbarkeit. Der in aller Regel den Täter eines Fahrlässigkeitsdelikts im Vergleich zu dem eines

---

Tatortstrafbarkeit in § 7 StGB, S. 69 (Betrachtung erfolgte nur für Auslandstaten, nicht für Distanzdelikte und unabhängig von vorsätzlicher oder fahrlässiger Begehung).

301 BGHSt 27, 30, 34; S/S-*Eser*, Vorbem. §§ 3–9, Rn. 79; *Jescheck/Weigend*, Strafrecht AT, § 18 V (S. 180); *Rehbinder*, Extraterritoriale Wirkungen des Kartellrechts, S. 75; LK-StGB[12]-*Werle/Jeßberger*, § 9, Rn. 105.

302 Zum Verbotsirrtum beim Fahrlässigkeitsdelikt *Arzt*, ZStW 91 (1979), S. 857 ff.; MünchKommStGB-*Joecks*, § 17, Rn. 73 ff.

303 Siehe hierzu auch die Ausführungen unter Teil 2, II.C.4.b)aa)(2)(a).

304 BVerfGE 75, 329, 342; 78, 374, 382; 85, 69, 72 f.; 87, 363, 391; 87, 399, 411.

305 *Welzel* in der Generaldebatte zu den gemeingefährlichen Handlungen während der Sitzungen der Großen Strafrechtskommission, in: BMJ, Niederschriften, Bd. 8, S. 422; kritisch dagegen *Dreher*, in: BMJ, Niederschriften, Bd. 8, S. 419.

306 So erwogen vom StIGH(E) 5, 73, 96.

307 *Gössel*, in: Maurach/Gössel/Zipf, Strafrecht AT, § 40, Rn. 68, 72; *Roxin*, Strafrecht AT II, § 29, Rn. 4; *Wessels/Beulke*, Strafrecht AT, Rn. 659.

korrespondierenden Vorsatzdelikts treffende verminderte Schuldvorwurf[308] beruht nicht auf einer geringeren objektiven Rechtsgutsverletzung, sondern darauf, dass sich der Täter nicht bewusst gegen die Rechtsordnung gestellt hat. Der beim Fahrlässigkeitsdelikt also gerade nicht zu vernachlässigende Erfolgsunwert unterscheidet sich in seiner Intensität nicht von dem eines Vorsatzdelikts.

Auch der Umstand der fehlenden Strafbewehrung von Fahrlässigkeitstaten in einigen Staaten der Welt lässt nicht darauf schließen, dass Fahrlässigkeitstaten im Völkerrecht nicht als strafwürdig gelten. So kommen beispielsweise die Autoren der Draft Convention on Jurisdiction with Respect to Crime, obwohl sie dem gegenüber fahrlässigen Taten eher zurückhaltenden angloamerikanischen Rechtskreis angehören, in ihrer Untersuchung zu der Auffassung, dass das Völkerrecht die Anknüpfung an einen durch ein fahrlässiges Handeln verursachten Erfolg nicht verbietet. Dementsprechend differenzieren sie in ihrer Untersuchung auch nicht zwischen vorsätzlich und nicht vorsätzlich verursachten Auswirkungen.[309] Auf europäischer Ebene wird bei Harmonisierungsbestrebungen ebenfalls eine Strafbarkeit von Fahrlässigkeitsdelikten nicht ausgeschlossen. So stellt die neueste Fassung des Corpus Juris[310] z.B. bei bestimmten Betrugstatbeständen grobe Fahrlässigkeit sowie Leichtfertigkeit unter Strafe.[311]

Eine Beeinträchtigung der Belange eines Staates, aus denen ein sinnvoller Anknüpfungspunkt im Sinne des Völkerrechts erwachsen kann, hängt folglich nicht davon ab, ob der Täter vorsätzlich oder fahrlässig handelt.

(bbb) Notwendigkeit einer Verletzung oder konkreten Gefährdung

Ein sinnvoller Anknüpfungspunkt könnte jedoch von der Intensität der Rechtsgutverletzung abhängig sein. Zu unterscheiden sind hier die tatsächliche Verletzung des jeweiligen Tatobjekts und damit einhergehend des zu schützenden Rechtsguts und der Grad seiner Gefährdung, wobei zwischen konkreten und abstrakten Gefahren zu differenzieren ist.

---

[308] In diesem Zusammenhang stellen die Strafrahmen für Delikte nach § 316 StGB eine Ausnahme dar. Wegen Trunkenheit im Verkehr wird nämlich der fahrlässig handelnde Täter nach dem gleichen Strafrahmen wie der vorsätzlich handelnde Täter bestraft.

[309] American Society of International Law, AJIL 29 (1935), 501.

[310] *Delmas-Marty/Vervaele*, The Implementation of the Corpus Juris in the Member States, vol. 1, S. 192; zur deutschen Übersetzung des französischen und englischen Originaltextes von *Walter*, abrufbar unter http://www.uni-regensburg.de/Fakultaeten/Jura/walter/daten/publikationen/corpus_iuris_deutsch.pdf [Stand: 6.11.2013].

[311] Siehe Art. 9 des Corpus Juris 2000, der in der deutschen Übersetzung wie folgt lautet: „Für alle Taten nach den Artikeln 1 bis 8 ist Vorsatz erforderlich mit Ausnahme der Delikte, die der Betrügerei zum Nachteil des Gemeinschaftshaushalts gleichgestellt sind (Artikel 1) und für die Leichtfertigkeit genügt."

Unstreitig ist eine extraterritoriale Hoheitsausübung bei Verletzung eines Rechtsguts grundsätzlich zulässig. Nach der Entscheidung des StIGH im „Lotus-Fall“[312] ist die Verletzung des jeweiligen Tatobjekts auf dem eigenen Hoheitsgebiet als sinnvoller Anknüpfungspunkt für die Eröffnung des nationalen Strafrechts ausreichend.[313] Wohl jeder Staat stellt die konkrete Verletzung, also eine spürbare tatsächliche Beeinträchtigung, bestimmter Rechtsgüter im Inland generell unter Strafe,[314] sodass insoweit von einer allgemeinen Übung gesprochen werden kann.

Umstritten ist indes, ob neben Verletzungen auch konkrete und abstrakte Gefährdungen von Rechtsgütern für die Begründung eines sinnvollen Anknüpfungspunkts ausreichend sind. Sowohl bei abstrakter als auch bei konkreter Gefährdung kommt es lediglich zu einer Bedrohung des Tatobjekts, nicht aber zu dessen Verletzung.[315] Während jedoch für eine konkrete Gefahr – unabhängig von den Meinungsunterschieden[316] bei den Einzelheiten der Ermittlung der Gefahrenintensität – Voraussetzung ist, dass der Täter das Tatobjekt nur durch Zufall nicht verletzt, liegt eine abstrakte Gefahr bereits vor, wenn der Täter eine Handlung vorgenommen hat, die schon aufgrund ihrer typischen Gefährlichkeit Anlass zur Strafbarkeit gibt, ohne dass eine Gefahr im Einzelfall tatsächlich eintreten muss.[317]

Verletzungs- und konkrete Gefährdungsdelikte unterscheiden sich zwar in ihrer Wirkung auf das geschützte Rechtsgut. Die Auswirkung auf die Rechtsordnung ist bei beiden aber nahezu identisch. Lediglich der selbst für den Täter kaum steuerbare Umstand, dass sich die seiner Handlung innewohnende spezifische Gefahr verwirklicht oder nicht, bildet den Unterschied. Deshalb hat z.B. der deutsche Gesetzgeber konkrete Gefährdungsdelikte nur für besonders gefährliche Handlungen und davon regelmäßig betroffene wichtige Rechtsgüter geschaffen, ohne dabei auf die Möglichkeit eines in der Außenwelt hervortretenden Erfolgs zu verzichten. Es entspricht dem legitimen Interesse eines Staates an der effektiven Sicherung seiner Rechtsordnung, eine Rechtsgutverletzung auf der Basis eines konkret gefährlichen Verhaltens zu antizipieren, den Strafrechtsschutz also ins Vorfeld der Verletzung zu verlagern. Bereits die Verwirklichung einer konkreten Gefahr stellt folglich eine sinnvolle Anknüpfung für eine extraterritoriale Hoheitsausübung dar.

---

312 Zur Fallbeschreibung siehe auch die Ausführungen unter Teil 2, II.C.4.a)bb).

313 StIGHE 5, 73, 95 f.

314 American Law Institute, vol. 1 Restatement Foreign Rel. Law 3rd, § 402, comment d, S. 239, Reporters’ Note Nr. 2, S. 243; Council of Europe, Extraterritorial criminal jurisdiction, S. 8 f., 24; *Oehler*, Internationales Strafrecht, S. 265, Rn. 356 i.V.m. S. 211 ff.

315 *Roxin*, Strafrecht AT I, § 10, Rn. 123.

316 Siehe dazu die Darstellung bei *Kindhäuser*, Gefährdung als Straftat, S. 189 ff., 201 ff. (auf die konkrete Gefahr bezogen); zum Gefahrbegriff vgl. ebenfalls BGHSt 18, 271, 272 f.; *Dreher*, in: BMJ, Niederschriften, Bd. 8, S. 418; *Hirsch*, FS Kaufmann, S. 545, 557 ff.; *Triantafyllou*, Das Delikt der gefährlichen Körperverletzung als Gefährdungsdelikt, S. 93 ff.

317 *Fischer*, StGB, Vor § 13, Rn. 19; *Jescheck/Weigend*, Strafrecht AT, § 26 II 2 (S. 263 f.); *Roxin*, Strafrecht AT I, § 10, Rn. 124.

Die abstrakte Gefahr kann indes – entgegen anderer Ansicht[318] – keinen sinnvollen Anknüpfungspunkt begründen, wenn der Täter im Ausland handelt. Solange es dem sich durch die Verwirklichung einer abstrakten Gefahr betroffen sehenden Staat an einer sich manifestierenden[319] beachtlichen[320] Wirkung auf seinem Hoheitsgebiet fehlt, weist er für eine extraterritoriale Hoheitsausübung keine besondere territoriale Beziehung zum betreffenden Sachverhalt – der extraterritorialen Handlung – auf. Eine abstrakte Gefahr wäre nach der gedanklichen Struktur dieser Delikte nämlich schon dann zu bejahen, wenn der Täter die tatbestandliche Handlung vornimmt, ohne dass das Tatobjekt überhaupt in den Gefahrenkreis gelangen und dessen Verletzung auch nur nahe liegen muss. Die Gefährdung des Rechtsguts wird bereits von Tatbestands wegen unwiderlegbar vermutet – mit der Folge, dass der Tatbestand nach zum Teil vertretener Ansicht selbst dann erfüllt sein soll, wenn die Unmöglichkeit der Verwirklichung der Gefahr nachgewiesen ist.[321] Das aus diesem Grund sehr geringe Eingriffsinteresse bleibt gegenüber jedem noch so geringen Abwehrinteresse zurück,[322] zumal sich der abwehrende Staat zu Recht darauf berufen kann, dass die inkriminierte Tat seine Grenzen lediglich in Gedankenkonstrukten verlassen hat und damit einer für ihn inneren Angelegenheit sehr nahe kommt. Die Strafbarkeit ist hier also so weit ins Vorfeld verlagert, dass sich der bloß abstrakt betroffene Staat zurücknehmen und der Rechtshoheit des Staates, in welchem der Täter handelte, den Vorzug gewähren muss. Erst zu dem Zeitpunkt, in dem der abstrakten Gefahr ein greifbarer Effekt im Sinne einer konkreten Gefährdung oder gar einer Verletzung des geschützten Rechtsguts folgt, kann der eingreifende Staat im Einzelfall einen sinnvollen territorialen Anknüpfungspunkt für sich reklamieren. In Konstellationen einer schlichten abstrakten Gefahr als Auswirkung versagt das Territorialitätsprinzip dagegen als Anknüpfungspunkt. Kann im Einzelfall gleichwohl dem Jurisdiktion beanspruchenden Staat der Verzicht auf eine eigene Regelung nicht zugemutet werden, z.B. weil wichtigste Staatsinteressen betroffen sind, so bleibt ihm nur die Berufung auf das vom Tatort unabhängige Schutzprinzip.[323]

---

318 *Volk*, Glücksspiele im Internet, S. 236, die einschränkend aber noch fordert, dass das im Ausland gezeigte Verhalten mit seiner inländischen Wirkung ein „konstituierendes Element" bildet und der Täter diese Wirkung unmittelbar beabsichtigte.

319 American Society of International Law, AJIL 29 (1935), 494 f.; Council of Europe, Extraterritorial criminal jurisdiction, S. 9, 24.

320 American Law Institute, vol. 1 Restatement Foreign Rel. Law 3rd, § 402 Abs. 1 lit. c sowie comment d, § 403 Abs. 2 lit. a, § 421 Abs. 2 lit. j; *Hermanns*, Völkerrechtliche Grenzen, S. 33; *Jennings*, BYIL 33 (1957), 146, 159; *Rehbinder*, Extraterritoriale Wirkungen des Kartellrechts, S. 91.

321 Zum Streit bei § 306a I StGB vgl. m.w.N. die umfangreiche Darstellung bei S/S-*Heine*, § 306a, Rn. 2; MünchKommStGB-*Radtke*, § 306a, Rn. 39 ff.

322 *Rehbinder*, Extraterritoriale Wirkungen des deutschen Kartellrechts, S. 90.

323 *Hermanns*, Völkerrechtliche Grenzen, S. 36 f.; *Rehbinder*, Extraterritoriale Wirkungen des deutschen Kartellrechts, S. 77; kritisch *Spang-Hanssen*, Cyberspace & Internatio-

Ein sinnvoller territorialer Anknüpfungspunkt ergibt sich auch nicht aus der im Einzelfall möglichen weltweiten Wahrnehmbarkeit abstrakter Gefährdungsdelikte, z.B. beim Abrufen unerwünscht versendeten pornografischen Materials aus dem Ausland im Inland (§ 184 Abs. 1 Nr. 6 StGB). Für die Wahrnehmbarkeit als sinnvoller Anknüpfungspunkt spricht zwar, dass diese eine in der Abrufmöglichkeit tatsächlich feststellbare, gefahrbegründende Auswirkung im Inland darstellt. Dennoch ist der Anknüpfungspunkt der internetvermittelten Wahrnehmbarkeit aber nicht sinnvoll, weil das resultierende Eingriffsinteresse zu schwach ist.[324] Die bloße Möglichkeit der Wahrnehmung, die sich nicht durch einen tatsächlichen Abruf zur konkreten Gefährdung oder gar Rechtsgutverletzung verdichtet hat, ist nicht einmal praktisch zu verfolgen, da es schließlich an der Kenntnis des inkriminierten Verhaltens selbst fehlt. Die Auswirkung und – daraus resultierend – das Ahndungsinteresse sind so gering, dass kein Fall denkbar ist, in dem allein aus der durch die Wahrnehmbarkeit vermittelten abstrakten Gefährdung ein Eingriffsinteresse folgte, das stark genug wäre, irgendein Abwehrinteresse eines anderen Staates zu überwinden.

Wie die abstrakten Gefährdungsdelikte sind ferner die abstrakt-konkreten Gefährdungsdelikte,[325] die zum Teil auch als abstrakte Eignungsdelikte,[326] als potentielle[327] oder besondere abstrakte Gefährdungsdelikte[328] bezeichnet werden, zu behandeln. Zum Tatbestand der abstrakt-konkreten Gefährdungsdelikte gehört eine Tathandlung oder ein Tatmittel, die bzw. das bei genereller Betrachtung der Tatumstände gefahrengeeignet sein muss. Der Eintritt einer konkreten Gefahr ist jedoch nicht erforderlich.[329]

Entscheidend für die Bewertung der abstrakt-konkreten Gefährdungsdelikte ist der Umstand, dass gerade keine konkrete Gefahr eintreten muss, damit der Täter den Tatbestand verwirklicht. Der Nachweis einer generellen Eignung für die Entstehung einer Gefahr für ein bestimmtes Rechtsgut reicht nicht aus, um einen Eingriff in die Hoheitsrechte anderer souveräner Staaten zu rechtfertigen. Die abstrakt-konkrete Gefahr ist lediglich eine besondere Ausgestaltung der abstrakten Gefahr. In den Tatbeständen der abstrakt-konkreten Gefährdungsdelikte ist die Handlung oder das Tatmittel nach allgemeinem Erfahrungswissen nicht exakt als generell

---

nal Law, S. 348. Siehe auch Council of Europe, Recommendation No. (89) 9, Erläuternder Bericht, S. 85 f.; ders., Extraterritorial criminal jurisdiction, S. 13 f.; United Nations, Manual on the prevention and control of computer-related crime, Tz. 258 f.

[324] So wie hier auch *Jeßberger*, JZ 2001, 432, 434, allerdings ohne nähere Begründung; *Schmidt*, Gefahrenabwehrmaßnahmen im Internet, S. 254 f., ebenfalls ohne nähere Begründung.

[325] *Schröder*, JZ 1967, 522, 522.

[326] *Roxin*, Strafrecht AT I, § 11, Rn. 162.

[327] *Fischer*, StGB, Vor § 13, Rn. 19.

[328] SK-StGB-*Wolters/Horn*, Vor § 306, Rn. 18.

[329] BGH NJW 1999, 2129, 2129; *Fischer*, StGB, Vor § 13, Rn. 19; *Jescheck/Weigend*, Strafrecht AT, § 26 II 2 (S. 264 f.); *Roxin*, Strafrecht AT I, § 11, Rn. 162.

gefährlich beschreibbar. Erst durch die Koppelung an das wertausfüllungsbedürftige Merkmal der Geeignetheit ist das Verhalten des Täters, soweit der Richter eine Gefahreneignung feststellt, nach Ansicht des Gesetzgebers strafwürdig.[330] Die Strafbarkeit wegen eines abstrakt-konkreten Gefährdungsdelikts hängt folglich nicht von einer sich in der Außenwelt konkretisierenden Gefahrenlage ab. Das Erfordernis der Geeignetheit ist vielmehr Ausdruck der Schwierigkeiten der sprachlichen Umschreibung einer strafwürdigen Tathandlung oder eines Tatmittels. Die Strafwürdigkeit abstrakt-konkreter Gefährdungsdelikte geht nicht über diejenige rein abstrakter Gefährdungsdelikte hinaus. Insbesondere folgt aus der (abstrakt zu beurteilenden) Geeignetheit einer Handlung noch nicht eine besondere (konkret zu bemessende) Auswirkung, an welche zur Begründung eines Eingriffsinteresses angeknüpft werden könnte. Es ergibt sich folglich für das Eingriffsinteresse keine von den Ausführungen bei den rein abstrakten Gefährdungsdelikten abweichende Beurteilung.

(c) Abwehrinteresse

Dem vorstehend beschriebenen Eingriffsinteresse steht das Abwehrinteresse des Staates gegenüber, auf dessen Gebiet sich der Täter bei der Straftatbegehung befand. Durch die Ausdehnung des Strafrechts auf sich – auch – in einem fremden Staat ereignende Vorgänge mischt sich der eingreifende deutsche Staat in den dargestellten Beispielsfällen einer völkerrechtlichen Konfliktlage[331] in das völkerrechtlich geschützte Recht des abwehrenden Staates auf Selbstbestimmung ein.

(d) Abwägung der widerstreitenden Interessen

Zur Auflösung des sich aus den widerstreitenden Interessen der betroffenen Staaten ergebenden Konflikts sind das Eingriffs- und das Abwehrinteresse gegeneinander abzuwägen. In Betracht kommen hierzu eine generell-abstrakte (nachfolgend unter (aa)) oder eine individuell-konkrete Abwägung (unter (bb)).

(aa) Ablehnung einer generell-abstrakten Hierarchie

Eine generell-abstrakte Hierarchie der potentiell mit Strafgewalt ausgestatteten Staaten[332] konnte sich in der Praxis bisher nicht durchsetzen,[333] insbesondere ist

---

[330] *Berz*, Formelle Tatbestandsverwirklichung und materialer Rechtsgüterschutz, S. 59; *Graul*, Abstrakte Gefährdungsdelikte und Präsumtionen im Strafrecht, S. 116 f.

[331] Siehe hierzu die Ausführungen unter Teil 2, II.C.4.a)aa)(1)–(3).

[332] Zu einem Vorschlag der Rangfolge der Anknüpfungspunkte siehe z.B. MünchKommStGB-*Ambos*, Vor §§ 3–7, Rn. 64 ff.; ebenso Art. 5 Abs. 4 Draft International Convention to Enhance Protection from Cyber Crime and Terrorism, abgedruckt in *Sofaer/Goodman*, The Transnational Dimension of Cyber Crime and Terrorism, S. 249 ff. Siehe

eine solche Rangfolge völkergewohnheitsrechtlich nicht vorgeschrieben.[334] Praktische Ansätze zur generell-abstrakten Hierarchiebildung enthielt beispielsweise der – später nicht verwirklichte[335] – Konventionsentwurf des Europarats zur Lösung von Zuständigkeitskonflikten aus dem Jahr 1965.[336] Nach Art. 3,[337] Art. 4 Abs. 2[338] und Art. 5[339] des Entwurfs sollte primär der Tatortstaat zur Verfolgung berechtigt sein, wobei der Staat, in dem der Täter oder die Tatbeteiligten handelten, vor dem Staat, in dem ein Beitrag zur Tat geleistet wurde, zuständig sein sollte.

---

hierzu auch *Sofaer*, in: Sofaer/Goodman, The Transnational Dimension of Cyber Crime and Terrorism, S. 221, 232 f.

[333] *Brenner*, in: Koops/Brenner, Cybercrime and Jurisdiction, S. 327, 331; *Lagodny*, Strafgewaltkonflikte, S. 44 ff.; *Ligeti*, Strafrecht und strafrechtliche Zusammenarbeit, S. 84 ff.; *Vander Beken* et al., Finding the Best Place for Prosecution, S. 23, Rn. 63, S. 59.

[334] *Lagodny*, Strafgewaltkonflikte, S. 44; *Pappas*, Stellvertretende Strafrechtspflege, S. 87 f., Fn. 104; *Vander Beken/Vermeulen/Lagodny*, NStZ 2002, 624, 625; so im Ergebnis auch Kommission der Europäischen Gemeinschaften, KOM(2000) 495 endg., S. 20.

[335] Zum Scheitern des Entwurfs siehe *Lagodny*, Strafgewaltkonflikte, S. 48 f.; *Vander Beken* et al., Finding the Best Place for Prosecution, S. 22, Rn. 60.

[336] Draft European Convention on Conflicts of Jurisdiction in Criminal Matters (prepared by the Legal Committee of the Council of Europe), European Consultative Assembly, Doc. No. 1873; Recommendation 420 on the Settlement of Conflicts of Jurisdiction in Criminal Matters (1965), European Consultative Assembly, Sixteenth Ordinary Session.

[337] Art. 3 Konventionsentwurf des Europarats zur Lösung von Zuständigkeitskonflikten (1965) lautet: "(1) Subject to the jurisdiction specified in Article 2 (2), the State in whose territory the offence was committed shall have the primary right to exercise jurisdiction. (2) The place of the offence shall be deemed to be the territory on which has taken place an act or omission constituting an offence or an attempt, or an act of complicity, and the territory on which the act or omission produced its effect. (3) Where in application of the preceding paragraph, more than one State claims that the offence was committed on its territory, jurisdiction shall be exercised in the following order: first, the State on whose territory the constituent factor of the offence or attempted offence was committed or the constituent omission occurred; then, the State on whose territory an act of complicity was committed; lastly the State on whose territory the effect was produced. When more than one State can claim equal right to exercise jurisdiction, primary right of jurisdiction shall lie with the State on whose territory the offender is found. (4) The State whose territorial jurisdiction is secondary may exercise jurisdiction if the State having the primary right to do so waives that right either *proprio motu* or at the request of the other State."

Art. 2 Abs. 2 Konventionsentwurf des Europarats zur Lösung von Zuständigkeitskonflikten (1965) lautet: "(2) Furthermore, the State has the right to prosecute and try offences committed outside its territory, even by aliens, if such offences constitute a danger to its external or internal safety, or if they consist in the counterfeiting of its currency or of its official stamps, seals, marks or other imprints."

[338] Art. 4 Abs. 2 Konventionsentwurf des Europarats zur Lösung von Zuständigkeitskonflikten (1965) lautet: "(2) Such [ratione personae] jurisdiction shall be subsidiary to that of the State where the offence was committed."

[339] Art. 5 Konventionsentwurf des Europarats zur Lösung von Zuständigkeitskonflikten (1965) lautet: "The State in whose territory is found the perpetrator of a grave offence committed abroad against life, limb, freedom, morality or property, or an offence against common interests protected by international law, may prosecute and try him if the States competent under Articles 3 and 4 fail to prosecute, refrain from requesting or refuse an offer of extradition."

Erst nach diesen Staaten wäre der Staat des Erfolgsorts zur Verfolgung berufen. Die umgekehrte Reihenfolge sollte nur gelten, soweit sich eine Straftat gegen die äußere und innere Sicherheit eines Staates richtete (Art. 7[340] des Entwurfs). Dem vorstehenden Konventionsentwurf folgten wenig später das Europäische Übereinkommen über die internationale Geltung von Strafurteilen[341] und das über die Übertragung der Strafverfolgung,[342] die keine strikte hierarchische Kompetenzordnung mehr vorsahen, sondern vielmehr in Art. 5[343] bzw. Art. 8[344] eine Liste objektiver und subjektiver Kriterien beinhalteten, anhand derer entweder der Urteilsstaat einen anderen Staat um Vollstreckung der Sanktion bzw. ein Vertragsstaat einen anderen um Strafverfolgung ersuchen konnte. Aber selbst diese Konventionen setzten sich aufgrund der schleppenden Ratifizierung in den einzelnen Unterzeichner-

---

340 Art. 5 Konventionsentwurf des Europarats zur Lösung von Zuständigkeitskonflikten (1965) lautet: "The jurisdiction of the State whose safety or credit has been jeopardised in the conditions defined in Article 2 (2) is independent of that of any other State and cannot be affected by the exercise of the latter jurisdiction."

341 Vom 28.5.1970 (ETS No. 70).

342 Vom 15.5.1972 (ETS No. 73).

343 Art. 5 Europäisches Übereinkommen über die internationale Geltung von Strafurteilen lautet: „Der Urteilsstaat kann einen anderen Vertragsstaat um Vollstreckung einer Sanktion nur ersuchen, wenn eine oder mehrere der folgenden Voraussetzungen erfüllt sind: (a) wenn der Verurteilte seinen gewöhnlichen Aufenthalt in dem anderen Staat hat; (b) wenn die Vollstreckung der Sanktion im anderen Staat geeignet ist, die soziale Wiedereingliederung des Verurteilten zu erleichtern; (c) wenn es sich um eine freiheitsentziehende Sanktion handelt, die in dem anderen Staat im Anschluß an eine andere vom Verurteilten in diesem Staat angetretene oder zu verbüßende freiheitsentziehende Sanktion vollstreckt werden könnte; (d) wenn der andere Staat der Heimatstaat des Verurteilten ist und sich schon bereit erklärt hat, die Vollstreckung dieser Sanktion zu übernehmen; (e) wenn er der Auffassung ist, daß er die Sanktion – auch durch Erwirkung der Auslieferung – nicht selbst vollstrecken kann und der andere Staat dazu in der Lage ist."

344 Art. 8 Übereinkommen über die Übertragung der Strafverfolgung lautet: „(1) Ein Vertragsstaat kann einen anderen Vertragsstaat um Verfolgung in einem oder mehreren der folgenden Fälle ersuchen: (a) wenn der Beschuldigte seinen gewöhnlichen Aufenthalt im ersuchten Staat hat; (b) wenn der Beschuldigte Angehöriger des ersuchten Staates oder wenn dieser Staat sein Herkunftsstaat ist; (c) wenn der Beschuldigte im ersuchten Staat eine freiheitsentziehende Sanktion verbüßt oder zu verbüßen hat; (d) wenn der Beschuldigte im ersuchten Staat wegen derselben oder wegen einer anderen strafbaren Handlung verfolgt wird; (e) wenn er der Auffassung ist, daß die Übertragung der Verfolgung im Interesse der Wahrheitsfindung liegt und daß sich insbesondere die wichtigsten Beweismittel im ersuchten Staat befinden; (f) wenn nach seiner Auffassung die Vollstreckung einer etwaigen Verurteilung im ersuchten Staat geeignet ist, die Wiedereingliederung des Verurteilten in die Gesellschaft zu erleichtern; (g) wenn nach seiner Auffassung die Anwesenheit des Beschuldigten in der Hauptverhandlung im ersuchten, nicht aber im ersuchenden Staat gewährleistet werden kann; (h) wenn er der Auffassung ist, daß er eine etwaige Verurteilung – auch durch Erwirkung der Auslieferung – nicht selbst vollstrecken kann und daß der ersuchte Staat dazu in der Lage ist. (2) Ist der Beschuldigte in einem Vertragsstaat rechtskräftig verurteilt worden, so kann dieser Staat um Übernahme der Verfolgung in einem oder mehreren der in Absatz 1 vorgesehenen Fälle nur ersuchen, wenn er die Sanktion – auch durch Erwirkung der Auslieferung – nicht selbst vollstrecken kann und wenn der andere Vertragsstaat ausländische Urteile grundsätzlich nicht vollstreckt oder die Vollstreckung des betreffenden Urteils ablehnt."

staaten nur bedingt durch.[345] Deutschland unterzeichnete z.B. zwar das Übereinkommen über die internationale Geltung von Strafurteilen bereits am Tag der Zeichnung der Konvention, ratifizierte es dann aber nicht. Das Übereinkommen über die Übertragung der Strafverfolgung unterzeichnete Deutschland erst gar nicht. Ebenso ohne praktische Auswirkungen blieb die Untersuchung des European Committee on Crime Problems aus dem Jahr 1988 zur Erstreckung der Strafgewalt auf Taten mit Bezug zum Ausland, in der insbesondere durch Rechtsvergleichung und Hinweis auf bereits existierende, aber zum Teil noch nicht ratifizierte Übereinkommen Vorschläge zum Abbau von Kompetenzkonflikten entwickelt wurden.[346]

Der Lösung positiver Kompetenzkonflikte widmeten sich überdies die bereits dargestellten[347] Arbeiten US-amerikanischer Rechtswissenschaftler, die teils aus der nationalen Rechtsprechung (1965 und 1986),[348] teils aus dem kodifizierten wie ungeschriebenen Völkerrecht (2001)[349] destillierte Abwägungskriterien zu systematisieren versuchten. Auf eine abstrakt-generelle Hierarchiebildung verzichteten jedoch beide Arbeiten ausdrücklich[350] oder implizit.[351] Nach Ansicht der Projektmitarbeiter können die Besonderheiten des jeweiligen Einzelfalls nämlich nur dann hinreichend einbezogen werden, wenn nicht nur die bloße Existenz von Einzelfaktoren, sondern auch deren Gewicht in der Gesamtabwägung berücksichtigt werden.[352] Anders entschieden sich indes die Verfasser des Stanford Draft für eine International Convention to Enhance Protection from Cyber Crime and Terrorism (2000/2001), die eine abstrakt generelle Hierarchie von Anknüpfungspunkten vorschlugen.[353] Der Entwurf setzte sich in der Praxis aber nicht durch.

---

345 Council of Europe, Extraterritorial criminal jurisdiction, S. 36.; ders., Recommendation No. (89) 9, Erläuternder Bericht, S. 90.

346 Council of Europe, Extraterritorial criminal jurisdiction, S. 30 ff.

347 Siehe hierzu die Ausführungen unter Teil 2, II.C.4.a)cc)(3)(a).

348 American Law Institute, Restatement Foreign Rel. Law 2nd, § 40; dass., vol. 1 Restatement Foreign Rel. Law 3rd, §§ 402 f., 421 f., 431 ff., 441 ff.

349 *Macedo*, The Princeton Principles on Universal Jurisdiction, Principle 8, S. 32.

350 Ebenda, S. 53.

351 American Law Institute, Restatement Foreign Rel. Law 2nd, § 40, der eine Abwägungspflicht unter nicht abschließender Aufführung bestimmter Faktoren postuliert; dass., vol. 1 Restatement Foreign Rel. Law 3rd, § 403, der eine nicht abschließende Liste von abzuwägenden Kriterien aufführt; § 441, der die Kriterien präzisiert.

352 *Macedo*, The Princeton Principles on Universal Jurisdiction, S. 53; im Ergebnis ebenso *Brenner*, in: Koops/Brenner, Cybercrime and Jurisdiction, S. 327, 331.

353 Siehe Art. 5 Abs. 4 Stanford Draft, der lautet: "Each State Party will exercise its rights and fulfill its obligations under this Convention to the extent practicable in accordance with the following priority of jurisdiction: first, the State Party in which the alleged offender was physically present when the alleged offense was committed; second, the State Party in which substantial harm was suffered as a result of the alleged offense; third, the State Party of the alleged offender's dominant nationality; fourth, any State Party where the alleged offender may be found; and fifth, any other State Party with a reasonable basis for jurisdiction.", abgedruckt in *Sofaer/Goodman*, The Transnational Dimension of Cyber

Die Europäische Union beschäftigte sich im Zuge der Umsetzung der Zielstellung des Vertrags von Amsterdam,[354] einen Raum der Freiheit, der Sicherheit und des Rechts zu errichten, ebenfalls intensiver mit Fragen der Auflösung von Kompetenzkonflikten. Hierzu erarbeiteten der Rat und die Kommission den Ende 1998 vorgestellten sogenannten Wiener Aktionsplan.[355] Danach sollte im Bereich der justiziellen Zusammenarbeit in Strafsachen u.a. die „Frage, ob die grenzüberschreitende Zusammenarbeit bei der Übertragung von Strafprozessen und bei der Strafverfolgung verbessert werden kann" geprüft sowie im Weiteren untersucht werden, ob „Kompetenzkonflikte zwischen den Mitgliedstaaten [verhütet werden könnten], indem beispielsweise die Möglichkeit geprüft wird zu registrieren, ob in verschiedenen Mitgliedstaaten gegen ein und dieselbe Person aus demselben Grund ein Verfahren läuft [sowie] […] Maßnahmen zur Koordinierung bei strafrechtlichen Ermittlungen und laufenden Verfolgungen in den Mitgliedstaaten [ausgearbeitet werden können]".[356] Im Fortgang teilte die Kommission dem Rat und dem Europäischen Parlament im Juli 2000 Überlegungen zur gegenseitigen Anerkennung von Endentscheidungen in Strafsachen mit, die u.a. mit Blick auf den Grundsatz ne bis in idem Vorarbeiten zu einer allgemeinen Harmonisierung des jeweiligen internationalen Strafrechts der Mitgliedstaaten enthielten.[357] Hiernach sollten positive Kompetenzkonflikte zwischen den Mitgliedstaaten vermieden werden, indem grundsätzlich nur ein Mitgliedstaat zuständig sei, vorzugsweise der Staat des Handlungsorts bzw. der Unterlassung (Territorialitätsprinzip).[358] Die auf einer Sachverständigensitzung diskutierten Vorschläge der Kommission stießen jedoch, soweit sie sich auf eine starre Rangordnung von Anknüpfungspunkten bezogen, auf Ablehnung.[359]

Das von der Kommission bei renommierten Strafrechtsprofessoren in Auftrag gegebene Corpus Juris, welches Vorschläge für den Schutz der finanziellen Interessen der Gemeinschaft enthält, versucht positive Kompetenzkonflikte u.a. durch die Bildung eines europäischen Territorialitätsgrundsatzes unter starker Einengung der

---

Crime and Terrorism, S. 249 ff. Siehe hierzu auch *Sofaer*, in: Sofaer/Goodman, The Transnational Dimension of Cyber Crime and Terrorism, S. 221, 232 f.

354 Vertrag zur Gründung der Europäischen Gemeinschaft in der Fassung des Vertrages von Amsterdam vom 2.10.1997 (ABl. EG 1997, Nr. C 340, S. 1 ff.), zuletzt geändert durch EU-Beitrittsakte 2003 vom 16.4.2003 (ABl. EU 2003, Nr. L 236, S. 33 ff.).

355 Aktionsplan des Rates und der Kommission zur bestmöglichen Umsetzung der Bestimmung des Amsterdamer Vertrages über den Aufbau eines Raums der Freiheit, der Sicherheit und des Rechts, ABl. EG 1999, Nr. C 19, S. 1 ff.

356 Siehe Wiener Aktionsplan, ABl. EG 1999, Nr. C 19, S. 14 f., Rn. 49 c, e.

357 Kommission der Europäischen Gemeinschaften, KOM(2000) 495 endg., S. 19 ff.; Maßnahmenprogramm zur Umsetzung des Grundsatzes der gegenseitigen Anerkennung gerichtlicher Entscheidungen in Strafsachen, ABl. EG 2001, Nr. C 12, S. 15 f.

358 Andeutend in der Mitteilung der Kommission der Europäischen Gemeinschaften, KOM(2000) 495 endg., S. 22 f.

359 Arbeitsdokument der Kommissionsdienststellen, Anhang zum Grünbuch über Kompetenzkonflikte und den Grundsatz ne bis in idem in Strafverfahren, SEK(2005), 1767, S. 9.

Souveränität der Staaten auszuschalten, indem die „Staatsgebiete der Mitgliedstaaten der Union einen einheitlichen Rechtsraum für die Erforschung der Taten, für ihre Verfolgung, für das Hauptverfahren und für die Vollstreckung der Verurteilungen“[360] bilden sollen.[361] Innerhalb dieses Territoriums soll jedes Verfahren in dem Mitgliedstaat abgeurteilt werden, „dessen Gericht dafür im Interesse einer guten Rechtspflege am geeignetsten erscheint. […] Die wichtigsten Auswahlkriterien sind: a) der Staat, in dem sich der größte Teil der Beweise befindet, b) der Staat des Aufenthaltsortes oder der Staatsangehörigkeit des Beschuldigten (oder der Hauptbeschuldigten), c) der Staat, in dem die wirtschaftlichen Auswirkungen der Tat am größten sind“.[362] Eine abstrakte Rangfolge von Anknüpfungskriterien sieht das Corpus Juris indes nicht vor; es geht vielmehr von einer gesamteuropäischen Strafgewalt unter Einrichtung einer Europäischen Staatsanwaltschaft[363] aus, durch welche allerdings Kompetenzkonflikte streng genommen nicht gelöst, sondern nur auf eine untere Ebene, die der Gerichtszuständigkeit, verlagert werden.[364]

Ebenfalls gegen eine strenge Hierarchie von Kriterien zur Bestimmung der Zuständigkeit wandten sich die Verantwortlichen des Projekts „Finding the Best Place for Prosecution“ im Jahr 2002[365] sowie Eurojust nach einem 2003 zu diesem Themenkomplex durchgeführten Seminar in den Entscheidungsleitlinien „Die Lösung von Kompetenzkonflikten“.[366] Gleiches gilt für die Wissenschaftler des Max-Planck-Instituts für ausländisches und internationales Strafrecht in ihrer Untersuchung über konkurrierende Zuständigkeit und das Verbot der Mehrfachverurteilung in der Europäischen Union (2003)[367] sowie für ein im Auftrag des Bundesministeriums der Justiz 2001 erstelltes Gutachten zu der Frage, ob sich die Normierung einer europäischen Gerichtskompetenz für Strafgewaltskonflikte empfiehlt.[368] Die – im Ergebnis nicht erfolgreiche – Initiative Griechenlands aus dem Jahr 2003 für einen Rahmenbeschluss des Rates über die Anwendung des ne bis in idem-Prinzips[369] hob desgleichen auf ein individuell-konkretes Verfahren zur Ermittlung der Zuständigkeit eines Staates bei positiven Kompetenzkonflikten ab.[370]

---

360 Art. 18 Abs. 1 Corpus Juris 2000.

361 Zur deutschen Übersetzung des französischen und englischen Originaltextes von *Walter*, abrufbar unter http://www.uni-regensburg.de/Fakultaeten/Jura/walter/daten/publikationen/corpus_iuris_deutsch.pdf [Stand: 6.11.2013].

362 Art. 26 Abs. 2 Corpus Juris 2000.

363 *Ligeti*, Strafrecht und strafrechtliche Zusammenarbeit, S. 90.

364 Ebenda.

365 *Vander Beken* et al., Finding the Best Place for Prosecution, S. 59; siehe auch *Vander Beken/Vermeulen/Lagodny*, NStZ 2002, 624, 626.

366 Eurojust, Jahresbericht 2003, Anhang, S. 60 ff.

367 *Biehler* et al., Freiburg Proposal, S. 14, zu § 1 (3), Rn. 3, 5 f.

368 *Lagodny*, Strafgewaltkonflikte, S. 44 ff., 135.

369 ABl. EU 2003, Nr. C 100, S. 24 ff.

370 Siehe Art. 3, 4 und 6 des Vorschlags Griechenlands, ABl. EU 2003, Nr. C 100, S. 25 f.

Das Problem der Verhinderung und Lösung von Kompetenzkonflikten erneut angehend, legte die Kommission im Dezember 2005 das Grünbuch über die Kompetenzkonflikte und den Grundsatz ne bis in idem in Strafverfahren[371] vor. In diesem propagierte sie ein mindestens dreistufiges Verfahren zur Verhinderung und Lösung von Kompetenzkonflikten. In einem ersten Schritt sollten das Strafverfolgungsinteresse anderer Mitgliedstaaten festgestellt und diese sodann informiert werden.[372] Anschließend sei in einer zweiten, sogenannten Konsultations- und Diskussionsphase zu prüfen, welcher Staat zur Verfolgung am besten berufen wäre. Hierzu sollten inhaltliche Kriterien zur Abwägung der widerstreitenden Anknüpfungspunkte erarbeitet,[373] aber gleichzeitig auf eine starre Regelung verzichtet werden.[374] Die Kommission favorisierte im Ergebnis einen positiven Kriterienkatalog mit dem Territorialitätsprinzip als Hauptanknüpfungspunkt, wobei die Einzelheiten jedoch noch zu klären seien; insbesondere, ob und welche weiteren Prinzipien hinzutreten, wie sie zueinander in Beziehung stehen (Rangordnung und Ausschließlichkeit) sowie ob negative – nicht für die Konfliktlösung maßgebliche – Kriterien aufzunehmen seien.[375] Im dritten Schritt sollten die Mitgliedstaaten eine Streitbeilegung ggf. unter Einschaltung eines Mediators (z.B. Eurojust) anstreben.[376] In einem möglichen zusätzlichen Schritt sollte eine EU-Einrichtung eine verbindliche Entscheidung herbeiführen können.[377] Im letztlich verabschiedeten Rahmenbeschluss zur Vermeidung und Beilegung von Kompetenzkonflikten in Strafverfahren[378] sind allerdings weder eine verbindliche Rangordnung von Jurisdiktionskriterien noch eine Entscheidungskompetenz, sondern lediglich Mechanismen einer verbindlichen, direkten Konsultation zwischen den betroffenen Staaten festgelegt. Nunmehr sind der Kommission indes mit Art. 82 Abs. 1 UAbs. 2 lit. b und c

---

371 Kommission der Europäischen Gemeinschaften, KOM(2005) 696 endg.; Arbeitsdokument der Kommissionsdienststellen, Anhang zum Grünbuch über Kompetenzkonflikte und den Grundsatz ne bis in idem in Strafverfahren, SEK(2005), 1767.

372 Kommission der Europäischen Gemeinschaften, KOM(2005) 696 endg., S. 5; Arbeitsdokument der Kommissionsdienststellen, Anhang zum Grünbuch über Kompetenzkonflikte und den Grundsatz ne bis in idem in Strafverfahren, SEK(2005), 1767, S. 22 f.

373 Kommission der Europäischen Gemeinschaften, KOM(2005) 696 endg., S. 5 f.; Arbeitsdokument der Kommissionsdienststellen, Anhang zum Grünbuch über Kompetenzkonflikte und den Grundsatz ne bis in idem in Strafverfahren, SEK(2005), 1767, S. 23 ff.

374 Arbeitsdokument der Kommissionsdienststellen, Anhang zum Grünbuch über Kompetenzkonflikte und den Grundsatz ne bis in idem in Strafverfahren, SEK(2005), 1767, S. 38.

375 Ebenda, S. 38 ff.

376 Kommission der Europäischen Gemeinschaften, KOM(2005) 696 endg., S. 6; Arbeitsdokument der Kommissionsdienststellen, Anhang zum Grünbuch über Kompetenzkonflikte und den Grundsatz ne bis in idem in Strafverfahren, SEK(2005), 1767, S. 25 f.

377 Kommission der Europäischen Gemeinschaften, KOM(2005) 696 endg., S. 6; Arbeitsdokument der Kommissionsdienststellen, Anhang zum Grünbuch über Kompetenzkonflikte und den Grundsatz ne bis in idem in Strafverfahren, SEK(2005), 1767, S. 27 f.

378 Rahmenbeschluss 2009/948/JI des Rates vom 30.11.2009 zur Vermeidung und Beilegung von Kompetenzkonflikten in Strafverfahren, ABl. EU 2009, Nr. L 328, S. 42 ff.

AEUV weitere Handlungsmöglichkeiten an die Hand gegeben, den Rahmenbeschluss in eine (verbindlichere) Richtlinie zu transferieren,[379] auch wenn diesem Szenario nur wenige Erfolgsaussichten eingeräumt werden.[380]

(bb) Befürwortung einer individuell-konkreten Abwägung

Bei der zu favorisierenden individuell-konkreten Abwägung[381] sind im jeweiligen Einzelfall die konkret widerstreitenden Interessen der betroffenen Staaten – Individualinteressen sind nur beachtlich, soweit sie denen der Staaten entsprechen[382] – nach abstrakter Wertigkeit und konkretem Gewicht im Einzelfall gegenüberzustellen.

Ergibt die Würdigung der Interessen nach generellen Kriterien, dass das Eingriffsinteresse dem Abwehrinteresse nicht mindestens gleichwertig ist, darf der betroffene Staat sein Strafrecht nicht auf den Täter anwenden. Überwiegt dagegen das Eingriffsinteresse das Abwehrinteresse stets, so ist der Eingriff völkerrechtlich unbedenklich und einer Anwendung des nationalen Strafrechts durch den Eingriffsstaat steht nichts im Wege. Im dritten Falle, wenn weder das eine noch das andere Interesse generell, also nach seiner abstrakten Wertigkeit, obsiegt, ist die Abwägung nach den verschiedenen Wertigkeiten der Interessen innerhalb der Rechtsordnung des jeweiligen Staates und ihrer Anerkennung im Völkerrecht fortzuführen.

Zu unterscheiden sind Interessen von untergeordneter Bedeutung, solche von Verfassungsrang, staatstragende Interessen von Verfassungsrang sowie die Interessen, die den Bestand des Staates an sich betreffen.[383] Innerhalb der Interessengruppen hat eine weitere Differenzierung nach Ge- und Verbotsvorschriften sowie speziellen (z.B. verfassungsrechtliche Meinungsfreiheit, einfachrechtliche Genehmigungen durch die Verwaltung) und allgemeinen (z.B. verfassungsrechtliche allgemeine Handlungsfreiheit) freiheitsgewährenden Normen zu erfolgen.

Stehen sich Interessen aus der gleichen Gruppe gegenüber, sind sie aber in jeweils andere Unterkategorien innerhalb dieser Interessengruppe einzuordnen, so ist das Interesse des abwehrenden Staates, in dem der Täter aufgrund einer Gebotsnorm gehandelt hat, grundsätzlich höher zu bewerten als das Eingriffsinteresse des Staates, in dem der Täter gegen eine Verbotsnorm verstößt. Ebenso überwiegt die Ausübung einer speziellen Freiheit gegenüber der Verletzung einer allgemeinen aus der gleichen Kategorie und zieht damit ein Abwehrrecht gegenüber dem eingreifenden Staat nach sich.

---

379 *Eisele*, ZStW 125 (2013), 1, 11.

380 *Vogel*, in: Grabitz/Hilf/Nettesheim, Das Recht der Europäischen Union, Art. 82 AEUV, Rn. 61.

381 *Lagodny*, Strafgewaltkonflikte, S. 104.

382 *Meessen*, Völkerrechtliche Grundsätze des internationalen Kartellrechts, S. 107.

383 *Jennings*, BYIL 33 (1957), 146, 151 f.

Sind die sich gegenüberstehenden Interessen aber nach der Abwägung gleichwertig, so gebührt dem Eingriffsinteresse regelmäßig der Vorrang, da ein Eingriff keiner völkerrechtlichen Erlaubnis bedarf, sondern nur an entgegenstehenden Verboten scheitern kann. Damit ergibt sich ein Regel-Ausnahme-Verhältnis zugunsten des Eingriffsinteresses. Derjenige, der ein Abweichen vom Normalfall (ein Abwehrrecht) für sich reklamiert, muss dies nach allgemeinen Rechtsgrundsätzen darlegen und beweisen. Nur wenn der abwehrende Staat ein vom Normalfall abweichendes höherwertiges Interesse nachweisen kann, geht die Abwägung zu seinen Gunsten aus. Im Zweifel verbleibt es daher bei der Regel (Eingriffsrecht). Die Kollision gleichwertiger Interessen entscheidet also generell das Eingriffsinteresse für sich; der Eingriff ist in diesen Fällen prinzipiell völkerrechtskonform.

Anders verhält es sich nur, wenn der Abwehrstaat in seinem Bestandsinteresse betroffen ist. Da das Bestandsinteresse eines Staates seine ureigensten Interessen und damit den Kern seiner völkerrechtlichen Existenz betrifft, ist ein solches als absolut geschützt anzusehen. Dies hat zur Folge, dass ein überwiegendes Eingriffsinteresse nicht denkbar ist. Auch der Fall eines auf das eigene Bestandsinteresse gründenden Eingriffs – etwa wenn ein Staat im Internet zum Sturz der Regierung eines anderen Staates aufruft[384] – kann dann nicht zur Rechtfertigung des Eingriffs führen. In diesem Fall stößt das Völkerrecht als eine auf Koexistenz und gedeihliche Zusammenarbeit angelegte Rechtsordnung an seine Grenzen. Es ist gerade kein abgeschlossenes Rechtssystem, welches jeden Streitfall löst bzw. lösen kann.[385]

Einen Sonderfall bilden die Konstellationen, in denen die zugrunde liegende Materie Gegenstand völkerrechtlicher Vereinbarungen zwischen den beteiligten Völkerrechtssubjekten ist. Die in solchen Verträgen getroffenen Regelungen geben eine Leitschnur für die Gewichtung von Eingriffs- und Abwehrinteresse vor. Verstößt der eingreifende Staat gegen ein Verbot aus einem völkerrechtlichen Vertrag, so wird sein Eingriffsinteresse aufgrund der bindenden Übereinkunft regelmäßig zurückstehen müssen. Nur im Ausnahmefall überwiegt das Eingriffsinteresse, weil entweder der Vertrag selbst Ausnahmevorschriften für besondere Fälle vorsieht oder die getroffene Vereinbarung in Extremfällen aus übergeordneten Rechtsgrundsätzen (etwa dem Rechtsmissbrauchsverbot) unanwendbar sein kann. Im Normalfall muss bei vertraglichen Verbotsnormen allerdings das Eingriffs- hinter das Abwehrinteresse zurücktreten. Umgekehrt gilt die durch Vertrag festgelegte Gewichtung von Abwehr- und Eingriffsinteresse bei völkervertraglichen Erlaubnisnormen zugunsten des Letzteren – auch hier aber nur bis zur Grenze übergeordneter Rechtsprinzipien.

---

[384] So z.B. die Auseinandersetzungen zwischen Indien und Pakistan, insbesondere um die Region Kaschmir.

[385] *Bertele*, Souveränität und Verfahrensrecht, S. 53.

dd) Zwischenergebnis

Deutsche Strafverfolgungsbehörden sind für die Ermittlung und Verfolgung von im Internet begangenen Straftaten, wenn der Täter vom Ausland aus agiert, nur eingeschränkt zuständig, da bereits der nationale Gesetzgeber völkerrechtlichen Einschränkungen bei der Ausgestaltung seines internationalen Strafanwendungsrechts unterliegt und damit zugleich auch der Anwender bei der Vollziehung des Rechts. Die Begrenzung der allgemeinen völkerrechtlichen Freiheit, ohne spezielle Erlaubnisnorm Sachverhalte mit Auslandsbezug nationalen Regelungen zu unterwerfen, ist durch Ausgleich der entgegenstehenden Interessen für den jeweiligen Einzelfall zu ermitteln, wobei dieser in zwei Schritten – der Interessenfeststellung und der Interessenabwägung – vorzunehmen ist. Ein Rückgriff auf das allgemeine Rechtsmissbrauchsverbot oder die alleinige Bezugnahme auf das Erfordernis eines genuine link führt dagegen zu keiner gerechten Lösung von positiven Jurisdiktionskonflikten.

Ein völkerrechtlich relevantes Eingriffsinteresse kann derjenige Staat vorweisen, der einen sinnvollen Anknüpfungspunkt zur Tat hat. Bei extraterritorialem Handeln existiert ein solcher insbesondere, wenn eine Verletzung oder konkrete Gefährdung eines Rechtsguts auf dem Staatsgebiet des eingreifenden Staates eintritt. In diesen Fällen liegt dann auch ein Erfolgstatort i.S.d. § 9 Abs. 1, 3. Var. StGB vor. Nicht ausreichend sind dagegen abstrakte oder abstrakt-konkrete Gefährdungen. Das Abwehrinteresse geht regelmäßig aus dem völkerrechtlich geschützten Recht des abwehrenden Staates auf Selbstbestimmung hervor. Beide entgegengesetzten Interessen sind bei der Konfliktlösung auszugleichen. Innerhalb der Interessenabwägung ist eine Eingruppierung der jeweiligen Interessen nach Bestandsinteresse, staatstragendem Interesse von Verfassungsrang, Interesse von Verfassungsrang und sonstigem Interesse vorzunehmen. Eine Unterteilung dieser Gruppen erfolgt weiter nach Ge- und Verbotsnormen sowie nach speziellen und allgemeinen freiheitsgewährenden Normen. Bei Gleichwertigkeit der Interessen überwiegt in der Regel das Eingriffsinteresse. Völkerrechtliche Verträge nehmen eine eigenständige Gewichtung von Abwehr- und Eingriffsinteresse vor, die nur in seltenen Fällen, insbesondere durch übergeordnete Rechtsprinzipien, durchbrochen werden kann.

b) Ausreichen der strafrechtlichen und strafprozessualen Begrenzungen

Das vorstehend ermittelte Auslegungsergebnis, wonach die Zuständigkeit der deutschen Strafverfolgungsbehörden bei Auslandstaten völkerrechtlich auf solche mit tatbestandsmäßigen Verletzungen oder konkreten Gefährdungen im Inland beschränkt ist, erfährt durch das allgemeine Straf- und Strafprozessrecht zusätzliche Einschränkungen (nachfolgend unter aa) und bb)). Darüber hinaus bedarf es – im Unterschied zu den eingangs dargestellten Auffassungen zur Frage der Anwend-

barkeit des deutschen Strafrechts auf im Ausland begangene Straftaten im Internet[386] – keiner weitergehenden Begrenzung.

aa) Strafrechtliche Begrenzungen der Strafbarkeit des Täters

Die Ahndung von Straftaten ist insbesondere durch das Erfordernis der Zurechenbarkeit eines tatbestandlichen Erfolgs (nachfolgend unter (1)) sowie die Schuld des Täters (unter (2)) – speziell unter Berücksichtigung des Verbotsirrtums – über das gewonnene Auslegungsergebnis hinaus beschränkt. Des Weiteren ist im Einzelfall nach Art. 296 EGStGB schon auf Tatbestandsebene die Strafbarkeit ausgeschlossen (unter (3)).

(1) Zurechenbarkeit des Erfolgs

Strafgerichte können einen Täter nur wegen ihm zurechenbarer tatbestandlicher Erfolge bestrafen; fehlt es an einem solchen Erfolgseintritt, ist er nicht zu verurteilen. Der durch menschliches Verhalten verursachte Erfolg ist objektiv zurechenbar, wenn der Täter eine rechtlich missbilligte Gefahr schafft und sich diese Gefahr in dem tatbestandsmäßigen Erfolg verwirklicht.[387] Ist dagegen der in Gang gesetzte Kausalverlauf bzw. die geschaffene Erfolgsgefahr nicht beherrsch- und steuerbar oder verringert der Täter ein bereits geschaffenes Risiko, ist ihm der Erfolg nicht zurechenbar.[388] Gleiches gilt, wenn sich der Täter nicht pflichtwidrig verhält bzw. auch bei pflichtgemäßem Verhalten der Erfolg eingetreten wäre und wenn die geschaffene Gefahr sich nicht im eingetretenen Erfolg realisiert oder der Erfolg außerhalb des Schutzzweckzusammenhangs liegt.[389]

(a) Keine Bestimmung in Abhängigkeit der Technik

Ob ein zurechenbarer tatbestandlicher Erfolg bei im Internet begangenen Straftaten immer vorliegt, ist infolge der technischen Besonderheiten des Netzes fraglich. Die Auswirkungen einer Straftat im Internet beschränken sich nämlich i.d.R. nicht auf wenige Staaten, sondern wirken sich häufig weltweit aus. So verbreitete

---

386 Siehe dazu im Einzelnen die unter Teil 2, II.C.3.a)–f) aufgeführten Ansichten.

387 BayObLGSt 48 (1998), 97, 102; *Fischer*, StGB, Vor § 13, Rn. 25; *Jescheck/Weigend*, Strafrecht AT, § 28 IV (S. 287); *Kühl*, Strafrecht AT, § 4, Rn. 43; SK-StGB-*Rudolphi*, Vor § 1, Rn. 57.

388 *Fischer*, StGB, Vor § 13, Rn. 27 f.; *Jescheck/Weigend*, Strafrecht AT, § 28 IV (S. 287 f.); S/S-*Lenckner/Eisele*, Vorbem. §§ 13 ff., Rn. 93 f.; *Roxin*, Strafrecht AT, § 11, Rn. 53 ff.

389 *Fischer*, StGB, Vor § 13, Rn. 29 f.; *Jescheck/Weigend*, Strafrecht AT, § 28 IV (S. 288 f.); S/S-*Lenckner/Eisele*, Vorbem. §§ 13 ff., Rn. 95/96 ff.; *Roxin*, Strafrecht AT, § 11, Rn. 65 ff., 84 ff.

sich z.B. der Blaster-Wurm (auch Lovesan-Wurm genannt) im Jahr 2003 weltweit über das Internet und sonstige Netzwerke und führte zu unkontrollierten Rechnerabstürzen nach sogenannten Distributed Denial of Service (DDoS)-Attacken. Der Wurm nutzte bei den angegriffenen Rechnern eine Schwachstelle in Windows NT/2000/XP- und Windows Server 2003-Systemen. Die so von ihm infizierten Computer führten ihrerseits eine Denial of Service (DoS)-Attacke gegen einen Microsoft-Server aus. Da erst die speziellen technischen Gegebenheiten des Internet diese weltweiten Auswirkungen ermöglichten, könnte die Technik entscheidenden Einfluss auf die Beantwortung der Frage nach der objektiven Zurechenbarkeit von tatbestandlichen Erfolgen haben.

Manche Literaturvertreter[390] befassen sich bereits bei der Ermittlung der Anwendbarkeit des deutschen Strafrechts auf Internetsachverhalte mit der objektiven Zurechnung tatbestandlicher Erfolge, indem sie auf die Unterscheidung des Auf- und Herunterladens von Daten in Push- und Pull-Technologien abstellen.

Ob ein Internetnutzer technisch betrachtet im Einzelfall aktiv mittels Push-Technologie handelt oder passiv bleibt (Pull-Technologie), führt jedoch zu keiner eindeutigen juristischen Bewertung der Zurechenbarkeit von tatbestandlichen Erfolgen.[391] Die technischen Abläufe bei Push- und Pull-Technologien gleichen sich nämlich bei näherem Hinsehen. Entweder der Empfänger fordert Daten an und gibt ihren Weg in seinen Rechner frei (Pull) oder er wird benachrichtigt, dass Daten zum Abruf bereitstehen und nimmt diese dann unter Öffnung seines Rechners auf (Push). Bereits aus Sicherheitsgründen ist der Rechner des Empfängers regelmäßig für den Empfang von Daten so lange gesperrt, bis dessen Öffnung durch einen gesonderten Befehl erfolgt. Im Fall der Push-Technologie stimmt der Empfänger also einer *ihm angebotenen* Übertragung zu, während er bei der Pull-Technologie seinen Rechner für eine *von ihm erbetene* Übertragung von Daten öffnet. Die vereinfachende technische Differenzierung zwischen Aktivität und Passivität des jeweiligen Nutzers anhand des Einsatzes von Push- oder Pull-Technologien täuscht also darüber hinweg, dass die Übertragung der Daten in beiden Fällen auf gleichem Wege erfolgt. Die automatische Bearbeitung der Anfragen aufseiten des Anbieters bei Verwendung der Pull-Technologie stellt lediglich eine zur Vereinfachung der Abwicklung eingesetzte Arbeitshilfe dar, die in umgekehrter Richtung auch bei der Push-Technologie Anwendung findet. So erfolgt bei Letzteren, z.B. bei der Ver-

---

[390] *Gercke*, Rechtswidrige Inhalte im Internet, S. 29 f.; *Sieber*, NJW 1999, 2065, 2071 f.; *ders.*, in: Koops/Brenner, Cybercrime and Jurisdiction, S. 183, 200 f.; *Volk*, Glücksspiel im Internet, S. 206, 208.

[391] Gegen eine alleinige Abhängigkeit der strafrechtlichen Beurteilung von den technischen Gegebenheiten BGH MMR 2001, 676, 677 f. = BGH NStZ 2001, 596, 597; BGH NJW 2001, 3558, 3559; *Hilgendorf*, ZStW 113 (2001), 650, 653, 668; *Klam*, Die rechtliche Problematik von Glücksspielen im Internet, S. 63; *Poenig*, Die strafrechtliche Haftung des Linkanbieters, S. 174 f.; *Schmidt*, Gefahrenabwehrmaßnahmen im Internet, S. 255; *Schwarzenegger*, ZStrR 118 (2000), 119, 126 (für die Schweiz).

sendung von E-Mails, aus Sicherheitsgründen keine direkte Datenverbringung auf den Rechner des Empfängers ohne dessen vorherige Einwilligung. In der Regel findet eine Zwischenspeicherung auf einem Mailserver o.Ä. statt, von dem sich der Empfänger die Daten aus eigenem Entschluss und ohne weitere Rückgriffsmöglichkeit des Absenders an seinen Rechner senden lässt.

Gegen eine pauschale Abgrenzung nach der Art des Zugriffs auf Daten spricht ferner, dass unter Berücksichtigung der klassischen Dienste des Internet dem Anbieter, der Daten auf den Empfängerrechner lädt, nur dann ein Erfolg zurechenbar wäre, wenn er etwa eine E-Mail direkt an den Empfänger in Deutschland schickte. Schon wenn die E-Mail – wie üblich – zunächst an einen externen Mailserver (der u.U. im Ausland steht) versendet würde und der Adressat diese bei dem Mailserver abrufen müsste, würde nach der vorstehend beschriebenen Abgrenzung von Pull- und Push-Technologien das selbstständige Abrufen streng genommen wieder unter Einsatz einer Pull-Technologie erfolgen und somit ein eigenverantwortliches Handeln eines Dritten darstellen, welches dem Anbieter gerade nicht mehr zurechenbar sein soll.[392] Bei strikter Befolgung einer Abgrenzung zwischen Pull- und Push-Technologien wäre eine Strafbarkeit des Anbieters im vorgenannten Fall nur zu bejahen, wenn der Empfänger sich die E-Mail nicht selbstständig von seinem Mailserver herunterladen müsste. Diese an den technischen Gegebenheiten und praktischen Bedürfnissen vorbeigehende künstliche Aufspaltung geht aber über eine sinnvolle Abschichtung der Verantwortungsbereiche hinaus und bürdet dem eigentlichen Opfer in diesem Fall eine Verantwortung für fremdes Fehlverhalten auf.

Zudem spricht gegen eine strenge technische Unterscheidung auch die Abhängigkeit der Bestimmung strafrechtlich relevanter Erfolge allein von den technischen Gegebenheiten. In weiten Bereichen des Internet, wie etwa in den über das WWW verfügbaren Diensten (z.B. News-Dienst,[393] Seitenabrufe[394] etc.), finden Push-Technologien nur eingeschränkt Anwendung, sodass ganze Bereiche des Internet keiner befriedigenden Problemlösung zugeführt würden.[395]

Es kann also keine verallgemeinernde Aussage getroffen werden, dass beim Herunterladen von Daten der Empfänger objektiv zurechenbar einen tatbestandlichen Erfolg herbeiführte, während dem Anbieter der Daten der entsprechende Erfolg nicht zurechenbar sei. Auch der pauschalen Aussage, beim Upload von Daten handele der Anbieter aktiv, sodass ihm ein eintretender tatbestandlicher Erfolg

---

[392] *Gercke*, Rechtswidrige Inhalte im Internet, S. 29.

[393] *Poenig*, Die strafrechtliche Haftung des Linkanbieters, S. 175; *Schmidt*, Gefahrenabwehrmaßnahmen im Internet, S. 255.

[394] EuGH, Urteil vom 6.11.2003, *Strafverfahren gegen Bodil Lindqvist*, Rs. C-101/01, Slg. 2003, S. I-00000 ff., Rn. 68 ff. (der in dem Zugänglichmachen von Inhalten auf einer Internetseite noch keine Übermittlung von Daten sieht).

[395] *Schwarzenegger*, ZStrR 118 (2000), 126 (für die Schweiz).

objektiv zurechenbar sei, dem Empfänger der Daten der Erfolg jedoch nicht,[396] ist zu widersprechen. Eine Differenzierung nach der Art des Zugriffs auf Daten ist wegen der nur scheinbar eindeutigen technischen Unterscheidbarkeit nicht entscheidend für die Untersuchung der objektiven Zurechnung eines tatbestandlichen Erfolgs.

(b) Bestimmung nach allgemeinen Grundsätzen

Die Zurechenbarkeit tatbestandlicher Erfolge gegenüber dem Empfänger oder dem Absender strafbarer Inhalte ist vielmehr unter Berücksichtigung der allgemeinen in der Strafrechtslehre herausgearbeiteten Voraussetzungen der objektiven Zurechnung zu bestimmen.

Eine objektive Zurechenbarkeit des Erfolgs scheidet mangels Begründung eines tatbestandstypischen Risikozusammenhangs für den Ersttäter aus, wenn ein Dritter zwar an das gefahrtragende Verhalten des Ersttäters anknüpft, aber mit seiner (Zweit-)Handlung eine eigene Gefahr schafft, die sich – von der Ersthandlung unabhängig – in dem nachfolgenden Erfolg realisiert.[397] Werden mehrere Personen nacheinander bzw. u.U. auch nebeneinander tätig, so sollen sie selbst für ihr jeweiliges Verhalten Verantwortung übernehmen – sofern die Personen nicht vorsätzlich als Beteiligte zusammenwirken und somit die Regelungen der §§ 25 ff. StGB als speziellere Vorschriften für die Zurechnung fremden Verhaltens eingreifen. Damit wird der einzelne Täter nur für das Verhalten strafrechtlich zur Verantwortung gezogen, welches ihm auch tatsächlich vorzuwerfen ist.[398] Sendet beispielsweise A dem B eine E-Mail zu, in welcher er B verleumdet, und fängt C die E-Mail ab, um diese anschließend zu verfälschen und D im Namen von A zu verleumden, so hat A zwar ursprünglich die Gefahr der Verleumdung geschaffen, der tatbestandliche Erfolg der Verleumdung gegenüber D ist dem A aber objektiv nicht zurechenbar. Nicht anders verhält es sich, wenn A eine Webseite im Internet betreibt und B sich von dort strafbare Inhalte herunterlädt. Die Verantwortungsbereiche von A und B sind klar abgegrenzt, Ersterer hat strafbare Inhalte zur Verfügung gestellt, Letzterer ruft diese ab. Beide machen sich strafbar, wenn das Gesetz sowohl das Zugänglichmachen als auch das Sichverschaffen der betreffenden Inhalte unter Strafe stellt. Wird lediglich eine dieser Verhaltensweisen vom Gesetzgeber für strafwürdig erachtet, so ist demjenigen, der die strafbewehrte Handlung nicht selbst begangen hat, diese nach dem Verantwortungsprinzip grundsätzlich nicht zurechenbar. Etwas anderes gilt nur dann, wenn gesetzlich festgeschrieben ist, dass derjenige,

---

396 So aber *Sieber*, NJW 1999, 2065, 2072; *ders.*, in: Koops/Brenner, Cybercrime and Jurisdiction, S. 183, 200 f.; ihm folgend *Gercke*, Rechtswidrige Inhalte im Internet, S. 29; wohl auch *Vec*, NJW 2002, 1535, 1538.

397 S/S-*Lenckner/Eisele*, Vorbem. §§ 13 ff., Rn. 101, 101a; *Roxin*, Strafrecht AT, § 11, Rn. 30.

398 S/S-*Lenckner/Eisele*, Vorbem. §§ 13 ff., Rn. 100.

der den Erfolg mittelbar verursacht hat, sich die weiteren Folgen des eigenverantwortlichen Handelns eines Dritten zurechnen lassen muss. So werden etwa nach § 29 Abs. 3 Nr. 2, § 30 Abs. 1 Nr. 3 BtMG[399] durch Gesetz dem Lieferanten von Rauschgift die beim Konsumenten eintretenden schweren Folgen zugerechnet. Fehlt die gesetzliche Bestimmung einer solchen Zurechnung, ist diese weder aus einer analogen Anwendung von Normen, in denen der Gesetzgeber eine solche bestimmt hat,[400] noch aus den Grundsätzen der objektiven Zurechnung herleitbar.

Der Eintritt eines tatbestandlichen Erfolgs ist dem Ersttäter aber auch zurechenbar, wenn er dafür Sorge zu tragen hat, dass sich ein Dritter die von ihm geschaffene Lage nicht zunutze macht, oder wenn sich die erfolgsvermittelnde Zweithandlung als Rettungshandlung darstellt und der Retter den Erfolg nur leicht fahrlässig herbeigeführt hat.[401] Hackt sich A beispielsweise in eine der im Internet zum Abruf bereitgehaltenen Hassseiten des B ein, um diese zu übernehmen und zu entfernen, und versendet er beim Herunterladen der Daten zu Beweiszwecken die Seite an eine Vielzahl von Unbeteiligten, so ist B die Verbreitung durch A in der Regel zurechenbar. Dieser Schluss beruht auf dem Gedanken, dass Internetnutzer Daten regelmäßig mit dem Willen in das Internet einstellen, diese allgemein und unkontrolliert zum Abruf zur Verfügung zu stellen. Dem Ersttäter ist damit grundsätzlich der jeweilige tatbestandliche Erfolg des Zweittäters zurechenbar. Der Fall, dass durch einen bezweckten Abruf eine neue, abweichende Gefahr geschaffen wird, die eine objektive Zurechnung tatbestandlicher Erfolge entfallen lässt, wird nur ausnahmsweise vorliegen. Eine solche Konstellation ist etwa dann denkbar, wenn der Informationsanbieter geeignete Vorsichtsmaßnahmen (z.B. Passwortschutz) gegen eine unkontrollierte Verbreitung seiner Daten ergriffen hat. Nur dann schafft der Empfänger, der die Kontrollmechanismen durchbricht, eine nicht mehr im Einflussbereich des Anbieters liegende Gefahr. An die Kontrollmaßnahmen müssen jedoch erhöhte Anforderungen gestellt werden. Ein nur der Form halber aufgenommener Schutz vor einem Zugriff Dritter ist von vornherein wertlos. Allerdings kann auch ein absoluter Schutz vor unbefugten Zugriffen Dritter nicht verlangt werden, da ein solcher nach derzeitigem technischem Stand nicht möglich ist.

Zusammenfassend ist Folgendes festzuhalten: Die Zurechenbarkeit eines tatbestandlichen Erfolgs kann durch eine eigenständige Handlung eines Dritten, die zwar an die vom Ersttäter geschaffene Gefahr anknüpft, aber eine eigene, von dieser unabhängige neue Gefahr begründet, durchbrochen werden. Dem Ersttäter sind die Handlungen Dritter jedoch zurechenbar, wenn ihn eine besondere Sorgfaltspflicht zur Abwendung eines Schadens durch eine Weiterverwendung der Daten

---

[399] Gesetz über den Verkehr mit Betäubungsmitteln vom 28.7.1981, BGBl. I 1981, S. 681, 1187, zuletzt geändert durch Artikel 1 der Verordnung vom 9.7.2013, BGBl. I 2013, S. 2274.

[400] S/S-*Lenckner/Eisele*, Vorbem. §§ 13 ff., Rn. 101b.

[401] Ebenda, Rn. 101c ff.

trifft. Im Regelfall liegt ein zurechenbarer tatbestandlicher Erfolg vor. Wirken der Erst- und der Zweittäter zusammen, müssen sie sich ihre Handlungsbeiträge zurechnen lassen. Nicht von entscheidender Bedeutung ist hingegen, ob der Datentransfer vom Anbieter selbst mittels Push-Technologie seinen Weg nimmt oder, ob der Internetnutzer sich die Daten selbst holt (Pull-Technologie).

(2) Schuld des Täters

Handelt der Täter ohne Schuld, ist er gleichfalls nicht zu bestrafen. Der Feststellung der Schuld des Täters kommt daher eine wesentliche Bedeutung für dessen Strafbarkeit zu.

(a) Verbotsirrtum, § 17 StGB

Als ein ausgleichendes Element gegenüber der u.U. weitläufigen Erfolgsbegründung bei der Verwirklichung von Straftaten im Internet dient auf der Schuldebene der Verbotsirrtum nach § 17 StGB. Bei der Feststellung der Schuld geht es nicht darum, dass der Täter im Einzelfall das Bewusstsein besessen hat, mit seiner Tat den Geltungsbereich eines fremden Strafrechts zu berühren oder gar speziell nach deutschem Strafrecht verantwortlich zu sein.[402] Die Regelungen über die Anwendbarkeit des Strafrechts sind nämlich nicht Teil des zu verwirklichenden Tatbestands,[403] auf welchen sich das Unrechtsbewusstsein beziehen muss. Maßgeblich ist allein, ob der Täter in der konkreten Sachverhaltskonstellation wissen musste oder wissen konnte, dass die von ihm verwirklichte Rechtsgutsverletzung Unrecht ist.[404]

Straftaten im Internet sind wegen des grenzüberschreitenden Charakters des Netzes regelmäßig Distanzdelikte, da der Handlungs- und der Erfolgsort auseinanderfallen. Aufgrund der u.U. verschiedenartigen Lebensumstände und der sich unterscheidenden Lebensumgebung am Tatort kann ein Spannungsverhältnis zwischen den in den betroffenen Kulturkreisen sich unterscheidenden Ansichten darüber entstehen, was Unrecht ist und was nicht. Dieses Verhältnis lässt sich auf der Ebene der Schuld, wo es um das Unrechtsbewusstsein des Täters geht, bei der Prüfung des Verbotsirrtums berücksichtigen.[405]

---

[402] BGH NJW 1999, 2908, 2909; LK-StGB[12]-*Werle/Jeßberger*, Vor § 3, Rn. 453; *Zieher*, Das sog. Internationale Strafrecht nach der Reform, S. 69.

[403] MünchKommStGB-*Ambos*, Vor §§ 3–7, Rn. 3; S/S-*Eser*, Vorbem. §§ 3–9, Rn. 79; *Jescheck/Weigend*, Strafrecht AT, § 18 V (S. 180); *Satzger*, Jura 2010, 108, 111; LK-StGB[12]-*Werle/Jeßberger*, Vor § 3, Rn. 452.

[404] MünchKommStGB-*Ambos*, Vor §§ 3–7, Rn. 3; S/S-*Eser*, Vorbem. §§ 3–9, Rn. 79; *Jescheck/Weigend*, Strafrecht AT, § 18 V (S. 180).

[405] *Jofer*, Strafverfolgung im Internet, S. 114 ff.; *Volk*, Glücksspiel im Internet, S. 225.

Der Schuldvorwurf entfällt, wenn der Täter zum Zeitpunkt der Tat kein Unrechtsbewusstsein besessen hat und das Fehlen des Unrechtsbewusstseins und damit der Irrtum über das Unrecht nicht vermeidbar war (§ 17 Satz 1 StGB). Nach herrschender Ansicht fehlt dem Täter das Unrechtsbewusstsein, wenn er sich in Bezug auf den konkreten Tatbestand zur Tatzeit nicht bewusst war, dass er mit seinem Verhalten gegen irgendeine gesetzliche Bestimmung verstoßen und damit Unrecht begehen würde.[406] Nicht ausreichend hierfür ist jedoch, dass der Täter im Tatzeitpunkt lediglich kein aktuelles Bewusstsein besaß, Unrecht zu tun. Ein sachgedankliches Mitbewusstsein, d.h. das bloße Begleitwissen, etwas Verbotenes zu tun,[407] genügt. Soll die Schuld des Täters ausscheiden (§ 17 Satz 1 StGB), so darf zudem der Irrtum über das Unrecht nicht vermeidbar gewesen sein. Vermeidbar ist ein Verbotsirrtum, wenn dem Täter sein Vorhaben unter Berücksichtigung seiner Fähigkeiten und Kenntnisse hätte Anlass geben müssen, über dessen mögliche Rechtswidrigkeit nachzudenken oder sich zu erkundigen, und er auf diesem Wege zur Unrechtseinsicht gekommen wäre.[408]

Im Alltag sind zwar Fälle denkbar, in denen der inländische Täter das Bewusstsein, etwas Verbotenes zu tun, nicht besitzt, der Irrtum darüber wird aber regelmäßig vermeidbar sein. Es spielt für gewöhnlich keine Rolle, ob der Täter in Deutschland lebt oder sich hier nur als Gast aufhält. Beiden Personengruppen ist es nämlich grundsätzlich zumutbar, sich über das Recht ihres Aufenthaltstaates zu informieren. Scheidet daher ein unvermeidbarer Verbotsirrtum aus, bleibt nur die Möglichkeit der Strafmilderung nach § 17 Satz 2 StGB.[409] Für Personen, die im Ausland zu Hause sind, gelten im Grundsatz keine anderen Anforderungen. Insbesondere deutsche Staatsbürger, die nur im Ausland verweilen, werden regelmäßig schon aufgrund ihrer Herkunft über das Unrechtsbewusstsein verfügen; auch bei Ausländern, denen die Rechtsauffassungen in Deutschland geläufig sind, wird das der Fall sein. Allerdings kann sich das Unrechtsbewusstsein von In- und Ausländern im Einzelfall wegen der zum Teil stark abweichenden Kulturkreise, die das Bewusstsein, Unrecht zu tun, vornehmlich prägen, erheblich voneinander unterscheiden. Deshalb ist eine differenzierte Beurteilung im Einzelfall gerechtfertigt. Da in diesen Ausnahmefällen nicht wesentlich Gleiches, sondern wesentlich Ungleiches nicht gleich behandelt wird, geht damit auch kein Verstoß gegen Art. 3 Abs. 1 GG einher.[410] Zwar kann bei sich im Ausland aufhaltenden Personen für das Unrechtsbewusst-

---

406 BGHSt 11, 263, 266; OLG Stuttgart JR 1993, 328, 330; S/S-*Sternberg-Lieben*, § 17, Rn. 8 ff.

407 LK-StGB[12]-*Vogel*, § 17, Rn. 26.

408 *Fischer*, StGB, § 17, Rn. 7.

409 *Hilgendorf*, ZStW 113 (2001), 650, 676.

410 Ausländer sind ebenfalls Begünstigte des Gleichheitsgrundsatzes nach Art. 3 Abs. 1 GG – *Jarass*, in: Jarass/Pieroth, GG, Art. 3, Rn. 5.

sein entgegen anderer Ansicht[411] nicht einschränkend verlangt werden, dass sich das Bewusstsein, Unrecht zu tun, dahingehend konkretisiert, dass ein bestimmtes Verhalten nach deutschem Recht Unrecht darstellt. Die Anwendbarkeit des deutschen Strafrechts ist nämlich gerade nicht Teil des Tatbestands, auf den allein sich das Unrechtsbewusstsein beziehen muss. Eine für zu weit befundene Jurisdiktionserstreckung kann also nicht mit dem Mittel des Verbotsirrtums systemfremd nachträglich korrigiert werden. An eine Person aus dem Ausland, der das Wissen um die deutschen Gesetze fehlt, können aber nicht die hohen Anforderungen an die Vermeidbarkeit des Irrtums über das Unrecht gestellt werden, die einen Inländer oder eine sich im Ausland befindliche Person, der das Recht bekannt ist, treffen.[412] Zu einer Überspannung der Anforderungen an die betreffende Person würde es führen, wenn ihr die Pflicht auferlegt würde, sich grundsätzlich immer über das Recht aller Länder der Welt zu informieren, bevor sie bestimmte Daten ins Internet einstellt.[413] An dieser Bewertung ändert auch die durch das Internet bestehende einfachere Möglichkeit der Recherche nichts. Nicht jedes Land verfügt über kodifiziertes Recht und darüber hinaus ist es regelmäßig unzumutbar, sich eine Übersetzung sämtlicher einschlägiger geschriebener Gesetze oder Rechtsprechung zu beschaffen.

Bei Straftaten von Ausländern im Internet mit einem Erfolgsort in Deutschland wird ein unvermeidbarer Verbotsirrtum nach dem Vorstehenden also dann anzunehmen sein, wenn der Täter mit dem deutschen Recht bisher nicht in Berührung gekommen war und bei der Tat keinen besonderen Anlass hatte, sich gerade auch in Bezug auf die Strafbarkeit nach deutschem Recht zu informieren. Dies gilt umso mehr, wenn die Tat nach dem Recht des Handlungsorts nicht mit Strafe bedroht, sondern erlaubt oder sogar geboten war. Für den Täter darf die Strafbarkeit also nicht vorhersehbar gewesen sein. Kommuniziert der Täter hingegen bewusst mit Personen eines bestimmten Staates, wird er regelmäßig ein Unrechtsbewusstsein bilden können;[414] in diesen Fällen war es für ihn vorhersehbar, dass er sich strafbar machen kann.[415] Unvermeidbar ist aber auch hier der Irrtum, wenn sich der Täter zuvor hat hinreichend rechtlich beraten lassen und nach diesem Rechtsrat eine Strafbarkeit für sich ausschließen konnte.[416]

---

411 So aber wohl *Jofer*, Strafverfolgung im Internet, S. 115; *Oehler*, Internationales Strafrecht, Rn. 159; *Valerius*, NStZ 2003, 341, 343 f.; *Volk*, Glücksspiel im Internet, S. 225.

412 *Hilgendorf*, ZStW 113 (2001), 650, 676.

413 *Valerius*, NStZ 2003, 341, 345.

414 Ebenda.

415 Zum Vorhersehbarkeitserfordernis siehe Council of Europe, Extraterritorial criminal jurisdiction, S. 22 ff.

416 OLG Stuttgart CR 2006, 634, 635 f. zum unvermeidbaren Verbotsirrtum bei Online-Angebot von Glücksspiel im EU-Ausland.

(b) Überzeugungstäter

Ein weiteres das Unrechtsbewusstsein beeinflussendes Moment ist die Überzeugung, mit welcher der Täter im Einzelfall mit dem Wissen z.B. Daten ins Netz stellt, dass er sich hiermit nach dem Recht anderer Staaten strafbar macht. Problematisch sind insbesondere jene Fälle, in denen der Täter nach dem Recht des Handlungsorts rechtmäßig handelt, seine Handlung in einem anderen Staat aber einen verbotenen Erfolg herbeiführt.

Die wohl erstmals von *Radbruch* unter dem Begriff des Überzeugungsverbrechers[417] diskutierte Problematik befasst sich also mit Tätern, die sich durch ihre innere Überzeugung (sittlicher, religiöser oder politischer Art) auszeichnen, mit der sie eine bestimmte Handlung in dem Wissen vornehmen, sich gegen geltendes Recht zu stellen.[418] Die Überzeugung des Täters, z.B. weil er die Verbindlichkeit der Verbotsnorm für sich selbst ablehnt, lässt sein Unrechtsbewusstsein nicht entfallen.[419] Ein die Schuld ausschließender Verbotsirrtum kann folglich nicht vorliegen. Vielmehr kann gerade die Ablehnung einer Verbotsnorm als Ausdruck der Ablehnung einer gesellschaftlichen Ordnung insgesamt, wie dies beispielsweise für terroristische Aktivitäten typisch ist,[420] Anlass eines Strafbedürfnisses sein.

Ob dem Überzeugungstäter eine Sonderstellung gegenüber sonstigen Tätern eingeräumt werden sollte, ist strittig. Ursprünglich sah das StGB in § 20 StGB a.F.[421] eine Regelung vor, die auch für den Überzeugungstäter eine gewisse Privilegierung enthielt.[422] Nach § 20 StGB a.F. durfte, wenn das Gesetz die Wahl zwischen Zuchthaus und Einschließung gestattete, auf Zuchthaus nur erkannt werden, wenn die strafbare Handlung einer ehrlosen Gesinnung entsprungen war. Eine solche im Einzelfall mögliche Privilegierung des Überzeugungstäters per Gesetz ist dem heute geltenden deutschen Strafrecht jedoch fremd. Die Überzeugungstat kann nur noch bei der Strafzumessung berücksichtigt werden. Nach § 46 Abs. 1 Satz 1 StGB ist die Schuld jedes Täters die Grundlage für die Strafzumessung. Ist bei einem Überzeugungstäter die Schuld im Einzelfall vermindert, fließt dieser Umstand in die Strafzumessung mit ein.

---

417 *Radbruch*, ZStW 44 (1924), 34, 34 f.; siehe auch § 71 Entwurf eines Allgemeinen Deutschen Strafgesetzbuches von 1922.

418 *Lang-Hinrichsen*, JZ 1966, 153.

419 *Fischer*, StGB, § 17, Rn. 3a.

420 Art. 1 Rahmenbeschluss 2002/475/JI des Rates vom 22.6.2002 zur Terrorismusbekämpfung, ABl. EG 2002, Nr. L 164, S. 3 ff.; vgl. auch *Zöller*, JZ 2007, 763, 764.

421 § 20 in der Fassung durch das Dritte Strafrechtsänderungsgesetz vom 4.8.1953, BGBl. I 1953, S. 735, 737, aufgehoben durch das Achte Strafrechtsänderungsgesetz vom 25.6.1968, BGBl. I 1968, S. 741, 747.

§ 20 StGB a.F. lautete: „Wo das Gesetz die Wahl zwischen Zuchthaus und Einschließung gestattet, darf auf Zuchthaus nur dann erkannt werden, wenn festgestellt wird, dass die strafbare Handlung einer ehrlosen Gesinnung entsprungen ist."

422 *Schünemann*, GA 1986, 293, 305.

Die Rechtsprechung der Strafgerichte lehnte zunächst eine solche Strafmilderung bei Gewissenstätern häufig ab. Sie verwies auf die mit der Überzeugung einhergehende besondere und trotz Bestrafung fortdauernde Gefährlichkeit des Täters und begründete daraus sogar eine erhebliche Strafschärfung.[423] Gegen diese Sichtweise sprach sich allerdings das BVerfG aus, das aus Art. 4 GG gegenüber Gewissenstätern ein „Wohlwollensgebot" herleitete.[424] Art. 4 Abs. 1 GG schützt u.a. die Freiheit des Glaubens und des Gewissens. Diese Freiheiten, insbesondere die des Gewissens, gelten jedoch nicht völlig unbeschränkt, sondern finden ihre Grenzen in den entgegenstehenden Verfassungsrechten, etwa den Grundrechten Dritter oder den Belangen der Allgemeinheit mit Verfassungsrang.[425] Beispielsweise schützt die Gewissensfreiheit nach Art. 4 Abs. 1 GG den Grundrechtsträger bei einem im Internet verbreiteten Aufruf an alle Soldaten, ihre Waffen in Zeiten von Einsätzen in Afghanistan oder im ehemaligen Jugoslawien niederzulegen und die Kasernen zu verlassen (öffentliche Aufforderung zur Straftat der Fahnenflucht, § 111 Abs. 1 StGB i.V.m. § 16 Abs. 1 WStG[426]). Indes besteht dieser Schutz nur, soweit durch die Stellungnahme nicht über Gebühr in das Interesse der Allgemeinheit an einem Funktionieren der Landesverteidigung eingegriffen wird.[427] Kann sich der Täter auf die Gewissensfreiheit stützen, so hat die Grundrechtsausübung im Einzelfall entschuldigenden oder strafmildernden Einfluss bei der Strafzumessung.[428]

Soweit dem Überzeugungstäter spezifische Normen am ausländischen Handlungsort (Rechtfertigungs-, Entschuldigungs- und Schuldausschließungsgründe, verfassungsmäßige Rechte) zugute kämen, gelten diese im deutschen Strafprozess nicht unmittelbar. Ist das deutsche Strafrecht auf einen bestimmten Fall anwendbar, ist damit gleichzeitig die Entscheidung für die deutsche Rechtsordnung als allein maßgebliche verbunden. Der Import einzelner ausländischer Vorschriften in die in sich ausgewogene, homogene deutsche Rechtsordnung würde zu deren Destabilisierung und mittelbar zu einer einzelfallabhängigen internationalisierten Rechtsordnung führen. Eine grundlegende Berücksichtigung der ausländischen Vorschriften ist bereits dadurch gewährleistet, dass diese im Rahmen der völkerrechtlichen Abwägung, ob die deutsche Rechtsordnung zur Anwendung kommt, einbezogen werden. Ausländische Normen sind jedoch im jeweiligen Einzelfall bei der Strafzumessung zu berücksichtigen. Mittels dieser Normen können die Motive des Täters sowie die Begleitumstände der Tat beleuchtet und bewertet werden und so-

---

423 BGHSt 8, 162, 164 f.

424 BVerfGE 23, 127, 134.

425 *Jarass*, in: Jarass/Pieroth, GG, Art. 4, Rn. 27 f.

426 Wehrstrafgesetz in der Fassung vom 24.5.1974, BGBl I 1974, S. 1213 ff., zuletzt geändert durch Artikel 15 des Gesetzes vom 22.4.2005, BGBl. I 2005, S. 1106 ff.

427 Siehe zum Spannungsfeld von Gewissensfreiheit und soldatischer Pflicht zuletzt Urteil des BVerwG NJW 2006, 77.

428 OLG Düsseldorf NStZ-RR 1996, 90, 91; *Fischer*, StGB, § 46, Rn. 28; *Schünemann*, GA 1986, 293, 306 ff.; S/S-*Stree/Kinzig*, § 46, Rn. 15.

mit eine hinreichende, einzelfallgerechte Einschätzung der Schwere der Tat bei der Strafzumessung erfolgen.

(3) Tatbestandsausschluss nach Art. 296 EGStGB

Während die vorgenannten Einschränkungsmöglichkeiten der Strafbarkeit des Täters keine spezifischen tatbestandlichen Begrenzungen seiner Strafbarkeit darstellen, enthält Art. 296 EGStGB für Straftaten i.S.d. § 86 Abs. 1 StGB einen speziellen Tatbestandsausschluss.[429] Nach Art. 296 EGStGB ist eine Person, die Propagandamittel verfassungswidriger Organisationen verbreitet, nicht nach § 86 Abs. 1 StGB zu bestrafen, wenn die Schrift im Ausland in ständiger, regelmäßiger Folge erscheint und dort allgemein und öffentlich vertrieben wird. Art. 296 EGStGB bezieht sich unmittelbar zwar nur auf in Druckform vertriebene Zeitungen und Zeitschriften, nach § 86 Abs. 2, § 11 Abs. 3 StGB sind unter einer Schrift i.S.d. § 86 Abs. 1 StGB aber auch Veröffentlichungen im Internet zu verstehen.[430] Voraussetzung hierfür ist nur, dass die im Internet verfügbaren Ausgaben redaktionell aufbereitet sind und in dieser Form periodisch erscheinen. Auch elektronische Abbilder von in Druckform erschienenen Zeitungen oder Zeitschriften, die mit deren Erscheinen fortgeschrieben werden, fallen in den Geltungsbereich des Art. 296 EGStGB.

Die Schrift erscheint an jedem Ort, an dem diese mit dem Willen des Verfügungsberechtigten den Bereich der vorbereitenden Handlungen zum Zwecke der Verbreitung an einen größeren Personenkreis verlässt.[431] Hierzu gehört auch der Ort, an dem die fertige Information durch Aufgabe in das Transportmedium aus dem Einflussbereich des Verfassers an einen größeren unkontrollierbaren Personenkreis gelangt.[432] Dies bedeutet für eine Verbreitung im Internet, dass Erscheinungsort bereits der Ort ist, an dem der Täter den Inhalt festlegt und auf den die Verbreitung durchführenden Server versendet. Die sich aufdrängenden Möglichkeiten, zur Umgehung der Strafbarkeit den Erscheinungsort gezielt zu verlegen, sind durch die Definition des Erscheinungsorts hinreichend eingegrenzt. Selbst wenn der geistige Urheber den inländischen Erscheinungsort durch die gezielte Nutzung eines ausländischen Servers und die Einschaltung eines Mittäters im Ausland, der die Informationen verfasst, vermeidet, dürfte sich der allgemeine und öffentliche Vertrieb am gewollten Erscheinungsort nur schwer nachweisen lassen. Eine hinreichende Stellung im ausländischen Markt ergibt sich nur, wenn eine allgemeine

---

[429] LK-StGB[12]-*Laufhütte/Kuschel*, § 86, Rn. 41; S/S-*Sternberg-Lieben*, § 86, Rn. 20; SK-StGB-*Rudolphi*, § 86, Rn. 18.

[430] *Jofer*, Strafverfolgung im Internet, S. 113.

[431] RGSt 40, 354, 359; 64, 292, 292 f.; BGHSt 13, 257, 258; *Meyer-Goßner*, StPO[50], § 7, Rn. 9; anders nunmehr aber *Meyer-Goßner*, StPO[55], § 7, Rn. 9, der jetzt auf die Geschäftsniederlassung des Verlegers bzw. des verantwortlichen Redakteurs abstellt.

[432] RGSt 64, 292, 293.

Wahrnehmbarkeit am Erscheinungsort festgestellt wird.[433] Problematisch ist eine solche Feststellung insbesondere bei einem Vertrieb über das Internet, da ein solcher regelmäßig auf eine weltweite Verbreitung ausgelegt und nicht begrenzt auf einen oder mehrere bestimmte Staaten ist. Bereits die Tatsache einer in deutscher Sprache verbreiteten Schrift ist ein starkes Indiz für einen auch auf Deutschland abzielenden Vertrieb. Zudem stellt eine Übersetzung einer in ausländischer Sprache verfassten Schrift durch eine in Deutschland vertriebene Schrift wiederum nicht mehr die im Ausland erscheinende Schrift dar. Wählt der Täter das deutschsprachige Ausland, ist zu prüfen, ob gerade in diesem Staat die Zeitschrift allgemein und öffentlich vertrieben wird. Art. 296 EGStGB soll also lediglich das Informationsrecht des Einzelnen durch den Bezug allgemein erhältlicher, ausländischer periodischer Zeitschriften wahren. Nicht geschützt sind demgegenüber eigens zum Zweck des Vertriebs in Deutschland hergestellte Propagandamittel.[434] Fehlt es an der Identität,[435] ist Art. 296 EGStGB unanwendbar.

Eine weitergehende analoge Anwendung des Art. 296 EGStGB über Straftaten i.S.d. § 86 Abs. 1 StGB unter Verwendung des Internet hinaus ist wegen des insoweit begrenzten Wortlauts des Art. 296 EGStGB und des Ausnahmecharakters der Vorschrift nicht möglich.[436] Die Begrenzung der Strafbarkeit von Tätern durch Art. 296 EGStGB wirkt sich folglich kaum aus.

bb) Strafprozessuale Einschränkungen des Legalitätsprinzips

Neben den eingangs dargestellten materiell-rechtlichen Ausschlussmöglichkeiten der Strafbarkeit ist auch die Strafverfolgung des Täters im Einzelfall durch prozessuale Einschränkungen des Legalitätsprinzips begrenzt. So kann die Staatsanwaltschaft abseits der allgemeinen Einstellungsmöglichkeiten nach den §§ 153, 153a StPO unter den durch § 153c StPO bestimmten Voraussetzungen bei reinen Auslandsstraftaten und bei Inlandsstraftaten mit einem ausländischen Handlungsort von Strafe absehen.[437] Die Einstellung kann bereits in einem frühen Stadium der Strafverfolgung stattfinden; die Ermittlungen brauchen weder zum Abschluss gekommen noch überhaupt durchgeführt worden zu sein.[438]

---

433 Siehe LK-StGB[12]-*Laufhütte/Kuschel*, § 86, Rn. 41 – für Druckschriften.

434 BT-Drucks. V/2860, S. 9; *Stegbauer*, Rechtsextremistische Propaganda im Lichte des Strafrechts, S. 75.

435 BGHSt 28, 296, 298; S/S-*Sternberg-Lieben*, § 86, Rn. 20; LK-StGB[12]-*Laufhütte/Kuschel*, § 86, Rn. 41.

436 *Jofer*, Strafverfolgung im Internet, S. 113.

437 *Werle/Jeßberger*, JuS 2001, 35, 36.

438 LR-StPO-*Beulke*, § 153c, Rn. 7; *Meyer-Goßner*, StPO[55], § 153c, Rn. 2; KMR-*Plöd*, § 153c, Rn. 4; KK-StPO-*Diemer*, § 153c, Rn. 3.

Für die Strafverfolgung von mittels des Internet begangenen Taten ist insbesondere der Anwendungsbereich des § 153c Abs. 3 StPO interessant, da dieser eine Einstellungsmöglichkeit für Distanzdelikte, also Straftaten, bei denen der Täter im Ausland handelt, ein Erfolg aber im Inland eintritt, vorsieht.[439] Grundvoraussetzung für die Einstellung nach § 153c Abs. 3 StPO ist jedoch die Anwendbarkeit des deutschen Strafrechts auf die entsprechenden Sachverhalte,[440] d.h. § 153c StPO selbst löst das Problem der Ermittlung des Anwendungsbereichs des deutschen Strafrechts nicht.

Entgegen anderer Ansicht[441] führt die Einstellungsmöglichkeit nach § 153c Abs. 3, 2. Var. StPO (sonstige überwiegende öffentliche Interessen) bei vom Ausland aus begangenen Straftaten im Internet trotz zumeist aufwändiger und wenig Erfolg versprechender Ermittlungen auch in der Praxis regelmäßig nicht weiter. An die Einstellung nach § 153c Abs. 3, 2. Var. StPO sind nämlich keine geringeren Anforderungen als an die bei der Begründung der Gefahr eines schweren Nachteils i.S.d. § 153c Abs. 3, 1. Var. StPO zu stellen. Der wahrscheinliche Eintritt eines Schadens für die äußere oder innere Sicherheit oder das Wohl der Bundesrepublik Deutschland oder eines der Bundesländer[442] ist lediglich eine wichtige Ausformung der sonstigen entgegenstehenden öffentlichen Interessen i.S.d. 2. Var. des § 153c Abs. 3 StPO.[443] Als ausdrücklich benannter Beispielsfall gibt § 153c Abs. 3, 1. Var. StPO folglich das Gewicht der in § 153c Abs. 3, 2. Var. StPO genannten sonstigen öffentlichen Belange vor.[444]

Im Unterschied zu reinen Auslandstaten sind bei Distanzdelikten notwendig inländische Rechtsgüter betroffen, sodass grundsätzlich das öffentliche Interesse an der Strafverfolgung vorliegt[445] und nur ausnahmsweise andere Interessen gegenüber diesem obsiegen können.[446] Es sind kaum Konstellationen denkbar, in denen sonstige überwiegende öffentliche Interessen das bestehende öffentliche Interesse an der Strafverfolgung verdrängen.[447] Interessen der Justizökonomie reichen hierfür allein nicht aus.[448] Die Möglichkeit der Einstellung nach § 153c Abs. 3 StPO

---

439 *Bock*, GA 2010, 589, 591; *Meyer-Goßner*, StPO[55], § 153c, Rn. 13; *Pfeiffer*, StPO, § 153c, Rn. 5.

440 LR-StPO-*Beulke*, § 153c, Rn. 3.

441 *Jofer*, Strafverfolgung im Internet, S. 118.

442 LR-StPO-*Beulke*, § 153c, Rn. 27 mit Verweis auf § 153d, Rn. 7 ff.; *Meyer-Goßner*, StPO[55], § 153c, Rn. 14.

443 LR-StPO-*Beulke*, § 153c, Rn. 27 mit Verweis auf § 153d, Rn. 7 ff.; *Meyer-Goßner*, StPO[55], § 153c, Rn. 15.

444 LR-StPO-*Beulke*, § 153c, Rn. 27 mit Verweis auf § 153d, Rn. 7 ff.

445 KK-StPO-*Diemer*, § 153c, Rn. 14.

446 LR-StPO-*Beulke*, § 153c, Rn. 27 mit Verweis auf § 153d, Rn. 7 ff.

447 *Breuer*, MMR 1998, 141, 143; *Hilgendorf*, NJW 1997, 1873, 1874; *Kienle*, Internationales Strafrecht und Straftaten im Internet, S. 116; *Vec*, NJW 2002, 1535, 1536.

448 *Koch*, JuS 2002, 123, 124.

bietet daher für die Verfolgung von Straftaten, die mittels des Internet begangen werden, keine wesentlichen Einschränkungen des Legalitätsprinzips zugunsten des Opportunitätsprinzips.

5. Ergebnis

Deutsche Strafverfolgungsbehörden sind für die Aufnahme von Ermittlungen bei im Internet begangenen Straftaten nach dem Territorialitätsprinzip zuständig, wenn der Täter in Deutschland körperlich handelte oder einen tatbestandlichen Erfolg in Deutschland herbeiführte. Der Täter handelt grundsätzlich nur an seinem physischen Aufenthaltsort. Einen Erfolg i.S.d. §§ 9 Abs. 1, 3. Var., 3 StGB führt er herbei, wenn tatbestandsmäßige Verletzungen oder konkrete Gefährdungen in Deutschland eintreten. Einer über diese Auslegungsergebnisse hinausgehenden weiteren Beschränkung der Anwendbarkeit deutschen Strafrechts bedarf es aus völkerrechtlicher Sicht nicht. Die – wenn auch sehr eingeschränkten – Möglichkeiten, welche das Strafrecht und das Strafprozessrecht zur Begrenzung der Strafbarkeit im Übrigen bieten, genügen. Eine weitergehende Beschränkung des deutschen Strafrechts[449] kann richtigerweise nur auf rechtspolitische Erwägungen gestützt werden und bedarf neuer gesetzlicher Regelungen. Allein mit einer restriktiveren Auslegung sind gesetzeskonform keine zusätzlichen Einschränkungen umsetzbar.

Ob in der Praxis bei der strafrechtlichen Beurteilung von Taten im Internet, die zu mehreren Staaten einen Anknüpfungspunkt aufweisen, in Zukunft politische Konfliktfälle größeren Ausmaßes auftreten werden, die eine Einschränkung der Strafanwendungsregeln erforderlich machen, bleibt abzuwarten.[450] Im Ergebnis ist es sicherlich wünschens- und empfehlenswert, durch international abgestimmte Regelungen den Schwierigkeiten bei der Bestimmung der Anwendbarkeit nationalen Rechts auf im Ausland begangene Sachverhalte, die sich insbesondere bei der Internetkriminalität ergeben, zu begegnen.[451] In naher Zukunft besteht jedoch kaum begründeter Anlass zu der Hoffnung, dass sich die Mehrheit der Staaten auf internationaler Ebene auf gemeinsame Standards für die Zuständigkeit zur Verfolgung von Straftaten im Internet einigt. Zu unterschiedlich sind bereits die Auffassungen zur Strafwürdigkeit einzelner Verhaltensweisen. Mit einem ausschließlich an internationales Recht angelehnten „nationalen“ Strafrecht wäre außerdem eine weitgehende Rücknahme des teilweise auf geschichtlichen Entwicklungen eines jeden

---

[449] Siehe dazu die im Einzelnen aufgeführten Vorschläge im Rahmen der Darstellung des Meinungsstands in Literatur und Rechtsprechung unter Teil 2, II.C.3.a)–f).

[450] Solche Konfliktsituationen zeichneten sich etwa im Fall CompuServe ab. Im Urteil des AG München CR 1998, 500 ff. gegen *Felix Somm*, damaliger Geschäftsführer des Onlinedienstes CompuServe Deutschland, wurde dem Angeklagten mittelbar auch die Verbreitung von pornografischem Material über Newsgroups vorgeworfen.

[451] *Sieber*, COMCRIME-Study, S. 132 f.; United Nations, Manual on the prevention and control of computer-related crime, Tz. 260.

Strafrechts beruhenden nationalen Rechtsgüterschutzes verbunden. Selbst die – über den Geltungsbereich der Europäischen Union hinausgehende – Convention on Cybercrime des Europarats, die neben materiellen Strafvorschriften auch Regelungen für die Strafverfolgung enthält, hilft dem Problem der Jurisdiktionskonflikte nur bedingt ab, weil sie neben der schlichten Anknüpfung insbesondere an das Territorialitäts- und Personalitätsprinzip keine Instrumente zur Auflösung des bei mehreren Anknüpfungspunkten entstehenden Konfliktpotentials vorsieht, sondern lediglich eine freiwillige Konsultation der betroffenen Staaten befürwortet (Art. 22 Abs. 5 CCC).

III. Inlandstaten von im EU-Ausland niedergelassenen Diensteanbietern

Für nach deutschem Recht strafbewehrte Angebote von Diensteanbietern aus dem EU-Ausland setzt das Gemeinschaftsrecht mit dem sogenannten Herkunftslandprinzip nach Art. 3 Abs. 2 ECRL[452] den Mitgliedstaaten und ihren Strafverfolgungsbehörden auf dem Gebiet des Straf- und Strafverfahrensrechts Schranken.[453]

Nach dem in § 3 Abs. 2 Satz 1 TMG durch den deutschen Gesetzgeber umgesetzten Herkunftslandprinzip darf der freie Dienstleistungsverkehr von Telemedien nicht eingeschränkt werden, wenn entsprechende Dienste in der Bundesrepublik Deutschland von Diensteanbietern mit Sitz in einem Staat innerhalb des Geltungsbereichs der Richtlinie 2000/31/EG geschäftsmäßig angeboten oder erbracht werden. Mit der pauschalen Anwendung deutscher Strafnormen auf diese Sachverhalte wäre also eine Beschränkung des Dienstleistungsverkehrs verbunden, dessen Freiheit die Richtlinie jedoch gerade gewährleisten will. In der Strafrechtswissenschaft hat das Prinzip bisher aber nur wenig Beachtung gefunden, da bereits unklar ist, ob es auch für den Bereich des Strafrechts gilt. Seine Anwendbarkeit vorausgesetzt, ist darüber hinaus ungeklärt, ob das Prinzip die Normen des Strafanwendungsrechts überlagert oder aber zusätzlich nach nationalem Recht die Anwendbarkeit des deutschen Strafrechts zu prüfen bleibt.

---

[452] Art. 3 Abs. 2 ECRL lautet: „Die Mitgliedstaaten dürfen den freien Verkehr von Diensten der Informationsgesellschaft aus einem anderen Mitgliedstaat nicht aus Gründen einschränken, die in den koordinierten Bereich fallen."

[453] Für Inlandstaten mit Bezug zum EU-Ausland, die bereits aufgrund der richtlinienimmanenten Einschränkung nicht dem Herkunftslandprinzip unterfallen, gelten allerdings die unter Teil 2, II. gemachten Ausführungen.

A. Geltung des Herkunftslandprinzips im Strafrecht

Die Frage nach der Geltung des Herkunftslandprinzips im Strafrecht kann nur mittels einer Zusammenschau der primär- und sekundärrechtlichen Vorgaben des Gemeinschaftsrechts beantwortet werden (nachfolgend unter 1. und 2.). Diese europarechtlichen Vorgaben bilden den Hintergrund für das Herkunftslandprinzip der E-Commerce-Richtlinie, das der deutsche Gesetzgeber mit § 3 TMG (vormals § 4 TDG, § 5 Abs. 5 MDStV) umsetzte (unter 3.).

1. Herkunftslandprinzip im primären Gemeinschaftsrecht

Ein ausdrückliches, allgemeines, übergreifendes Herkunftslandprinzip in dem Sinne, dass Waren und Dienstleistungen, die den rechtlichen Anforderungen des Herkunftsstaates genügen, auch im Gemeinsamen Markt unabhängig von etwaigen entgegenstehenden Regelungen der Aufnahmestaaten abgesetzt werden dürfen, enthält der Vertrag über die Arbeitsweise der Europäischen Union (AEUV)[454] nicht.[455] Nach Art. 3 Abs. 1 lit. b) AEUV ist es allerdings u.a. Aufgabe der Europäischen Union, das Funktionieren des Binnenmarktes durch den Erlass von Wettbewerbsregeln zu sichern. Zur Erfüllung dieser Aufgabe trifft die Union u.a. gemäß Art. 26 Abs. 1 und 2 AEUV die erforderlichen Maßnahmen, um einen gemeinsamen Binnenmarkt, also einen Raum ohne Binnengrenzen, in dem der freie Verkehr von Waren, Personen, Dienstleistungen und Kapital gewährleistet wird, zu verwirklichen. Der Realisierung dieser Zielstellung dient u.a. das grundsätzliche Verbot der Begrenzung des freien Warenverkehrs nach Art. 34 und 35 AEUV durch mengenmäßige Ein- und Ausfuhrbeschränkungen oder Maßnahmen gleicher Wirkung. Zulässig sind solche Beschränkungen nur, wenn sie u.a. aus Gründen der öffentlichen Sicherheit und Ordnung gerechtfertigt sind (Art. 36 Satz 1 AEUV). Korrespondierend zum Warenverkehr sind Beschränkungen des freien Dienstleistungsverkehrs[456] innerhalb der Union für Angehörige der Mitgliedstaaten, die in einem anderen Staat der Union als dem des Leistungsempfängers ansässig sind, ebenfalls grundsätzlich verboten (Art. 56 Abs. 1 AEUV). Prinzipiell darf also kein Angehöriger eines Mitgliedstaates, der seine Leistungen am Niederlassungssitz rechtmäßig erbringt, durch einen anderen Mitgliedstaat, in welchem er seine Leistung ebenfalls anbieten will, weiteren Beschränkungen unterworfen werden.

---

[454] Früher Vertrag zur Gründung der Europäischen Gemeinschaft; umbenannt gemäß Art. 2 des Vertrages von Lissabon vom 13.12.2007 (ABl. EU 2007, Nr. C 306, S. 42 ff.).

[455] EuGH, Urteil vom 13.3.1997, *Bundesrepublik Deutschland ./. Europäisches Parlament und Rat der Europäischen Union*, Rs. C-233/94, Slg. 1997, S. I-02405 ff., Rn. 64; *Ruess*, Die E-Commerce-Richtlinie und das deutsche Wettbewerbsrecht, S. 63.

[456] Zu Beispielen für die Einordnung als Dienstleistung oder aber als Ware siehe *Frenz*, Handbuch Europarecht, Bd. 1, Rn. 2474 ff., 2536.

In den vorgenannten Art. 34, 35, 56 AEUV klingt demzufolge bereits an, dass Angehörige in Mitgliedstaaten der Europäischen Union nicht durch Regelungen anderer Mitgliedstaaten im Bereich des Verkehrs von Waren und Dienstleistungen behindert werden dürfen. Der Rechtsprechung des EuGH zu diesen Grundfreiheiten[457] wird daher nicht selten zumindest auch ein eingeschränktes Herkunftslandprinzip[458] oder Prinzip der gegenseitigen Anerkennung[459] entnommen.[460]

Die ersten Entscheidungen zur Verwirklichung eines Binnenmarktes traf der EuGH zur Warenverkehrsfreiheit. Im sogenannten „Dassonville"-Urteil entschied er, dass „jede Handelsregelung der Mitgliedstaaten, die geeignet ist, den innergemeinschaftlichen Handel unmittelbar oder mittelbar, tatsächlich oder potentiell zu behindern, […] als Maßnahme mit gleicher Wirkung wie eine mengenmäßige Beschränkung anzusehen"[461] sei. Ein Mitgliedstaat könne nur im Fall fehlender Gemeinschaftsregelungen Maßnahmen ergreifen, um unlautere Verhaltensweisen zu unterbinden. Die Maßnahmen müssten dann jedoch sinnvoll sein und ggf. geforderte Nachweise dürften keine Behinderung des Handels zwischen den Mitgliedstaaten bewirken.[462] Fünf Jahre darauf entschied der EuGH im sogenannten „Cassis de Dijon"-Urteil, dass „es Sache der Mitgliedstaaten [sei], alle die Herstellung und Vermarktung […] betreffenden Vorschriften für ihr Hoheitsgebiet zu erlassen. Hemmnisse für den Binnenhandel der Gemeinschaft, die sich aus den Unterschieden der nationalen Regelungen […] ergeben, müssen hingenommen werden, soweit diese Bestimmungen notwendig sind, um zwingenden Erfordernissen gerecht zu werden".[463] Im sogenannten „Keck"-Urteil nahm der Gerichtshof 1993 eine weitere Präzisierung vor:

> „Entgegen der bisherigen Rechtsprechung [ist] die Anwendung nationaler Bestimmungen, die bestimmte Verkaufsmodalitäten beschränken oder verbieten, auf Erzeugnisse aus anderen Mitgliedstaaten nicht geeignet, den Handel zwischen den Mitgliedstaaten im Sinne des Urteils Dassonville […] zu behindern, sofern diese Bestimmungen für alle betroffenen Wirtschaftsteilnehmer gelten, die ihre Tätigkeit im Inland ausüben, und so-

---

457 Siehe auch die Mitteilung der Kommission vom 3.10.1980 aus Anlass der „Cassis de Dijon"-Entscheidung des EuGH, ABl. EG 1980, Nr. C 256, S. 2.

458 *Frenz*, Handbuch Europarecht, Bd. 1, Rn. 2690; *Haratsch/Koenig/Pechstein*, Europarecht, Rn. 834; *Ruess*, Die E-Commerce-Richtlinie und das deutsche Wettbewerbsrecht, S. 75.

459 *Leible*, in: Grabitz/Hilf, Bd. I, Art. 28 EGV, Rn. 26.

460 Für ein Herkunftslandprinzip ohne Nennung von Einschränkungen: *Bröhl*, MMR 2001, 67, 69; *Bullinger/Mestmäcker*, Multimediadienste, S. 102; *Müller-Graf*, in: von der Groeben/Schwarze, EGV, Art. 28 EG, Rn. 190 f.; *Tettenborn*, K&R 1999, 252, 256; *Tettenborn* et al., Beilage Nr. 10 zu BB 2001, 1, 9.

461 EuGH, Urteil vom 11.7.1974, *Staatsanwaltschaft ./. Benoit und Gustave Dassonville*, Rs. 8-74, Slg. 1974, S. 00837 ff., Rn. 5.

462 Ebenda, Rn. 6.

463 EuGH, Urteil vom 20.2.1979, *Rewe-Zentral AG ./. Bundesmonopolverwaltung für Branntwein*, Rs. 120-78, Slg. 1979, S. 00649 ff., Rn. 8.

fern sie den Absatz der inländischen Erzeugnisse und der aus anderen Mitgliedstaaten rechtlich wie tatsächlich in der gleichen Weise berühren."[464]

Für die mit der Warenverkehrsfreiheit verwandte Dienstleistungsfreiheit stellte der EuGH im sogenannten „Säger"-Urteil ähnliche Vorgaben auf, indem er entschied, dass „eine nationale Regelung, die die Ausübung bestimmter Dienstleistungen durch ein in einem anderen Mitgliedstaat niedergelassenes Unternehmen im Inland von der Erteilung einer behördlichen Erlaubnis abhängig macht, […] eine Beschränkung der Dienstleistungsfreiheit im Sinne von Artikel 59 EWG-Vertrag [a.F.]" darstelle.[465] Der freie Dienstleistungsverkehr dürfe „nur durch Regelungen beschränkt werden, die durch zwingende Gründe des Allgemeininteresses gerechtfertigt sind und die für alle im Hoheitsgebiet des Bestimmungsstaates tätigen Personen oder Unternehmen gelten, und zwar nur soweit, als dem Allgemeininteresse nicht bereits durch die Rechtsvorschriften Rechnung getragen ist, denen der Leistungserbringer in dem Staat unterliegt, in dem er ansässig ist".[466] In der 1995 folgenden sogenannten „Alpine Investments"-Entscheidung stellte der Gerichtshof sodann eine Verbindung zu den in der „Keck"-Entscheidung zur Warenverkehrsfreiheit herausgearbeiteten Grundsätzen für die Dienstleistungsfreiheit her.[467] Beschränkungen der Dienstleistungsfreiheit sind danach verboten, wenn sie den Zutritt der Dienstleistung zu den Märkten anderer Mitgliedstaaten behindern.[468]

Zusammenfassend ist den vorgenannten Urteilen des EuGH zur Waren- und Dienstleistungsfreiheit zu entnehmen, dass der Aufnahmestaat einer Ware oder Dienstleistung aus dem EU-Ausland die Regelungen des Herkunftsstaates respektieren muss, wenn die Ware oder Dienstleistung nach dessen Vorschriften rechtmäßig angeboten oder erbracht wird. Mit der Mitgliedschaft in der Europäischen Union ordnet der jeweilige Mitgliedstaat seine nationalen Interessen bestimmten gemeinschaftlichen Interessen unter. Sein Eingriffsinteresse ist daher i.d.R. schwächer als das Abwehrinteresse des Staates, aus dem der Anbieter kommt. In der Abwägung der entgegenstehenden Interessen von Aufnahme- und Herkunftsstaat ob-

---

[464] EuGH, Urteil vom 24.11.1993, *Strafverfahren gegen Bernard Keck und Daniel Mithouard*, Rs. C-267/91 und C-268/91 Slg. 1993, S. I-06097 ff., Rn. 16.

[465] EuGH, Urteil vom 25.7.1991, *Manfred Säger ./. Dennemeyer & Co Ltd*., Rs. C-76/90, Slg. 1991, S. I-04221 ff., Rn. 14; siehe auch *ders.*, Urteil vom 25.7.1991, *Stichting Collectieve Antennevoorziening Gouda und andere ./. Commissariaat voor de Media*, Rs. C-288/89, Slg. 1991, S. I-4007 ff., Rn. 1, 12.

[466] EuGH, Urteil vom 25.7.1991, *Manfred Säger ./. Dennemeyer & Co Ltd*., Rs. C-76/90, Slg. 1991, S. I-04221 ff., Rn. 15; siehe auch *ders.*, Urteil vom 25.7.1991, *Stichting Collectieve Antennevoorziening Gouda u.a. ./. Commissariaat voor de Media*, Rs. C-288/89, Slg. 1991, S. I-4007 ff., Rn. 13 ff.

[467] EuGH, Urteil vom 10.5.1995, *Alpine Investments BV ./. Minister van Financien*, Rs. C-384/93, Slg. 1995, S. I-01141 ff., Rn. 36 ff.; *Frenz*, Handbuch Europarecht, Bd. 1, Rn. 2559 f.; kritisch hierzu *Tiedje/Troberg*, in: von der Groeben/Schwarze, EGV, Art. 49 EG, Rn. 103 ff.

[468] EuGH, Urteil vom 10.5.1995, *Alpine Investments BV ./. Minister van Financien*, Rs. C-384/93, Slg. 1995, S. I-01141 ff., Rn. 38.

siegt folglich zumeist das durch das Binnenmarktprinzip aufgewertete Interesse des Herkunftsstaates der Ware oder Dienstleitung. Nur wenn dem Aufnahmestaat zwingende Gründe des Allgemeininteresses zur Seite stehen, ist sein Eingriffsinteresse höher zu bewerten als das Abwehrinteresse des Herkunftsstaates.[469]

Liegen zwingende Gründe des Allgemeininteresses vor, steht die Ausgestaltung der Beschränkungen im Ermessen des Aufnahmestaates. Sein Ermessen ist allerdings nicht grenzenlos, sondern beschränkt durch die gemeinschaftsrechtlichen Grundsätze, die für alle Mitgliedstaaten gleichermaßen gelten.[470] Einige dieser Grundsätze[471] enthält u.a. die Konvention zum Schutze der Menschenrechte und Grundfreiheiten (EMRK);[472] so sind z.B. nach Art. 8–11 EMRK Beschränkungen von Freiheiten nur zulässig, soweit sie für den Schutz in einer demokratischen Gesellschaft notwendig sind. Zwar gilt die EMRK als völkerrechtlicher Vertrag der Mitgliedstaaten des Europarats im Europäischen Gemeinschaftsrecht nicht unmittelbar. Die Europäische Union, deren Mitglieder als Angehörige des Europarats alle der EMRK beigetreten sind, verpflichtete sich aber in Art. 6 Abs. 2 des Vertrages über die Europäische Union[473] (EUV) zur Achtung der Grundrechte der EMRK, sodass die Grundsätze der EMRK mittelbar und als allen Mitgliedstaaten gemeinsames Mindestschutzniveau zu berücksichtigen sind.

2. Herkunftslandprinzip im sekundären Gemeinschaftsrecht

Das sekundäre Gemeinschaftsrecht dient ebenfalls der Verwirklichung des Gemeinsamen Marktes. Hierzu beschreitet die Europäische Union im Wesentlichen zwei Wege, den der Harmonisierung (oder auch Angleichung) und den der gegenseitigen Anerkennung. Bei der Harmonisierung bestimmt der Rechtsaktegeber für das Recht der Mitgliedstaaten einen gemeinsamen Standard, den die Mitgliedstaaten frei in der Wahl von Form und Mitteln, aber nicht in der Sache, umsetzen müs-

---

[469] EuGH, Urteil vom 25.7.1991, *Manfred Säger ./. Dennemeyer & Co Ltd*., Rs. C-76/90, Slg. 1991, S. I-04221 ff., Rn. 15; *ders.*, Urteil vom 25.7.1991, *Stichting Collectieve Antennevoorziening Gouda und andere ./. Commissariaat voor de Media*, Rs. C-288/89, Slg. 1991, S. I-4007 ff., Rn. 13 ff.

[470] EuGH, Urteil vom 28.10.1975, *Roland Rutili ./. Minister des Innern*, Rs. 36-75, Slg. 1975, S. 1219 ff., Rn. 26/28; *Bullinger/Mestmäcker*, Multimediadienste, S. 99.

[471] EuGH, Urteil vom 28.10.1975, *Roland Rutili ./. Minister des Innern*, Rs. 36-75, Slg. 1975, S. 1219 ff., Rn. 32.

[472] Konvention zum Schutze der Menschenrechte und Grundfreiheiten vom 4.11.1950 in der Neufassung vom 17.5.2002, BGBl. II 2002, S. 1055 ff., zuletzt geändert durch Gesetz zu dem Protokoll Nr. 14 vom 13.5.2004 zur Konvention zum Schutz der Menschenrechte und Grundfreiheiten über die Änderung des Kontrollsystems der Konvention (BGBl. II 2006, S. 136 ff.).

[473] Vertrag über die Europäische Union vom 7.2.1992 (ABl. EG 1992, Nr. C 191, S. 1 ff.) zuletzt geändert durch Art. 12 EU-Beitrittsakte 2003 vom 16.4.2003 (ABl. EU 2003, Nr. L 236, S. 33 ff.).

sen.[474] Er definiert damit das Eingriffsinteresse der Mitgliedstaaten auf einheitlichem Niveau. Anders geht der Rechtsaktegeber bei der Verpflichtung zur gegenseitigen Anerkennung des jeweils anderen nationalen Rechts durch die Mitgliedstaaten vor. Die Staaten werden in diesem Fall verpflichtet, ihr nationales Recht auf bestimmte Sachverhalte nicht mehr anzuwenden.[475] Im Vordergrund der Regelung steht folglich das durch das Sekundärrecht gesteigerte Abwehrinteresse des Herkunftsstaates. Der Bereich, in dem entweder eine Harmonisierung oder eine Anerkennung erfolgt, wird als koordinierter Bereich bezeichnet und zumeist in dem betreffenden Rechtsakt legal definiert.[476]

Das Herkunftslandprinzip der E-Commerce-Richtlinie ist, wie bereits anhand der Rechtsprechung des EuGH zur Waren- und Dienstleistungsfreiheit dargestellt, kein völlig neuartiges Konzept. In Richtlinienform gegossen, knüpft es an das in Art. 2 geregelte Sendelandprinzip der Fernsehrichtlinie 1997[477] an. Anders als das Sendelandprinzip der Fernsehrichtlinie 1997, in der gleichzeitig ein Mindeststandard an Rechtsregeln für den koordinierten Bereich in allen Mitgliedstaaten festgelegt wurde,[478] erstreckt sich das Herkunftslandprinzip nach Art. 3 ECRL aber nicht nur auf die durch die E-Commerce-Richtlinie harmonisierten Rechtsbereiche, sondern erfasst querschnittsartig auch alle nicht harmonisierten Bereiche, die den freien Verkehr der Dienste der Informationsgesellschaft betreffen.[479]

---

[474] *Vogel*, in: Zieschang/Hilgendorf/Laubenthal, Strafrecht und Kriminalität in Europa, S. 29, 34.

[475] *Frenz*, Handbuch Europarecht, Bd. 1, § 5, Rn. 170.

[476] Siehe etwa Art. 2 lit. h) ECRL.

[477] Richtlinie zur Koordinierung bestimmter Rechts- und Verwaltungsvorschriften der Mitgliedstaaten über die Ausübung der Fernsehtätigkeit – Richtlinie 89/552/EWG, ABl. EG 1989, Nr. L 298, S. 23 ff.; Novellierung durch die Richtlinie 97/36/EG zur Änderung der Richtlinie 89/552/EWG, ABl. EG 1997, Nr. L 202, S. 60 ff.; Nach dem Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates zur Änderung der Richtlinie 89/522/EWG des Rates zur Koordinierung bestimmter Rechts- und Verwaltungsvorschriften der Mitgliedstaaten über die Ausübung der Fernsehtätigkeit, KOM(2005) 646 soll die Begrenzung auf einen koordinierten Bereich beibehalten werden; so auch nach dem geänderten Vorschlag vom 29.3.2007, KOM(2007) 170. Dieses Anliegen kommt nunmehr in der verabschiedeten Richtlinie 2007/65/EG des Europäischen Parlaments und des Rates vom 11.12.2007 zur Änderung der Richtlinie 89/552/EWG des Rates zur Koordinierung bestimmter Rechts- und Verwaltungsvorschriften der Mitgliedstaaten über die Ausübung der Fernsehtätigkeit zum Ausdruck.

[478] EuGH, Urteil vom 9.7.1997, *Konsumentombudsmannen ./. De Agostini (Svenska) Foerlag AB und TV-Shop i Sverige AB*, Rs. C-34/95, C-35/95 und C-36/95, Slg. 1997, S. I-03843 ff., Rn. 26 ff.; *Bodewig*, GRURInt 2000, 475, 480; *Faßbender*, AfP 2006, 505, 508.

[479] *Altenhain*, in: Zieschang/Hilgendorf/Laubenthal, Strafrecht und Kriminalität in Europa, S. 107, 119 f. (kritisch gegenüber dem Verzicht auf die Setzung eines gemeinsamen Mindeststandards); *Bodewig*, GRURInt 2000, 475, 480; *Faßbender*, AfP 2006, 505, 508; *Ohly*, GRURInt 2001, 899, 901.

3. Herkunftslandprinzip in Umsetzung der E-Commerce-Richtlinie

Mit der Umsetzung des Herkunftslandprinzips der E-Commerce-Richtlinie in das deutsche Recht durch § 3 Abs. 2 Satz 1 TMG hat der deutsche Rechtsanwender grundsätzlich die Rechtsordnungen der Staaten innerhalb des Geltungsbereichs der E-Commerce-Richtlinie zu respektieren. Ein Diensteanbieter mit Sitz in einem Staat der Europäischen Union, der geschäftsmäßig Telemedien in einem Mitgliedstaat anbietet oder erbringt, braucht nur das Recht des Staates, in dem er sich niedergelassen hat, zu beachten. Für den Diensteanbieter sind folglich u.U. strengere rechtliche Vorschriften in anderen Staaten der Europäischen Union, in denen sein Angebot abgerufen werden kann, grundsätzlich nicht relevant.

a) Gesetzlicher Anwendungsbereich

Das Herkunftslandprinzip der E-Commerce-Richtlinie hat einen umgrenzten Anwendungsbereich, da ihm nur das geschäftsmäßige Anbieten und Erbringen von Diensten der Informationsgesellschaft in einem Mitgliedstaat der Europäischen Union durch einen Diensteanbieter mit Sitz in einem der Mitgliedstaaten unterfallen.

aa) Dienste der Informationsgesellschaft

Die Dienste der Informationsgesellschaft sind Regelungsgegenstand des Herkunftslandprinzips (Art. 3 Abs. 2 ECRL). Nach der Transparenzrichtlinie in der Fassung der Richtlinie 98/48/EG,[480] die in Art. 1 Nr. 2 den Begriff „Dienste“ näher definiert, sind darunter im Fernabsatz vertriebene Dienstleistungen zu verstehen, die elektronisch und auf individuellen Abruf eines Empfängers erbracht werden, also solche, die ohne gleichzeitige Anwesenheit der Vertragsparteien zur Verfügung gestellt werden. Elektronisch wird die Dienstleistung vorgenommen, wenn sie mittels Geräten für die elektronische Verarbeitung und Speicherung von Daten am Ausgangspunkt gesendet sowie am Endpunkt empfangen wird und die Dienstleistung vollständig über Draht, über Funk, auf optischem oder anderem elektromagnetischem Wege gesendet, weitergeleitet und empfangen wird. Auf individuellem Abruf erfolgt eine Dienstleistung, wenn sie durch die Übertragung von Daten auf individuelle Anforderung erbracht wird.[481] Die Definition des Dienstes knüpft an die Rechtsprechung des EuGH zum Begriff der Dienstleistung an, den der Ge-

---

[480] Richtlinie 98/48/EG des Europäischen Parlamentes und des Rates vom 20.1.1998 zur Änderung der Richtlinie 98/34/EG über ein Informationsverfahren auf dem Gebiet der Normen und technischen Vorschriften, ABl. EG 1998, Nr. L 217, S. 18 ff.

[481] *Tettenborn* et al., Beilage Nr. 10 zu BB 2001, 1, 6.

richtshof weit auslegt.[482] Das Herkunftslandprinzip erfasst jedoch nicht nur Dienstleistungen i.S.d. Art. 57 AEUV, sondern auch den Online-Verkauf von Waren, nicht aber deren Auslieferung.[483]

Der deutsche Bundesgesetzgeber und die Landesgesetzgeber haben den Begriff „Dienste der Informationsgesellschaft" anfangs nicht übernommen, weil dieser sowohl Tele- als auch Mediendienste erfasst[484] und die Gesetzgebungskompetenz für den Bereich der Teledienste beim Bundesgesetzgeber nach Art. 73 Nr. 7 und Art. 74 Nr. 11 GG und für die Mediendienste bei den Ländern gemäß Art. 70 Abs. 1 GG lag. Mit dem Verzicht der Bundesländer auf eine Regelung zumindest der wirtschaftsbezogenen Anforderungen an Mediendienste durch einen Staatsvertrag konnte der Bundesgesetzgeber im Telemediengesetz gemäß seiner Gesetzgebungskompetenz aus Art. 73 Nr. 7, Art. 74 Abs. 1 Nr. 11 und aus Art. 72 Abs. 2 GG zur Wahrung der Wirtschaftseinheit[485] nunmehr jedoch eine einheitliche Regelung treffen. Der eingefügte, bereits aus dem Jugendmedienschutzstaatsvertrag[486] bekannte Begriff der Telemedien umfasst nach der Legaldefinition des § 1 Abs. 1 Satz 1 TMG „alle elektronischen Informations- und Kommunikationsdienste, soweit sie nicht Telekommunikationsdienste nach § 3 Nr. 24 des Telekommunikationsgesetzes, die ganz in der Übertragung von Signalen über Telekommunikationsnetze bestehen, telekommunikationsgestützte Dienste nach § 3 Nr. 25 des Telekommunikationsgesetzes oder Rundfunk nach § 2 des Rundfunkstaatsvertrages sind".[487] Diensteanbieter ist nach § 2 Satz 1 Nr. 1, 1. HS TMG „jede natürliche oder juristische Person, die eigene oder fremde Telemedien zur Nutzung bereithält oder den Zugang zur Nutzung vermittelt".

---

[482] EuGH, Urteil vom 7.12.1993, *Stephan Max Wirth ./. Landeshauptstadt Hannover*, Rs. C-109/92, Slg. 1993, S. I-06447 ff., Rn. 14 f.; *Fröhlinger*, in: Drexl et al., Europarecht im Informationszeitalter, S. 9, 16.

[483] Erwägungsgrund 18 der E-Commerce-Richtlinie, ABl. EG 2000, Nr. L 178, S. 3; *Spindler*, in: Spindler/Schmitz/Geis, TDG, § 4, Rn. 10 f.

[484] *Brisch*, CR 1999, 235, 237 f.; *Hoeren*, MMR 1999, 192, 194; *Maennel*, in: Moritz/Dreier, Rechts-Handbuch zum E-Commerce[1], Teil C, Rn. 394; siehe auch *Bullinger/Mestmäcker*, Multimediadienste, S. 88 f.; *Tettenborn*, in: Moritz/Dreier, Rechts-Handbuch zum E-Commerce[1], Teil C, Rn. 448; *Tettenborn* et al., Beilage Nr. 10 zu BB 2001, 1, 6.

[485] So die Begründung zum Entwurf des TMG, BT-Drucks. 16/3078, S. 12.

[486] Staatsvertrag über den Schutz der Menschenwürde und den Jugendschutz in Rundfunk und Telemedien (JMStV) vom 10.9.2002 (GBl. BW 2003, S. 93), zuletzt mit Wirkung zum 1.4.2010 geändert durch Artikel 2 des Dreizehnten Rundfunkänderungsstaatsvertrags vom 30.10.2009.

[487] Zum Begriff „Telemedien" *Hoeren*, NJW 2007, 801, 802 f.; *Kitz*, ZUM 2007, 368, 369.

bb) Geschäftsmäßiges Anbieten und Erbringen

Nicht jedes, sondern lediglich das geschäftsmäßige Anbieten und Erbringen von Diensten der Informationsgesellschaft bzw. von Telemedien fällt unter das Herkunftslandprinzip. Ein Diensteanbieter handelt geschäftsmäßig, wenn er seine Dienste in einer nachhaltigen Tätigkeit mit oder ohne Gewinnerzielungsabsicht erbringt.[488] Er muss lediglich auf unbestimmte Zeit eine Wirtschaftstätigkeit ausüben.[489] Eine reine Nutzer-Nutzer-Beziehung via E-Mail reicht regelmäßig nicht aus, da sie keinen Dienst, sondern eine Individualkommunikation darstellt und eine wirtschaftliche Tätigkeit vermissen lässt;[490] anderes gilt bei kommerzieller Werbung für Waren- und Dienstleistungsangebote per E-Mail.[491] Nach der Begründung zum TDG – die aufgrund der ausdrücklichen Übernahme seiner Regelung des Herkunftslandprinzips in das TMG weiter Bestand hat[492] – sollen zudem Telemedien (ursprünglich Tele- und Mediendienste) von öffentlichen Bibliotheken und Museen, nicht jedoch private Gelegenheitsgeschäfte ein geschäftsmäßiges Handeln darstellen.[493]

cc) Ort der Niederlassung des Diensteanbieters

Der Diensteanbieter kommt nur in den Genuss des Herkunftslandprinzips, wenn er seinen Sitz im Regelungsbereich der Richtlinie hat und seine Dienste auch in diesem räumlichen Bereich erbringt. Gemäß § 2 Satz 1 Nr. 2 TMG ist ein „niedergelassener Diensteanbieter jeder Anbieter, der mittels einer festen Einrichtung auf unbestimmte Zeit Telemedien geschäftsmäßig anbietet oder erbringt“. Ist das Unternehmen nur für einen bestimmten Zeitraum gegründet, stellt der Ort der tatsächlichen Ausübung der wirtschaftlichen Tätigkeit mittels fester Einrichtungen eine Niederlassung dar.[494] Ein Unternehmen, das Dienstleistungen über eine Webseite erbringt, ist am Ort seiner Wirtschaftstätigkeit niedergelassen. Der Standort der technischen Einrichtung begründet gemäß § 2 Satz 1 Nr. 2, 2. HS TMG allein keine Niederlassung des Anbieters. Weder der Standort des Servers, auf dem die Webseite gespeichert, noch der Ort, wo sie zugänglich ist, entscheidet über den Niederlas-

---

488 Zum TDG BT-Drucks. 14/6098, Vorbem. zu § 4, S. 17; *Brunner*, in: Manssen, Telekommunikations- und Multimediarecht, Bd. 2, § 4 TDG, Rn. 33; *Tettenborn* et al., Beilage Nr. 10 zu BB 2001, 1, 11.

489 *Spindler*, in: Spindler/Schmitz/Geis, TDG, § 4 TDG, Rn. 12.

490 *Tettenborn* et al., Beilage Nr. 10 zu BB 2001, 1, 6.

491 BT-Drucks. 16/3078, zu § 1 I 1, S. 14.

492 Ebenda, zu § 3, S. 14.

493 Zum TDG BT-Drucks. 14/6098, Vorbem. zu § 4, S. 17; kritisch dazu *Spindler*, in: Spindler/Schmitz/Geis, TDG, § 4 TDG, Rn. 12.

494 Erwägungsgrund 19 der E-Commerce-Richtlinie, ABl. EG 2000, Nr. L 178, S. 4, zum TDG BT-Drucks. 14/6098, zu § 3 Satz 1 Nr. 6, S. 16.

sungsort.[495] Maßgeblich ist der Schwerpunkt der tatsächlich ausgeübten wirtschaftlichen Tätigkeit (§ 2a Abs. 1 TMG).[496] Im Fall mehrerer Niederlassungen in verschiedenen Ländern ist Ort der Niederlassung primär der Ort, von dem aus der jeweilige Dienst erbracht wird. Ist eine eindeutige Bestimmung nicht möglich, gilt der Ort des Schwerpunkts der wirtschaftlichen Tätigkeit des Diensteanbieters für den konkreten Dienst als Niederlassungsort.[497] Für Anbieter, welche unter die Geltung der Richtlinie 89/552/EWG fallen, also audiovisuelle Mediendienste oder Rundfunk anbieten, ist der Sitzort in § 2a Abs. 2 bis 4 TMG näher definiert.

b) Gesetzlich bestimmte Ausnahmen

Vom Grundsatz der alleinigen Berücksichtigung des Rechts am Niederlassungsort eröffnet der Richtliniengeber den nationalen Gesetzgebern nach Art. 3 Abs. 3 ECRL für bestimmte näher aufgezählte Rechtsbereiche Ausnahmemöglichkeiten, wovon der deutsche Gesetzgeber in § 3 Abs. 3 und 4 TMG Gebrauch machte. Die Ausnahmen in § 3 Abs. 3 TMG betreffen im Wesentlichen das nach den Regeln des internationalen Privatrechts anwendbare Sachrecht[498] und das für den Schutz personenbezogener Daten geltende Recht. Im vierten Absatz sind zudem im Einzelnen näher aufgezählte Bereiche, wie z.B. Gewinnspiele sowie das Kartell- und Urheberrecht, vom Herkunftslandprinzip ausgenommen. Neben diesen generellen Ausnahmen kompletter näher bestimmter Rechtsbereiche vom Herkunftslandprinzip sieht die Richtlinie in Art. 3 Abs. 4 lit. a ECRL überdies Ausnahmen beschränkt auf konkrete Einzelfälle vor. Die nationalen Behörden dürfen das innerstaatliche Recht auf im Ausland ansässige Diensteanbieter danach nur anwenden, wenn bestimmte Dienste der Informationsgesellschaft eine Beeinträchtigung oder ernsthafte und schwerwiegende Gefahr für bestimmte Schutzgüter – z.B. die öffentliche Sicherheit und Ordnung – darstellen. Diese Einzelfallausnahme versuchte der deutsche Gesetzgeber in § 3 Abs. 5 TMG umzusetzen.[499]

---

[495] Ebenda. Dies übersieht anscheinend *Poenig*, Die strafrechtliche Haftung des Linkanbieters, S. 106, wenn er gegen die Geltung des Herkunftslandprinzips für das Strafrecht anführt, der Diensteanbieter könne frei entscheiden, wo er seine Server aufstellt.

[496] EuGH, Urteil vom 25.7.1991, *The Queen ./. Secretary Of State For Transport, Ex Parte Factortame Ltd. u.a.*, Rs. C-221/89, Slg. 1991, S. I-03905 ff., Rn. 20; *Lammich*, in: Moritz/Dreier, Rechts-Handbuch zum E-Commerce[2], Teil B, Rn. 264; *Schmidt*, Gefahrenabwehrmaßnahmen im Internet, S. 277 f. i.V.m. 306.

[497] Erwägungsgrund 19 der E-Commerce-Richtlinie, ABl. EG 2000, Nr. L 178, S. 4.

[498] BT-Drucks. 14/6098, zu § 4 Abs. 3 TDG, S. 18.

[499] Vergleich zu den Umsetzungsdefiziten im Folgenden unter Teil 2, III.A.4.

4. Geltung des § 3 Abs. 2 Satz 1 TMG im Strafrecht

Die Frage nach der Geltung des Herkunftslandprinzips gemäß § 3 Abs. 2 Satz 1 TMG im deutschen Strafrecht beantwortet die Wissenschaft – soweit sie das Problem anspricht – unterschiedlich. Während eine Ansicht das Herkunftslandprinzip auf das Strafrecht prinzipiell anwendet und keinen der Ausnahmetatbestände des § 3 TMG zum generellen Ausschluss nutzt,[500] schließt eine weitere Auffassung die Geltung des Herkunftslandprinzips mittels des als Einzelfallausnahme konzipierten § 3 Abs. 5 TMG für das Strafrecht grundsätzlich aus.[501] Nach Ansicht anderer Literaturvertreter findet das Prinzip im Bereich des Strafrechts indes keine Anwendung, weil die Systematik des Art. 3 ECRL selbst das Strafrecht aus dem Geltungsbereich des Herkunftslandprinzips ausschließe[502] bzw. dem Richtliniengeber für das Strafrecht die Rechtsetzungskompetenz fehle.[503]

a) Grammatische Auslegung

Nach dem Wortlaut des § 3 Abs. 2 Satz 1 TMG ist das Recht des Staates, in dem der Diensteanbieter niedergelassen ist, in allen Rechtsbereichen maßgeblich, da das Gesetz nicht nach einzelnen Rechtsgebieten differenziert. Die generellen Ausnahmeregelungen des § 3 Abs. 3 und 4 TMG betreffen nach der Gesetzesformulierung den Bereich des Strafrechts ebenfalls nicht.

Der Anwendung des Herkunftslandprinzips auf dem Gebiet des Strafrechts könnte indes § 3 Abs. 5 Satz 1 TMG entgegenstehen, weil dieser nationale Maßnahmen zulässt, wenn das innerstaatliche Recht dem Schutz bestimmter Rechtsgüter vor

---

[500] So für die (früheren) inhaltsgleichen §§ 4 TDG/5 MDStV: *Altenhain*, in: Zieschang/Hilgendorf/Laubenthal, Strafrecht und Kriminalität in Europa, S. 107, 120, der jedoch die Anwendung des Herkunftslandprinzips im Ergebnis für den Bereich des Strafrechts für nicht sinnvoll erachtet, siehe S. 124; *Brunner*, in: Manssen, Telekommunikations- und Multimediarecht, Bd. 2, § 4 TDG, Rn. 6, 73; *Spindler*, in: Spindler/Schmitz/Geis, TDG, § 4 TDG, Rn. 68; *ders.*, RabelsZ 66 (2002), 633, 681 ff.; *ders.*, NJW 2002, 921, 926; *Vassilaki*, in: Moritz/Dreier, Rechts-Handbuch zum E-Commerce[2], Teil G, Rn. 11 f.

[501] So für die (früheren) inhaltsgleichen §§ 4 TDG/5 MDStV: *Kudlich*, HRRS 2004, 278, 284; *ders.*, JA 2002, 798, 799; *Nickels*, CR 2002, 302, 304, Fn. 28; *Poenig*, Die strafrechtliche Haftung des Linkanbieters, S. 107 f.; *Satzger*, in: Heermann/Ohly, Verantwortlichkeit im Netz, S. 161, 178; *ders.*, Internationales und Europäisches Strafrecht, § 5, Rn. 49; wohl auch *Schwarzenegger*, in: Plöckinger/Duursma/Mayrhofer, Internetrecht, 395, 424 (für Österreich); *Tettenborn* et al., Beilage Nr. 10 zu BB 2001, 1, 14; *Zöchbauer*, in: Plöckinger/Duursma/Mayrhofer, Internetrecht, 435, 440 (für Österreich); für § 3 TMG *Heghmanns*, in: Achenbach/Ransiek, HWSt[3], Rn. 22.

[502] *Von Bubnoff*, in: Zieschang/Hilgendorf/Laubenthal, Strafrecht und Kriminalität in Europa, S. 83, 101.

[503] So für den (früheren) inhaltsgleichen § 4 TDG: *Pelz*, E-Commerce – Strafbarkeit, das vergessene Risiko (online); *Poenig*, Die strafrechtliche Haftung des Linkanbieters, S. 107 f., der daneben aber auch die Argumente der vorgenannten zwei anderen Ansichten zum Ausschluss des Strafrechts aus dem Bereich des Herkunftslandprinzips heranzieht.

Beeinträchtigungen oder ernsthaften und schwerwiegenden Gefahren *dient* und die Maßnahmen verhältnismäßig sind. Der Wortlaut des § 3 Abs. 5 Satz 1 TMG ist allerdings gegenüber den Regelungsvorgaben in der E-Commerce-Richtlinie weiter gefasst. Nach Art. 3 Abs. 4 lit. a ECRL dürfen die Mitgliedstaaten nämlich nur verhältnismäßige nationale Maßnahmen ergreifen, wenn im Einzelfall ein Dienst der Informationsgesellschaft bestimmte näher aufgezählte Schutzziele *beeinträchtigt* oder eine ernsthafte und schwerwiegende Gefahr einer Beeinträchtigung dieser Ziele *vorliegt*. Mit dem Verzicht auf eine tatsächliche Beeinträchtigung bzw. ernsthafte und schwerwiegende Gefährdung der Schutzziele geht § 3 Abs. 5 Satz 1 TMG über die Richtlinienvorgaben hinaus, weil er das in Art. 3 Abs. 1 und 2 ECRL eingeführte Herkunftslandprinzip weiter begrenzt, als es die in Art. 3 Abs. 4 lit. a ECRL vorgesehenen Einschränkungen erlauben. Der deutsche Gesetzgeber setzte das Ziel der Richtlinie, die Verwirklichung eines gemeinsamen Binnenmarkts ohne Grenzen, folglich nicht vollständig um. Nach dem Wortlaut der deutschen Regelung könnte nämlich nahezu jede strafrechtlich relevante Handlung als Beeinträchtigung oder Gefährdung der näher bestimmten geschützten Rechtsgüter aufzufassen sein,[504] da der Wortlaut allein darauf abstellt, dass das innerstaatliche Recht dem Schutz der genannten Rechtsgüter dient. § 3 Abs. 5 Satz 1 TMG muss daher richtlinienkonform ausgelegt werden. Der nationale Gesetzgeber braucht die Richtlinienvorgaben zwar nicht wörtlich zu übernehmen,[505] die Zielsetzung der Richtlinie ist aber verbindlich[506] und die richtlinienkonforme Auslegung eine Rechtspflicht.[507] Die nationalen Gerichte müssen bei einer richtlinienkonformen Auslegung das nationale Recht so weit wie möglich am Wortlaut und Zweck der Richtlinie interpretieren und anwenden, um im Wege der Rechtsfortbildung der Richtlinie gerecht zu werden.[508] Die Fortbildung des Rechts gelangt erst dort an

---

[504] So denn auch die Begründung der Bundesregierung, BT-Drucks. 14/6098, S. 20 und ihr folgend *Poenig*, Die strafrechtliche Haftung des Linkanbieters, S. 102.

[505] EuGH, Urteil vom 20.2.1992, *Kommission der Europäischen Gemeinschaften ./. Königreich der Niederlande*, Rs. C-190/90, Slg. 1992, S. I-03265 ff., Rn. 17.

[506] EuGH, Urteil vom 10.4.1984, *Sabine von Colson und Elisabeth Kamann ./. Land Nordrhein-Westfalen*, Rs. 14/83, Slg. 1984, S. 01891 ff., Rn. 15; *ders.*, Urteil vom 13.11.1990, *Marleasing SA ./. Comercial Internacional De Alimentacion SA*, Rs. C-106/89, Slg. 1990, S. I-04135 ff., Rn. 8; *ders.*, Urteil vom 16.6.2005, *Strafverfahren gegen Maria Pupino*, Rs. C-105/03 (nicht in der amtlichen Sammlung veröffentlicht), Rn. 31 (= NJW 2005, 2839, 2840); *ders.*, Urteil vom 4.7.2006, *Konstantinos Adeneler u.a. ./. Ellinikos Organismos Galaktos*, Rs. C-212/04, (nicht in der amtlichen Sammlung veröffentlicht), Rn. 111 (= NJW 2006, 2465, 2467 f.); *Eisele*, JZ 2001, 1157, 1160.

[507] EuGH, Urteil vom 4.7.2006, *Konstantinos Adeneler u.a. ./. Ellinikos Organismos Galaktos*, Rs. C-212/04, (nicht in der amtlichen Sammlung veröffentlicht), Rn. 108 (= NJW 2006, 2465, 2467); *Brechmann*, Die richtlinienkonforme Auslegung, S. 258, 262 f.; *Herrmann*, EuZW 2005, 436, 437; *ders.*, Richtlinienumsetzung durch die Rechtsprechung, S. 104.

[508] EuGH, Urteil vom 13.11.1990, *Marleasing SA ./. Comercial Internacional De Alimentacion SA*, Rs. C-106/89, Slg. 1990, S. I-04135 ff., Rn. 8; *ders.*, Urteil vom 16.12.1993, *Teodoro Wagner Miret ./. Fondo De Garantia Salarial*, Rs. C-334/92,

ihre Grenzen, wo der Nationalstaat die Richtlinie bewusst unionsrechtswidrig in nationales Recht transformiert,[509] also eine richtlinienkonforme Auslegung contra legem wäre.[510]

Nach richtlinienkonformer Auslegung unterliegen also das Anbieten und Erbringen von Telemedien nur dann nicht dem Herkunftslandprinzip, sondern den Einschränkungen der betroffenen Mitgliedstaaten, wenn die jeweiligen nationalen Maßnahmen im Einzelfall zum Schutz näher bestimmter Rechtsgüter vor Beeinträchtigungen oder ernsthaften und schwerwiegenden Gefahren erforderlich sind und die auf der Grundlage des innerstaatlichen Rechts in Betracht kommenden Maßnahmen in einem angemessenen Verhältnis zu diesen Schutzzielen stehen. Die Ausnahmeregelung in § 3 Abs. 5 Satz 1 TMG widerspricht also nicht der Anwendbarkeit des Herkunftslandprinzips auf dem Gebiet des Strafrechts.[511]

b) Historische Auslegung

Für die Einbeziehung des Strafrechts in den Geltungsbereich der Richtlinie spricht ferner die Entstehung des Art. 3 Abs. 4 ECRL. Im Vorschlag der Europäischen Kommission für den Entwurf der E-Commerce-Richtlinie waren die später in veränderter Form in den Absätzen 3 bis 5 des Art. 3 ECRL aufgegangenen Regelungen in Art. 22[512] enthalten. Dieser Artikel sah in der Einzelfallausnahme (heute Art. 3 Abs. 4 lit. a) lit. i) ECRL) weder einen ausdrücklichen Bezug auf die Verhütung, Ermittlung, Aufklärung und Verfolgung von Straftaten noch einen Ausschluss von der Unterrichtungspflicht bei strafverfahrensrechtlichen Maßnahmen (heute Art. 3 Abs. 4 lit. b) ECRL)[513] vor. Im weiteren Verfahren wurden diese Veränderungen jedoch zur Gewährleistung der Bekämpfung der im Internet begangenen Straftaten aufgenommen. Dem Rat der Europäischen Union war daran gelegen, dass „der Richtlinienentwurf nicht zu einer Erschwerung der Ermittlung von Straf-

---

Sgl. 1993, S. I-06911 ff., Rn. 20; *ders.*, EuZW 2004, 691, 696, Rn. 113; *ders.*, Urteil vom 4.7.2006, *Konstantinos Adeneler u.a. ./. Ellinikos Organismos Galaktos*, Rs. C-212/04, (nicht in der amtlichen Sammlung veröffentlicht), Rn. 108 ff. (= NJW 2006, 2465, 2467 f.); *Brechmann*, Die richtlinienkonforme Auslegung, S. 259 ff.

509 EuGH, Urteil vom 16.12.1993, *Teodoro Wagner Miret ./. Fondo De Garantia Salarial*, Rs. C-334/92, Sgl. 1993, S. I-06911 ff., Rn. 20; *ders.*, EuZW 2004, 691, 696, Rn. 112; *Fetzer/Groß*, EuZW 2005, 550, 551.

510 EuGH, Urteil vom 4.7.2006, *Konstantinos Adeneler u.a. ./. Ellinikos Organismos Galaktos*, Rs. C-212/04, (nicht in der amtlichen Sammlung veröffentlicht), Rn. 110 (= NJW 2006, 2465, 2467); kritisch im Ergebnis, aber zustimmend *Auer*, NJW 2007, 1106, 1108 f.

511 *Altenhain*, in: Zieschang/Hilgendorf/Laubenthal, Strafrecht und Kriminalität in Europa, S. 107, 120 (noch zur a.F. des TDG).

512 Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates über bestimmte rechtliche Aspekte des elektronischen Geschäftsverkehrs im Binnenmarkt, KOM(1998) 586, ABl. EG 1999, Nr. C 30, S. 13 f.

513 Erwägungsgrund 26 der E-Commerce-Richtlinie, ABl. EG 2000, Nr. L 178, S. 4.

taten im Bereich des elektronischen Handels führen sollte, sodass der Kommissionsvorschlag in einigen Punkten entsprechend geändert wurde. Auf der Grundlage der in Art. 3 Abs. 4 ECRL (Art. 22 Abs. 3 des Kommissionsvorschlags) vorgenommenen Änderungen können die Mitgliedstaaten in besonderen Fällen von den Bestimmungen der Richtlinie über das Herkunftslandprinzip und den freien Verkehr von Diensten der Informationsgesellschaft abweichen, wenn dies zum Schutz der öffentlichen Ordnung, insbesondere zur Verhütung, Ermittlung, Aufklärung und Verfolgung von Straftaten erforderlich ist".[514] Der Richtliniengeber wollte das Strafrecht folglich in den Geltungsbereich des Rechtsakts einbeziehen und lediglich durch Ausnahmen im Einzelfall die Möglichkeit einer hinreichenden strafrechtlichen Aufklärung und Verfolgung sicherstellen.[515]

Hinweise auf die Nichtanwendbarkeit des Herkunftslandprinzips auf dem Gebiet des Strafrechts ergeben sich ferner nicht aus den Erwägungsgründen der Richtlinie. Nach dem Erwägungsgrund Nr. 8 zur E-Commerce-Richtlinie ist es nicht deren Ziel, den Bereich des Strafrechts zu harmonisieren,[516] was für einen generellen Ausschluss des Strafrechts aus dem Anwendungsbereich der Regelung der E-Commerce-Richtlinie sprechen könnte, wenn hiermit zwingend der Schluss der Nichtregelung des strafrechtlichen Bereichs verbunden wäre. Der fehlende Wille zur Harmonisierung steht der Anwendung des Herkunftslandprinzips auf das Strafrecht bei näherer Betrachtung jedoch nicht entgegen. Eine Harmonisierung innerstaatlichen Rechts hat die Europäische Gemeinschaft nur in einigen wenigen Bereichen angestrebt, beispielsweise bei den Regelungen zur Verantwortlichkeit der Provider in Form der Art. 12 bis 14 ECRL. Das Herkunftslandprinzip ist demgegenüber lediglich Ausdruck der gegenseitigen Anerkennung des innerstaatlichen Rechts anderer Mitgliedstaaten und nicht der Harmonisierung.[517] Wo der Richtliniengeber eine Harmonisierung nicht vorgenommen hat, kann der Rechtsanwender die Nichtanwendbarkeit einer Spezialregelung auf ein Rechtsgebiet jedoch nicht allein damit begründen, dass sich der Richtliniengeber mit einem Weniger an Eingriffen – hier der gegenseitigen Anerkennung anstelle der Harmonisierung – zufrieden gegeben hat. Nach dem zur Zeit des Erlasses der Richtlinie geltenden Art. 3b Abs. 3 EUV waren Maßnahmen der Gemeinschaft auf das für das Erreichen der Ziele des Vertrags erforderliche Maß zu begrenzen. Ist die Verwirklichung des freien Verkehrs

---

[514] Gemeinsamer Standpunkt (EG) Nr. 22/2000 vom Rat festgelegt am 28.2.2000 im Hinblick auf den Erlass der Richtlinie 2000/30/EG des Europäischen Parlaments und des Rates vom 8.6.2000 über bestimmte rechtliche Aspekte der Dienste der Informationsgesellschaft, insbesondere des elektronischen Geschäftsverkehrs, im Binnenmarkt, ABl. EG 2000, Nr. C 128, S. 49.

[515] *Altenhain*, in: Zieschang/Hilgendorf/Laubenthal, Strafrecht und Kriminalität in Europa, S. 107, 111.

[516] ABl. EG 2000, Nr. L 178, S. 2.

[517] *Altenhain*, in: Zieschang/Hilgendorf/Laubenthal, Strafrecht und Kriminalität in Europa, S. 107, 112; *Brunner*, in: Manssen, Telekommunikations- und Multimediarecht, Bd. 2, § 4 TDG, Rn. 5; *Kudlich*, HRRS 2004, 278, 282.

der Dienstleistungen bereits durch eine gegenseitige Anerkennung von Regelungen möglich, kann die fehlende Harmonisierung eines Rechtsbereichs der Anwendung der Regelungen der Richtlinie nicht entgegenstehen. Darüber hinaus darf auch der Umstand, dass der Richtliniengeber im Einzelfall gar keine Kompetenz für eine umfassende Harmonisierung hat, nicht aus den Augen verloren werden.

Der Ausschluss des Strafrechts aus dem Regelungsbereich der E-Commerce-Richtlinie kann zudem nicht auf den Erwägungsgrund Nr. 26 gestützt werden, in dem es heißt, „die Mitgliedstaaten können im Einklang mit den in dieser Richtlinie festgelegten Bedingungen ihre nationalen strafrechtlichen Vorschriften und Strafprozeßvorschriften anwenden, um Ermittlungs- und andere Maßnahmen zu ergreifen, die zur Aufklärung und Verfolgung von Straftaten erforderlich sind, ohne diese Maßnahmen der Kommission mitteilen zu müssen".[518] Im Erwägungsgrund ist nämlich lediglich erläutert, was nach Ansicht des Richtliniengebers ohnehin feststeht: Das nationale Strafrecht ist uneingeschränkt anwendbar, wo die Richtlinie entweder von vornherein nicht greift oder aber ein Ausnahmefall des Art. 3 Abs. 4 ECRL (§ 3 Abs. 5 Satz 1 TMG) vorliegt.

In der Begründung zum TDG – die der Gesetzgeber für das insoweit nahezu gleichlautende TMG in Bezug nimmt[519] – finden sich mit den vorgenannten Erwägungsgründen vergleichbare Aussagen, die lediglich auf den ersten Blick den Willen des Gesetzgebers hinsichtlich der Nichtanwendbarkeit des Herkunftslandprinzips auf das Strafrecht nahe legen. So soll beispielsweise die Anwendbarkeit des deutschen Straf- und Ordnungswidrigkeitenrechts durch § 4 Abs. 1, Abs. 5 Satz 1 Nr. 1 TDG (§ 3 Abs. 1, Abs. 5 Satz 1 TMG) nicht berührt werden.[520] Außerdem sei bei Erfüllung von Tatbeständen des deutschen Straf- und Ordnungswidrigkeitenrechts eine Beeinträchtigung bzw. Gefahr i.S.d. § 4 Abs. 5 Satz 1 TDG (§ 3 Abs. 5 Satz 1 TMG) gegeben, sodass das deutsche Straf- und Ordnungswidrigkeitenrecht bezogen auf die genannten Schutzgüter zur Anwendung komme.[521] Der deutsche Gesetzgeber widerspricht sich in den vorgenannten Begründungen damit bereits. Während einerseits das Straf- und Ordnungswidrigkeitenrecht überhaupt nicht berührt werden soll, soll andererseits die Ausnahmevorschrift des § 4 Abs. 5 Satz 1 TDG (§ 3 Abs. 5 Satz 1 TMG) in straf- und ordnungswidrigkeitsrechtlichen Fallkonstellationen die Regel sein. Der Wille des deutschen Gesetzgebers, das Strafrecht aus dem Geltungsbereich des Herkunftslandprinzips auszuscheiden, kommt im Übrigen in § 3 TMG objektiv an keiner Stelle zum Ausdruck.[522] Fehlt jede Umsetzung der gesetzgeberischen Begründung im Gesetz selbst, ist also der Wille

---

[518] ABl. EG 2000, Nr. L 178, S. 4.

[519] Insoweit verweist der Gesetzgeber bei der Begründung des TMG auf die des TDG, BT-Drucks. 16/3078, zu § 3 (Herkunftslandprinzip), S. 14.

[520] BT-Drucks. 14/6098, zu § 4 Vorbemerkung, S. 17.

[521] BT-Drucks. 14/6098, zu § 4 II, S. 18.

[522] *Kudlich*, HRRS 2004, 278, 281 f. (zu § 4 TDG und § 5 MDStV).

nicht Wort geworden, kommt der historischen Auslegung kein starkes Gewicht zu.[523] Entscheidend ist der objektiv im Wortlaut des Gesetzes manifestierte Wille, denn nur er ist verfassungsgemäß sichtbar, legitimiert und legalisiert. Darüber hinaus werden die Erwägungen des deutschen Gesetzgebers der Richtlinienvorgabe in Art. 3 Abs. 4 ECRL nicht gerecht, wonach nationale Maßnahmen des Aufnahmestaates nur dann und lediglich im Einzelfall zulässig sind, wenn sie aus den in Art. 3 Abs. 4 lit. a) lit. i) ECRL näher aufgezählten Gründen erforderlich sind. Eine Ausnahme vom Herkunftslandsprinzip ist folglich bloß im Einzelfall gestattet; eine vollständige Nichtanwendung des Herkunftslandprinzips auf dem Gebiet des Strafrechts verfolgt die Richtlinie und bei richtlinienkonformer Auslegung § 3 Abs. 5 Satz 1 TMG nicht.

c) Systematische Auslegung

Aus der Systematik der Richtlinie bzw. des § 3 TMG ergibt sich gleichfalls die Anwendbarkeit des Herkunftslandprinzips für den Bereich des Strafrechts. Während der Gesetzgeber in § 3 Abs. 2 TMG das Herkunftslandprinzip als eine Querschnittsregelung, die alle Rechtsbereiche einschließt,[524] für das geschäftsmäßige Angebot von Telemedien durch Diensteanbieter installiert hat, sind die Ausnahmen hiervon in den folgenden Absätzen geregelt. Dies macht deutlich, dass hier ein Regel-Ausnahme-Verhältnis normiert ist, bei dem Absatz 2 die Regel (Nichtanwendbarkeit innerstaatlichen Rechts in allen Rechtsbereichen) und die Absätze 3 bis 5 die Ausnahmen darstellen und daher tendenziell eng auszulegen sind.[525] Wenn aber das Strafrecht keine ausdrückliche Erwähnung in den Absätzen 3 und 4 findet und darüber hinaus das Gesetz nur eine Ausnahme für unbenannte wichtige Einzelfälle in Absatz 5 vorsieht, muss das Herkunftslandprinzip folglich auch im Strafrecht gelten.[526] Hätte das Herkunftslandprinzip den Bereich des Strafrechts generell nicht erfassen sollen, hätten das Europäische Parlament und der Rat in Art. 3 Abs. 4 lit. a) lit. i) ECRL nicht bestimmen müssen, dass die Mitgliedstaaten im Einzelfall gegen Dienste der Informationsgesellschaft zum Schutz der öffentlichen Ordnung, insbesondere zur Verhütung, Ermittlung, Aufklärung und Verfolgung von Straf-

---

[523] BVerfGE 1, 299, 312; 10, 234, 244; 11, 126, 130 f.; 20, 283, 293; 79, 106, 121; *Schmalz*, Methodenlehre für das juristische Studium, Rn. 263, spricht insoweit vom im Gesetz zum Ausdruck gekommenen objektivierten Willen des Gesetzgebers.

[524] *Fröhlinger*, in: Drexl et al., Europarecht im Informationszeitalter, S. 9, 14 (für § 4 TDG, § 5 MDStV).

[525] *Ruess*, Die E-Commerce-Richtlinie und das deutsche Wettbewerbsrecht, S. 50; *Spindler*, in: Spindler/Schmitz/Geis, TDG, § 4, Rn. 9, 36; *Tettenborn* et al., Beilage Nr. 10 zu BB 2001, 1, 12 (jeweils für § 4 TDG, § 5 MDStV).

[526] *Altenhain*, in: Zieschang/Hilgendorf/Laubenthal, Strafrecht und Kriminalität in Europa, S. 107, 113 f.; *Brunner*, in: Manssen, Telekommunikations- und Multimediarecht, Bd. 2, § 4 TDG, Rn. 59, 62, 68; *Spindler*, Beilage 7 zu MMR 2000, 4, 19; *ders.*, RabelsZ 66 (2002), 633, 683 (jeweils für § 4 TDG, § 5 MDStV); *ders.*, in: Spindler/Schmitz/Geis, § 4, Rn. 69.

taten vorgehen können.[527] Zudem wäre eine Regelung der Ausnahme von der allgemeinen Mitteilungspflicht nach Art. 3 Abs. 4 lit. b) ECRL,[528] umgesetzt in § 3 Abs. 5 Satz 2 TMG, nicht erforderlich gewesen.[529]

Aus der Rechtsprechung des EuGH ergibt sich ebenfalls, dass Ausnahmevorschriften – wie die der Absätze 3 bis 5 – eng auszulegen sind.[530] So fallen nach dem EuGH z.B. Regelungen nicht bereits deshalb unter den Begriff der öffentlichen Ordnung, weil Verstöße Strafsanktionen nach sich ziehen.[531] Der Begriff der öffentlichen Ordnung ist im Gemeinschaftsrecht restriktiv auszulegen, wenn er eine Ausnahme von einem wesentlichen Grundsatz des Gemeinschaftsrechts (hier des freien Waren- und Dienstleistungsverkehrs) rechtfertigten soll.[532] Will sich ein Mitgliedstaat auf den Schutz der öffentlichen Ordnung zur Beschränkung einer Grundfreiheit berufen, muss nach der Rechtsprechung des EuGH eine tatsächliche und hinreichend schwere Gefahr vorliegen, die ein Grundinteresse der Gesellschaft berührt.[533] Da aber nicht jedes innerstaatliche Interesse, das unter dem Schutz einer Strafnorm steht, ein solches Grundinteresse verkörpert, kann das Strafrecht auch nicht in Gänze unter den Ausnahmetatbestand des Schutzes der öffentlichen Ordnung fallen.[534] Die auf Einzelfälle begrenzte Ausnahme in § 3 Abs. 5 Satz 1 TMG eröffnet folglich keinen Weg für einen generellen Ausschluss des Strafrechts aus dem Geltungsbereich des Herkunftslandprinzips.[535]

Nach richtlinienkonformer Interpretation des deutschen Rechts (§ 3 Abs. 5 TMG) ist nicht entscheidend, ob die jeweilige Strafnorm dem Schutz vor Beein-

---

[527] *Altenhain*, in: Zieschang/Hilgendorf/Laubenthal, Strafrecht und Kriminalität in Europa, S. 107, 111; *Spindler*, ZRP 2001, 203, 205; *ders.*, RIW 2002, 183, 186; *ders.*, NJW 2002, 921, 926.

[528] Erwägungsgrund 26 der E-Commerce-Richtlinie, ABl. EG 2000, Nr. L 178, S. 4.

[529] *Spindler*, ZRP 2001, 203, 205; *ders.*, RabelsZ 66 (2002), 633, 682 (zu § 4 TDG).

[530] EuGH, Urteil vom 17.1.1985, *S.A. Piraiki-Patraiki u.a. ./. Kommission der Europäischen Gemeinschaften*, Rs. 11/82, Slg. 1985, S. 00207 ff., Rn. 26.

[531] EuGH, Urteil vom 13.3.1984, *Strafverfahren gegen Karl Prantl*, Rs. 16/83, Slg. 1984, S. 01299 ff., Rn. 33; *Altenhain*, in: Zieschang/Hilgendorf/Laubenthal, Strafrecht und Kriminalität in Europa, S. 107, 114.

[532] EuGH, Urteil vom 4.12.1974, *Yvonne von Duyn ./. Home Office*, Rs. 41-74, Slg. 1974, S. 01337, Rn. 4, 18/19.

[533] EuGH, Urteil vom 27.10.1977, *Pierre Bouchereau*, Rs. 30/77, Slg. 1977, S. 01999 ff., Rn. 33/35; ders., Urteil vom 18.5.1982, *Rezguia Adoui ./. Belgien u.a.* und *Dominique Cornuaille ./. Belgien*, Rs. 115/81 und 116/81, Slg. 1982, S. 01665 ff., Rn. 8; EuGH, Urteil vom 19.1.1999, *Strafverfahren gegen Donatella Calfa*, Rs. C-348/96, Slg. 1999, S. I-00011, Rn. 21; *ders.*, Urteil vom 14.3.2000, *Association Eglise des scientologie u.a. ./. Premier ministre*, Rs. C-54/99, Slg. 2000, S. I-01335, Rn. 17.

[534] *Altenhain*, in: Zieschang/Hilgendorf/Laubenthal, Strafrecht und Kriminalität in Europa, S. 107, 113 f.; *Brunner*, in: Manssen, Telekommunikations- und Multimediarecht, Bd. 2, § 4 TDG, Rn. 59, 62, 68; *Spindler*, Beilage 7 zu MMR 2000, 4, 19.

[535] *Tettenborn* et al., Beilage Nr. 10 zu BB 2001, 1, 12, anders allerdings auf S. 14, wo strafrechtlich sanktioniertes Verhalten generell § 4 V TDG unterstellt wird.

trächtigungen oder schwerwiegenden Gefahren dient, sondern ob im Einzelfall eine Beeinträchtigung oder schwerwiegende Gefahr vorliegt. Daher sind die Voraussetzungen des § 3 Abs. 5 Satz 1 TMG nicht bereits durch jedes strafbare Angebot erfüllt. Rein abstrakte Gefahren genügen beispielsweise nicht für die Anwendung des innerstaatlichen Strafrechts als Ausnahme vom Herkunftslandprinzip.[536] Eine abstrakte Gefahr liegt nämlich schon vor, wenn der Täter die tatbestandliche Handlung vornimmt, ohne dass das Tatobjekt überhaupt nur in den Gefahrenkreis gelangen und dessen Verletzung nahe liegen muss. Die Gefährdung des Rechtsguts wird von Tatbestands wegen unwiderlegbar vermutet mit der Folge, dass der Tatbestand nach zum Teil vertretener Ansicht auch erfüllt ist, wenn die Unmöglichkeit der Verwirklichung der Gefahr nachgewiesen ist.[537] Für eine nationale Maßnahme bedarf es aber gerade einer tatsächlichen und hinreichend schweren Gefahr,[538] eine abstrakte Gefahr erfüllt diese Anforderungen nicht. Dieser Ausschluss abstrakter Gefahren aus dem mitgliedstaatlichen Strafrechtsschutz ist ohnedies bereits unter dem Blickwinkel des Abwägungsgebotes zwischen Eingriffs- und Abwehrinteresse geboten.[539] Bei geringeren Gefahren kommt hinzu, dass die Richtlinie das Abwehrinteresse zusätzlich verstärkt.[540]

Für die Einbeziehung des Strafrechts in den Geltungsbereich der Richtlinie sprechen überdies die Vorschriften in den Art. 12 bis 14 ECRL, welche die Verantwortlichkeit der Diensteanbieter für Inhalte in Computernetzen regeln. Der Richtliniengeber hat mit diesen Vorschriften einen EU-einheitlichen (strafrechtlichen) Standard geschaffen[541] und daher den Bereich des Strafrechts gerade nicht aus der Richtlinie ausgeschlossen. Auch aus Art. 2 lit. h ECRL, der den koordinierten Bereich der Richtlinie umschreibt, kann der Schluss gezogen werden, dass das Strafrecht von der Richtlinie mit umfasst wird. In den koordinierten Bereich fallen u.a. die nationalen Regelungen, welche die Qualität und die Inhalte der Dienste betreffen. Gerade das Strafrecht hält aber Regelungen über Inhaltsbeschränkungen wie

---

[536] *Altenhain*, in: Zieschang/Hilgendorf/Laubenthal, Strafrecht und Kriminalität in Europa, S. 107, 114; ähnlich für das Gefahrenabwehrrecht *Greiner*, Die Verhinderung verbotener Internetinhalte im Wege polizeilicher Gefahrenabwehr, S. 177; *Schmidt*, Gefahrenabwehrmaßnahmen im Internet, S. 292, 309 f.

[537] Zum Streit bei § 306a Abs. 1 StGB vgl. m.w.N. die umfangreiche Darstellung bei S/S-*Heine*, § 306a, Rn. 2; MünchKommStGB-*Radtke*, § 306a, Rn. 39 ff.

[538] EuGH, Urteil vom 27.10.1977, *Pierre Bouchereau*, Rs. 30/77, Slg. 1977, S. 01999 ff., Rn. 33/35.

[539] Siehe hierzu die Ausführungen unter Teil 2, II.C.4.a)cc)(3)(b)(bb)(bbb).

[540] Siehe hierzu die Ausführungen unter Teil 2, II.C.4.a)cc)(3)(d)(bb).

[541] Kommission der Europäischen Gemeinschaften, KOM(1998) 586, Erwägungsgrund 16, ABl. EG 1999, Nr. C 30, S. 6; *Altenhain*, in: Zieschang/Hilgendorf/Laubenthal, Strafrecht und Kriminalität in Europa, S. 107, 112; *Ligeti*, Strafrecht und strafrechtliche Zusammenarbeit, S. 252; *Spindler*, NJW 2002, 921, 922; *Tettenborn* et al., Beilage Nr. 10 zu BB 2001, 1, 27.

z.B. in den §§ 185 ff. StGB[542] bereit, sodass die Richtlinie den Bereich des Strafrechts ausdrücklich hätte ausnehmen müssen, wenn dieser nicht miterfasst werden sollte.[543]

d) Teleologische Auslegung

Nach dem Sinn und Zweck des Herkunftslandprinzips ist das Strafrecht ebenfalls in den Geltungsbereich der Richtlinie eingeschlossen. Hintergrund der Einführung des Prinzips ist die Schaffung eines Raums ohne Binnengrenzen nach Art. 26 Abs. 2 AEUV. Mit der Anknüpfung an den Niederlassungsort soll die Dienstleistungsfreiheit gewährleistet und den Diensteanbietern Rechtssicherheit gegeben werden, indem diese ihr Handeln grundsätzlich nur am Recht des Niederlassungsstaates ausrichten müssen.[544] Das Herkunftslandprinzip ist aus den Grundfreiheiten des Vertrags der EG entwickelt worden,[545] um diese Rechte durch den Abbau staatlicher Beschränkungen zu verwirklichen. Der heute in Art. 2 Abs. 1 und 2 AEUV und Art. 6 Abs. 2 EUV verankerte Grundsatz der Gemeinschaftstreue und der Treue zu den Grundfreiheiten verbietet es den Mitgliedstaaten daher, Hürden für die Verwirklichung der Grundfreiheiten zu errichten. Auch das Strafrecht darf die durch das Gemeinschaftsrecht garantierten Grundfreiheiten also nicht beschränken,[546] was dafür spricht, dass das Herkunftslandprinzip auch das Gebiet des Strafrechts erfasst.

Soweit jedenfalls die Rechtsprechung und die h.M. in der Literatur der Europäischen Union im Grundsatz eine originäre Normsetzungskompetenz für den Bereich des Strafrechts weitgehend[547] absprechen,[548] steht diese fehlende Kompetenz der

---

[542] Zu Fallbeispielen der Beleidigung mittels Internet vgl. *Beck*, MMR 2009, S. 736 ff.

[543] *Altenhain*, in: Zieschang/Hilgendorf/Laubenthal, Strafrecht und Kriminalität in Europa, S. 107, 112.

[544] *Fröhlinger*, in: Drexl et al., Europarecht im Informationszeitalter, S. 9, 11 f.; *Satzger*, in: Heermann/Ohly, Verantwortlichkeit im Netz, S. 161, 176; *Tettenborn* et al., Beilage Nr. 10 zu BB 2001, 1, 9.

[545] Siehe hierzu die Ausführungen unter Teil 2, III.A.1.

[546] EuGH, Urteil vom 19.1.1999, *Strafverfahren gegen Donatella Calfa*, Rs. C-348/96, Slg. 1999, S. I-00011 ff., Rn. 17 unter Verweis auf ders., Urteil vom 2.2.1989, *Ian William Cowan ./. Tresor Public*, Rs. 186/87, Slg. 1989, S. 00195 ff., Rn. 19.

[547] Zu der durch Art. 83 Abs. 1 AEUV geschaffenen Möglichkeit, gerade im Bereich des Cybercrime durch die EU Mindeststandards und -strafen vorzugeben, vgl. *Gercke*, CRi 2010, 75 ff.

[548] EuGH, Urteil vom 11.11.1981, *Strafverfahren gegen Guerrino Casati*, Rs. 203/80, Slg. 1981, S. 02595 ff., Rn. 27; ders., Urteil vom 2.2.1989, *Ian William Cowan ./. Tresor Public*, Rs. 186/87, Slg. 1989, S. 00195 ff., Rn. 19; ders., Urteil vom 14.12.1995, *Strafverfahren gegen Giorgio Domingo Banchero*, Rs. C.-387/93, Slg. 1995, S. I-04663 ff., Rn. 58; ders., Urteil vom 16.6.1998, *Strafverfahren gegen Johannes Martinus Lemmens*, Rs. C.-226/97, Slg. 1998, S. 03711 ff., Rn. 19; ders., Urteil vom 13.9.2005, *Kommission der Europäischen Gemeinschaften ./. Europäisches Parlament*, Rs. C-176/03, Slg. 2005,

Geltung des Herkunftslandprinzips auch für das Strafrecht nicht entgegen.[549] Der Richtliniengeber stützte seine Kompetenz zum Erlass der E-Commerce-Richtlinie auf Art. 46 Abs. 2 und Art. 52, 94 EG[550] (heute Art. 52, 59, 115 AEUV), wonach er ermächtigt war, Richtlinien zur Gewährleistung des freien Dienstleistungsverkehrs und der Herstellung eines Binnenmarkts zu erlassen. Von diesem Regelungsbereich ist nach den vorstehenden Auslegungsergebnissen auch das Strafrecht betroffen. Das in der E-Commerce-Richtlinie niedergelegte Herkunftslandprinzip gilt jedoch nicht unmittelbar für die EU-Staaten, sondern erlangt erst durch die Umsetzung mittels nationaler Gesetze innerstaatliche Wirkung. Die hier zum Zuge kommende Anweisungskompetenz der Europäischen Union[551] ist von der begrenzten Befugnis der Europäischen Union, Kriminaltatbestände auf Grundlage des AEUV zu schaffen, strikt zu unterscheiden.[552] Die Mitgliedstaaten schaffen selbst nationale Strafnormen und gewährleisten durch den nationalen Umsetzungsakt, dass ein demokratisch gewähltes Parlament eines souveränen Staates die für seine Bürger verbindlichen Regelungen trifft.[553] Unabhängig davon stellte das BVerfG[554] für die Legitimation der EU auch auf dem Gebiet der Strafrechtspolitik keine gegenüber anderen Bereichen erhöhten Anforderungen. Die demokratische Legitimation der EU folge bereits aus dem Zustimmungsgesetz zu den Gründungsverträgen und den hierin festgelegten Befugnissen sowie durch die Regierungsvertreter im Rat,

---

S. 07879 ff., Rn. 47 (für eine enge Auslegung der fehlenden Strafrechtsetzungskompetenz); BGHSt 25, 190, 193 f., 27, 181, 182; 41, 127, 131 f.; MünchKommStGB-*Ambos*, Vor §§ 3–7, Rn. 7; *Braum*, wistra 2006, 121, 124 f. – der die Gefahren der engeren Auslegung der fehlenden Strafrechtskompetenz durch den EuGH (Urteil vom 13.9.2005, Rs. C-176/03) aufzeigt; *Dannecker*, in: Wabnitz/Janovsky, Handbuch des Wirtschafts- und Steuerstrafrechts, 2. Kap., Rn. 19; *Deutscher*, Die Kompetenzen der Europäischen Gemeinschaften, S. 309 ff., 388; *Hilgendorf*, in: Schwarzenegger/Arter/Jörg, Internet-Recht und Strafrecht, S. 257, 261; *Oehler*, FS Baumann, S. 561, 561 f., 565; *Satzger,* Die Europäisierung des Strafrechts, S. 90 ff., 143; *Schröder*, Europäische Richtlinien und deutsches Strafrecht, S. 104 ff., 161; *Tiedemann*, NJW 1993, 23, 23 f.; a.A. für den Bereich des Schutzes der finanziellen Interessen der Union *Vogel*, in: Sieber et al., Europäisches Strafrecht, 3. Kapitel, Rn. 6.

549 *Spindler*, in: Spindler/Schmitz/Geis, TDG, § 4 TDG, Rn. 69; a.A. *Pelz*, E-Commerce – Strafbarkeit; *Poenig*, Die strafrechtliche Haftung des Linkanbieters, S. 101 f., 107.

550 ABl. EG 2000, Nr. L 178, S. 1.

551 Zur Anweisungskompetenz siehe insbesondere EuGH, EuZW 2005, 632, 634 f., Rn. 48 ff.

552 *Deutscher*, Die Kompetenzen der Europäischen Gemeinschaften, S. 361 f.; *Sieber*, ZStW 103 (1991), 957, 968.

553 *Deutscher*, Die Kompetenzen der Europäischen Gemeinschaften, S. 369 (mit Kritik bei eingeschränktem Umsetzungsspielraum der Mitgliedstaaten, S. 369 ff.); *Eisele*, JZ 2001, 1157, 1160 (mit Kritik bei eingeschränktem Umsetzungsspielraum der Mitgliedstaaten, S. 1161); *Hilgendorf*, in: Schwarzenegger/Arter/Jörg, Internet-Recht und Strafrecht, S. 257, 286 (der jedoch den eingeengten Umsetzungsspielraum der einzelnen Mitgliedstaaten kritisiert); *Kudlich*, HRRS 2004, 278, 282; *Sieber*, ZStW 103 (1991), 957, 972; *Spindler*, RIW 2002, 183, 186; *ders.*, RabelsZ 66 (2002), 633, 682 f.

554 BVerfG NJW 1993, 3047, 3051 ff.

die ihrerseits wieder über die Parlamente der Mitgliedstaaten legitimiert sind. Die Mitwirkung des Europäischen Parlaments vervollständigt die Legitimation der EU.

Zudem führt die Umsetzung der Richtlinie nicht zur Begründung einer Strafbarkeit. Die Staaten außerhalb des Niederlassungssitzes des Diensteanbieters verpflichten sich lediglich, ihr Strafrecht nicht auf bestimmte Sachverhalte anzuwenden.[555] Die Europäische Union kann die Mitgliedstaaten jedenfalls dann verpflichten, bestehende strafbewehrte Ver- oder Gebote zu streichen oder einzuschränken, sogenannten ius non puniendi, wenn diese einen unmittelbaren Bezug zu den Grundfreiheiten aufweisen. Gerade die Gefahr strafrechtlicher Konsequenzen kann nämlich dazu führen, dass eine Freiheit nicht in Anspruch genommen wird.[556] In diesem Sinne hat der EuGH entschieden, dass das Gemeinschaftsrecht auch auf dem Gebiet des Straf- und Strafverfahrensrechts den Mitgliedstaaten Schranken setzt. Die mitgliedstaatlichen nationalen Maßnahmen „dürfen nicht über den Rahmen des unbedingt Erforderlichen hinausgehen, die Kontrollmaßnahmen dürfen nicht so beschaffen sein, dass sie die vom Vertrag gewollte Freiheit einschränken, und es darf daran keine Sanktion geknüpft sein, die so außer Verhältnis zur Schwere der Tat steht, dass sie sich als eine Behinderung der Freiheit erweist".[557] Die im Mittelpunkt des Gemeinschaftsrechts stehende Verwirklichung des Binnenmarkts kann nur dann erfolgreich sein, wenn dem Gemeinschaftsrecht Vorrang zukommt. Parallel hierzu muss die Mitgliedstaaten die Pflicht treffen, etwaige Hindernisse zu beseitigen, die der Anwendung des Gemeinschaftsrechts entgegenstehen. Diese Pflicht erstreckt sich auch auf den Bereich des Strafrechts, da anderenfalls das Gemeinschaftsrecht einen wesentlichen Teil seiner Funktion einbüßen würde.[558]

Für die Einbeziehung des Strafrechts spricht ferner, dass es dem Ziel der Richtlinie widerspricht, wenn ein Diensteanbieter zwar zivil- und öffentlichrechtlich nur die Vorschriften des Mitgliedstaates zu beachten hat, in dem er niedergelassen ist, gleichwohl aber die unterschiedlichen nationalen Strafrechtsnormen berücksichtigen muss.[559] Stellt beispielsweise ein Anbieter nach deutschem Recht stark

---

555 *Kudlich*, HRRS 2004, 278, 282.

556 Ebenda; *Schröder*, Europäische Richtlinien und deutsches Strafrecht, S. 198 f.; siehe dazu auch *Altenhain*, in: Zieschang/Hilgendorf/Laubenthal, Strafrecht und Kriminalität in Europa, S. 107, 115 f.

557 EuGH, Urteil vom 11.11.1981, *Strafverfahren gegen Guerrino Casati*, Rs. 203/80, Slg. 1981, S. 02595 ff., Rn. 27; siehe auch EuGH, Urteil vom 2.2.1989, *Ian William Cowan ./. Tresor Public*, Rs. 186/87, Slg. 1989, S. 00195 ff., Rn. 19; EuGH, Urteil vom 16.6.1998, *Strafverfahren gegen Johannes Martinus Lemmens*, Rs. C.-226/97, Slg. 1998, S. 03711 ff., Rn. 19. Natürlich darf das Strafrecht bereits auch nach nationalem Recht nie über den Rahmen des Erforderlichen hinausgehen.

558 Zur Verpflichtung der Mitgliedstaaten zur Schaffung von Strafnormen zum Schutz gemeinschaftlicher Interessen siehe *Schröder*, Europäische Richtlinien und deutsches Strafrecht, S. 179 ff.

559 *Pelz*, E-Commerce – Strafbarkeit, das vergessene Risiko, – Aussage jedoch als Gegenargument genutzt.

jugendgefährdende Inhalte i.S.d. § 4 JMStV zum Abruf bereit, entstünde das nicht zu rechtfertigende Ergebnis, dass die Inhalte zwar nach deutschem öffentlichem Recht weder indiziert noch gesperrt, aber gleichwohl in Deutschland strafrechtlich verfolgt werden dürften.[560] Dieses Ergebnis widerspräche der Einheit der Rechtsordnung.

e) Zusammenfassung

Das Herkunftslandprinzip gilt also auch für den Bereich des Strafrechts mit der Folge, dass im Anwendungsbereich der Richtlinie grundsätzlich allein das Strafrecht des Niederlassungsstaates maßgeblich ist. Die als Einzelfallausnahme konzipierte Vorschrift des § 3 Abs. 5 Satz 1 TMG führt entgegen anderer Auffassung[561] nicht zum generellen Ausschluss des Strafrechts aus dem Anwendungsbereich des Herkunftslandprinzips.[562]

5. Tauglichkeit des Herkunftslandprinzips im Strafrecht

Mit der Geltung des Herkunftslandprinzips auch im Bereich des Strafrechts ist jedoch nur auf den ersten Blick eine praktikable Lösung grenzüberschreitender Sachverhalte verbunden. Tatsächlich führen bereits die richtlinienimmanenten Einschränkungen in zahlreichen Fällen zum Ausschluss der Anwendbarkeit des Herkunftslandprinzips (nachfolgend unter a)). Die Tauglichkeit der Anknüpfung an den Niederlassungsort im Bereich des Strafrechts ist außerdem durch die mangels Harmonisierung weiter Rechtsbereiche eröffneten Anreize zur Umgehung bestimmter Rechtsordnungen fraglich (unter b)). Diese Zweifel verdichten sich zudem vor dem Hintergrund, dass andere internationale Abkommen und europäische Vereinbarungen bei der Regelung von Kompetenzkonflikten nicht auf das Herkunftslandprinzip, sondern zumeist vordergründig auf das Territorialitätsprinzip abstellen (unter c)).

---

[560] *Altenhain*, in: Zieschang/Hilgendorf/Laubenthal, Strafrecht und Kriminalität in Europa, S. 107, 112 f.

[561] *Nickels*, CR 2002, 302, 304, Fn. 28; *Kudlich*, HRRS 2004, 278, 284; *ders.*, JA 2002, 798, 799; *Satzger*, in: Heermann/Ohly, Verantwortlichkeit im Netz, S. 161, 178; *ders.*, Internationales und Europäisches Strafrecht, § 5, Rn. 49; wohl auch *Schwarzenegger*, in: Plöckinger/Duursma/Mayrhofer, Internetrecht, 395, 424 (für Österreich); *Tettenborn* et al., Beilage Nr. 10 zu BB 2001, 1, 14; *Zöchbauer*, in: Plöckinger/Duursma/Mayrhofer, Internetrecht, S. 435, 440 (für Österreich).

[562] *Altenhain*, in: Zieschang/Hilgendorf/Laubenthal, Strafrecht und Kriminalität in Europa, S. 107, 120; *Brunner*, in: Manssen, Telekommunikations- und Multimediarecht, Bd. 2, § 4 TDG, Rn. 73; *Spindler*, in: Spindler/Schmitz/Geis, TDG, § 4 TDG, Rn. 68; *ders.*, RabelsZ 66 (2002), 633, 681 ff. (jeweils für § 4 TDG, § 5 MDStV).

a) Begrenzter Geltungsbereich durch richtlinienimmanente Einschränkungen

Das Herkunftslandsprinzip hat auf dem Gebiet des Strafrechts nur begrenzte Auswirkungen, weil es viele strafrechtlich relevante Bereiche nicht erfasst. So gilt für in der Bundesrepublik Deutschland niedergelassene Diensteanbieter weiterhin das deutsche Recht, insbesondere wenn sie ihre Dienste im Inland anbieten oder erbringen. Bieten in Deutschland niedergelassene Diensteanbieter ihre Dienste in Staaten außerhalb der Europäischen Union an oder erbringen Anbieter mit Sitz außerhalb der Union ihre Dienste in Deutschland, werden sie von § 3 Abs. 2 Satz 1 TMG gleichermaßen nicht erfasst.[563] Da unter die Regelungen der Richtlinie nur geschäftsmäßige Diensteanbieter fallen, gilt das Herkunftslandprinzip zudem nicht für Privatpersonen. Darüber hinaus sind in Art. 3 Abs. 3 ECRL zahlreiche auch strafrechtlich relevante Rechtsbereiche vom Geltungsbereich der Richtlinie bereits im Vorhinein ausgeschlossen, so beispielsweise strafbare Urheberrechtsverletzungen und illegales Glücksspiel. Für all diese nicht unter das Herkunftslandprinzip fallenden Sachverhalte gelten die im zweiten Teil unter II. herausgearbeiteten Grundsätze.

b) Umgehungsmöglichkeiten mangels Harmonisierung

Zweifel an der Eignung der Anknüpfung an den Niederlassungsort im Bereich des Strafrechts kommen des Weiteren aufgrund der durch die fehlende Harmonisierung der betroffenen Rechtsbereiche eröffneten Anreize zur Umgehung strengerer Rechtsordnungen auf. Mit dem Verzicht der Europäischen Union auf die Harmonisierung der nationalen Regelungen im koordinierten Bereich der E-Commerce-Richtlinie[564] hängt der Schutz der nationalen Interessen in großem Maße von der Kontrolle der Angebote durch den Herkunftsstaat ab. Allein über die Klagemöglichkeiten nach Art. 18 ECRL kann im Fall einer Verletzung des Rechts des Herkunftsstaates durch den Diensteanbieter die Pflicht des Herkunftsstaates zur Kontrolle des Angebots kaum durchgesetzt werden. Kann die Prüfungspflicht des Herkunftsstaates jedoch nicht wirksam erzwungen werden, so besteht in erhöhtem Maße die Gefahr einer nachteiligen Rechtsentwicklung des strafrechtlichen Schutzes hin zum geringsten Schutzniveau, sogenanntes *race to the bottom*.[565] Die Ge-

---

[563] BT-Drucks. 14/6098, Vorbem. zu § 4, S. 17; *Maennel*, in: Ehlers/Wolffgang/Pünder, Rechtsfragen des Electronic-Commerce, S. 29, 49; *Spindler*, in: Spindler/ Schmitz/Geis, TDG, § 4 TDG, Rn. 8.

[564] Kritisch hierzu *Altenhain*, in: Zieschang/Hilgendorf/Laubenthal, Strafrecht und Kriminalität in Europa, S. 107, 119 ff.; *Bodewig*, GRURInt 2000, 475, 482; *Brunner*, in: Manssen, Telekommunikations- und Multimediarecht, Bd. 2, § 4 TDG, Rn. 27 ff.; *Lehmann*, ZUM 1999, 180, 181 f.

[565] *Bodewig*, GRURInt 2000, 475, 481; *Brunner*, in: Manssen, Telekommunikations- und Multimediarecht, Bd. 2, § 4 TDG, Rn. 29; *Kudlich*, HRRS 2004, 278, 283; *Poenig*, Die strafrechtliche Haftung des Linkanbieters, S. 104; *Schmidt*, Gefahrenabwehrmaßnah-

fahr potenziert sich zudem durch die regelmäßig grenzüberschreitende Begehung von Straftaten im Bereich der Computerkriminalität. Gegenteilig wirkt indes der Druck durch die anderen Mitgliedstaaten auf den jeweiligen Herkunftsstaat, dessen nationale Regelungen ausländische Rechtsgüter für gewöhnlich nicht schützen (sog. *race to the top*).[566]

Ein weiteres Problem stellt sich, wenn Inländer strengen strafrechtlichen Sanktionen unterworfen sind, während Ausländer bei Erfüllung des gleichen Sachverhalts gar nicht oder zumindest unter eine wesentlich geringere strafrechtliche Restriktion fallen. Diese sogenannte Inländerdiskriminierung hat der EuGH zwar aus dem Blickwinkel des EU-Rechts nicht beanstandet,[567] weil sie den Binnenmarkt unberührt lässt und folglich die grenzüberschreitenden Grundfreiheiten nicht beschränkt. Gleichwohl ist der Erfolg strafrechtlicher Verbote aber immer auch von deren Anerkennung in der Bevölkerung abhängig, sodass sich Strafdrohungen in Fällen der Inländerdiskriminierung als ungeeignet erweisen können, insbesondere wenn sich der Schutzzweck der jeweiligen Norm aufgrund der grenzüberschreitenden Auswirkungen von Taten ausländischer Anbieter nicht mehr verwirklichen lässt.[568]

c) Spannungsverhältnis zwischen Herkunftsland- und Territorialitätsprinzip

Das Herkunftslandprinzip der E-Commerce-Richtlinie stellt mit dem Niederlassungsort überdies auf einen anderen Anknüpfungspunkt ab als sonstige für den Bereich des Strafrechts bei Internetsachverhalten wichtige internationale und europäische Regelungen. Letztere gehen regelmäßig vom Territorialitäts- und ergänzend vom aktiven Personalitätsprinzip aus,[569] wie z.B. Art. 22 Abs. 1 Convention on Cybercrime des Europarates vom 23.11.2001[570] und der Rahmenbeschluss des Rates der Europäischen Union über Angriffe auf Informationssysteme vom 24.2.2005[571] in Art. 10.[572] Gleiches gilt für den Rahmenbeschluss des Rates der

---

men im Internet, S. 316, 338; *Schwarzenegger*, in: Plöckinger/Duursma/Mayrhofer, Internetrecht, 395, 423 (für Österreich).

[566] *Altenhain*, in: Zieschang/Hilgendorf/Laubenthal, Strafrecht und Kriminalität in Europa, S. 107, 121; *Poenig*, Die strafrechtliche Haftung des Linkanbieters, S. 105; *Schmidt*, Gefahrenabwehrmaßnahmen im Internet, S. 317, 339.

[567] EuGH, Urteil vom 16.6.1994, *Volker Steen ./. Deutsche Bundespost*, Rs. C-132/93, Slg. 1994, S. I-2715, Rn. 5, 9; *Bösch*, Jura 2009, 91, 93; *Bullinger/Mestmäcker*, Multimediadienste, S. 101; *Tettenborn* et al., Beilage Nr. 10 zu BB 2001, 1, 9.

[568] *Altenhain*, in: Zieschang/Hilgendorf/Laubenthal, Strafrecht und Kriminalität in Europa, S. 107, 122; *Kudlich*, HRRS 2004, 278, 283 f.

[569] *Vogel*, in: Zieschang/Hilgendorf/Laubenthal, Strafrecht und Kriminalität in Europa, S. 29, 53 f.

[570] Europarat, ETS No. 185.

[571] Rahmenbeschluss 2005/222/JI des Rates vom 24.2.2005 über Angriffe auf Informationssysteme, ABl. EU 2005, Nr. L 69, S. 67.

Europäischen Union zur Bekämpfung der sexuellen Ausbeutung von Kindern und der Kinderpornographie vom 22.12.2003[573] in Art. 8[574] sowie für den Rahmenbeschluss des Rates der Europäischen Union zur strafrechtlichen Bekämpfung von bestimmten Formen und Ausdrucksweisen von Rassismus und Fremdenfeindlichkeit vom 28.11.2008[575] in Art. 9. Die Umsetzung und Anwendung der vorstehenden Rechtsakte erfordert allerdings den Verzicht auf die Anwendung des Herkunftslandprinzips im Strafrecht, da es sich bei diesen um speziellere Regelungen handelt.[576]

Während die Anknüpfung an den Handlungs- und Erfolgsort (Territorialitätsprinzip) sowie an die Staatsangehörigkeit des Täters (aktives Personalitätsprinzip) in der völkerrechtlichen Praxis etabliert ist,[577] stellt das Herkunftslandprinzip mit der Anknüpfung an den Niederlassungssitz des Diensteanbieters zudem im Bereich des Strafrechts auf einen atypischen Bezugspunkt ab. Für das Strafrecht ist die Berufung auf den Ort der Niederlassung auch wenig sinnvoll, weil sich der Unternehmensstandort im Wesentlichen nach wirtschaftlichen Gesichtspunkten bestimmt[578] und für gewöhnlich keinen besonderen Bezug zur einzelnen Straftat aufweist. Der Niederlassungsort entspricht insbesondere nicht zwangsläufig dem Handlungsort, da je nach Fallkonstellation Mitarbeiter des Unternehmens außerhalb des Niederlassungsorts tätig werden oder aber wirtschaftlich nicht eigenständige Unternehmensteile die Dienste anbieten und erbringen können. In diesen Fällen können die Handlungen nur durch Zurechnung dem Unternehmen vorgeworfen werden. Dies bedingt wiederum, dass es möglich sein muss, auch das Unternehmen selbst strafrechtlich zur Verantwortung zu ziehen. Nicht jeder Mitgliedstaat – wie auch Deutschland – kennt allerdings eine Strafbarkeit juristischer Personen. Insbesondere wenn Mitarbeiter eines Unternehmens außerhalb des Herkunftslands tätig werden, erscheint die Anknüpfung an den Niederlassungsort für die Verfolgung der

---

572 Kommission der Europäischen Gemeinschaften, KOM(2002) 173, S. 16 f.; *Hilgendorf*, in: Schwarzenegger/Arter/Jörg, Internet-Recht und Strafrecht, S. 257, 279 f.

573 Rahmenbeschluss 2004/68/JI des Rates vom 22.12.2003 zur Bekämpfung der sexuellen Ausbeutung von Kindern und der Kinderpornographie, ABl. EU 2004, Nr. L 13, S. 44.

574 Siehe ebenso Rahmenbeschluss (2001/413/JI) des Rates vom 28.5.2001 zur Bekämpfung von Betrug und Fälschung im Zusammenhang mit unbaren Zahlungsmitteln, ABl. EG 2001, Nr. L 149, S. 1, 3, siehe Art. 9.

575 Rahmenbeschluss 2008/913/JI des Rates vom 28.11.2008 zur strafrechtlichen Bekämpfung bestimmter Formen und Ausdrucksweisen von Rassismus und Fremdenfeindlichkeit, ABl. EU 2008, Nr. L 328, S. 55 ff.

576 *Schwarzenegger*, in: Plöckinger/Duursma/Mayrhofer, Internetrecht, S. 395, 423 (für Österreich).

577 American Society of International Law, AJIL 29 (1935), 480 ff., S. 519 ff.; *Oehler*, Internationales Strafrecht, Rn. 153 f., Rn. 702 ff. jeweils mit Nachweisen, dass das Territorialitätsprinzip und das aktive Personalitätsprinzip weltweit verbreitet sind.

578 *Altenhain*, in: Zieschang/Hilgendorf/Laubenthal, Strafrecht und Kriminalität in Europa, S. 107, 123 f.

Straftatbegehung willkürlich. Wäre in diesen Fällen der Mitarbeiter unzutreffenderweise nicht im Wege der Zurechnung selbst als Diensteanbieter[579] anzusehen, würde für ihn das Herkunftslandprinzip nicht gelten. Er käme also nicht in den Genuss der Privilegierung, während sein Arbeitgeber nur mit dem Recht am Niederlassungsort konfrontiert wäre. Selbst wenn aber für jeden Mitarbeiter eines Unternehmens das Herkunftslandprinzip gilt, so bleibt es widersprüchlich, dass Personen ohne starre Unternehmenszugehörigkeit weiterhin das Recht aller betroffenen Staaten beachten müssen.[580] Kaum mit dem Rechtsempfinden zu vereinbaren ist zudem der Umstand, dass vorwiegend kommerziell tätige Straftäter durch das Herkunftslandprinzip privilegiert werden, da sie nur dem Recht des Herkunftsstaates unterliegen, während nicht geschäftsmäßig handelnde kriminelle Personen nach wie vor mit den Rechtsordnungen sämtlicher betroffener Staaten konfrontiert sind.[581]

6. Ergebnis

Im eingeschränkten Anwendungsbereich der E-Commerce-Richtlinie ist das Herkunftslandprinzip auch auf dem Gebiet des Strafrechts beachtlich. Im EU-Ausland niedergelassene Diensteanbieter unterliegen mit ihren Telemedien also grundsätzlich nicht den Anforderungen deutschen Rechts (§ 3 Abs. 2 TMG) und damit nicht der Zuständigkeit deutscher Strafverfolgungsbehörden, weil auch das Strafrecht den freien Dienstleistungsverkehr prinzipiell nicht einschränken darf. Da die Anknüpfung an den Niederlassungsort im Strafrecht aber eher Probleme bereitet als Lösungen für Kompetenzkonflikte bietet, sind aus diesem Prinzip keine verallgemeinerungsfähigen Schlüsse für Straftaten zu ziehen, die nicht in den koordinierten Bereich der Richtlinie fallen. Abseits des koordinierten Bereichs, also insbesondere außerhalb der Regelungen über das Verhalten des Diensteanbieters und seine Verantwortlichkeit (Art. 2 lit. h ECRL), greifen nur die oben dargestellten allgemeinen Grundsätze.[582]

---

[579] Für eine Zurechnung *Spindler*, in: Spindler/Schmitz/Geis, TDG, § 4 TDG, Rn. 13; dagegen wohl *Altenhain*, in: Zieschang/Hilgendorf/Laubenthal, Strafrecht und Kriminalität in Europa, S. 107, 124 f.

[580] *Altenhain*, in: Zieschang/Hilgendorf/Laubenthal, Strafrecht und Kriminalität in Europa, S. 107, 124 f.

[581] *Schwarzenegger*, in: Plöckinger/Duursma/Mayrhofer, Internetrecht, S. 395, 423 (für Österreich).

[582] Siehe hierzu die Ausführungen unter Teil 2, II.A.–C.

B. Verhältnis von Strafanwendungsrecht und Herkunftslandprinzip

Zu klären bleibt noch das Verhältnis des deutschen internationalen Strafanwendungsrechts zu dem nach der ECRL ins nationale Recht umgesetzten Herkunftslandprinzip. Der Rechtsanwender könnte zunächst das deutsche Strafanwendungsrecht zu prüfen haben und bei einer ausländischen Niederlassung die an sich einschlägige deutsche Strafnorm unbeachtet lassen. Gegen diese Reihenfolge der Untersuchung spricht jedoch, dass das Herkunftslandprinzip die inhaltsreichere und aktuellere Regelung für Konstellationen enthält, die in den koordinierten Bereich fallen. Setzt der Gesetzgeber wie beim Herkunftslandprinzip zudem zwingende Vorgaben einer Richtlinie in nationales Recht um, so genießt auch der nationale Umsetzungsakt Anwendungsvorrang vor sonstigem innerstaatlichem Recht, wenn mit Letzterem ein Konflikt besteht.[583] Im koordinierten Bereich kann sich der betroffene Diensteanbieter also unmittelbar auf das Herkunftslandprinzip berufen und damit auf die grundsätzlich ausschließliche Geltung des Rechts an seinem Niederlassungsort. Das bedeutet allerdings nicht zugleich, dass die nationalen Strafgerichte nunmehr ausländisches Strafrecht anzuwenden hätten. Weder der Richtlinie noch dem Umsetzungsakt sind Hinweise darauf zu entnehmen, dass das Herkunftslandprinzip eine Kollisionsnorm darstellt.[584] Gleiches gilt für die Grundfreiheiten des EU-Vertrags und der Fernsehrichtlinie,[585] auf die das Herkunftslandprinzip der E-Commerce-Richtlinie zurückgeht. Das Prinzip ist desgleichen kein Bestandteil des Strafanwendungsrechts, sondern vielmehr eine Regelung sui generis, über die der ausländische Diensteanbieter sein Handeln im Einzelfall rechtfertigen kann. Dem Herkunftslandprinzip kommt in Konstellationen eines Normwiderspruchs also Vorrang vor der Anwendung der Regelungen des internationalen deutschen Strafrechts zu.

Ist folglich vorab zu prüfen, ob deutsches Recht nach dem Herkunftslandprinzip angewendet werden kann, fragt sich, ob in einem zweiten Schritt weiterhin noch seine Anwendbarkeit nach nationalem internationalem Strafrecht zu untersuchen bleibt oder aber, ob das Herkunftslandprinzip das deutsche materielle Strafrecht direkt zur Anwendung bringt, ohne dass es dabei auf das nationale Strafanwendungsrecht ankäme.[586]

Nach seinem Wortlaut differenziert das Herkunftslandprinzip für Konstellationen, in denen das Recht eines Mitgliedstaates nicht ausgeschlossen werden soll,

---

[583] BVerfG NVwZ 2004, 1346, 1346 f.; BVerwG NVwZ 2005, 1178, 1181 (beide auf den nationalen Grundrechtsschutz bezogen); *Masing*, NJW 2006, 264, 265.

[584] *Schwarzenegger*, in: Plöckinger/Duursma/Mayrhofer, Internetrecht, S. 395, 423 (für Österreich); *Zöchbauer*, ebenda, S. 435, 440 (für Österreich).

[585] *Schmidt*, Gefahrenabwehrmaßnahmen im Internet, S. 313.

[586] Zu letzterer Fragestellung *Satzger*, CR 2001, 109, 117; *Spindler*, in: Spindler/Schmitz/Geis, TDG, § 4 TDG, Rn. 70.

nicht zwischen einzelnen Normen dieses Mitgliedstaates. So soll etwa nach Art. 3 Abs. 1 ECRL der Herkunftsstaat die Beachtung seiner innerstaatlichen Vorschriften sicherstellen. Auch die Einzelfallausnahmekompetenz nach Art. 3 Abs. 4 ECRL verweist auf keine bestimmte Norm, sondern stellt den mit den nationalen Normen verfolgten Zweck heraus.

In den Erwägungsgründen zur Richtlinie und der Begründung des Gesetzgebers zur nationalen Umsetzungsnorm finden sich gleichfalls keine Anhaltspunkte für eine einschränkende Verweisung nur auf das materielle Strafrecht. Lediglich für den Bereich des Zivilrechts macht der Richtliniengeber Aussagen über das internationale Privatrecht. Nach Erwägungsgrund 23 zielt die Richtlinie nicht darauf ab, zusätzliche Regeln im Bereich des internationalen Privatrechts für das anwendbare Recht zu schaffen. Die Vorschriften des anwendbaren Rechts, die durch Regeln des internationalen Privatrechts bestimmt seien, dürften die Freiheit zur Erbringung von Diensten der Informationsgesellschaft im Sinne der Richtlinie jedoch nicht einschränken.

Im Bereich des Zivilrechts ist daher ein heftiger Streit darüber entbrannt, ob das Herkunftslandprinzip auch auf das nationale Kollisionsrecht verweist[587] oder nur eingeschränkt auf das nationale materielle Sachrecht Bezug nimmt.[588] Hintergrund des Streits ist das Problem, dass mit der Einbeziehung deutschen internationalen Privatrechts in den Verweis des Herkunftslandprinzips eine Ungewissheit des Rechtsanwenders über das einschlägige Recht einhergeht, obwohl die ECRL gerade die Einfachheit und Klarheit der Rechtsanwendung erleichtern will.[589] Dieser Streitpunkt ist im Strafrecht jedoch von geringerer Bedeutung, da dieses kein dem internationalen Privatrecht – Art. 3 ff. EGBGB – vergleichbares Kollisionsrecht kennt.[590] Die §§ 3–7, 9 StGB sind gerade keine auf die Festlegung des *einen* anwendbaren Rechts abzielende Kollisionsnormen. Sie bestimmen vielmehr einseitig allein die Anwendbarkeit deutschen Strafrechts und bedingen hierdurch mittelbar die Verdrängung ausländischen Strafrechts.[591] Nach deutschem internationalem Strafrecht wird also nur geprüft, ob deutsches Recht auf die jeweilige Konstellation anwendbar ist, und nicht, welches sonstige nationale Recht Anwendung findet, sodass der Rechtsanwender nicht plötzlich mit einer neuen Rechtsordnung konfrontiert wird.

---

[587] *Fezer/Koos*, IPRax 2000, 349, 354; *Mankowski*, GRURInt. 1999, 909, 914 ff. (anders aber in ZVglRWiss 100 (2001), 137, 152 f.) je m.w.N.

[588] *Dethloff*, JZ 2000, 179, 181; *Mankowski*, ZVglRWiss 100 (2001), 137, 152 f. (anders aber in GRURInt. 1999, 909, 915 ff.; 921); *Ohly*, GRURInt. 2001, 899, 905; *Spindler*, in: Spindler/Schmitz/Geis, TDG, § 4, Rn. 23; *Tettenborn* et al., Beilage Nr. 10 zu BB 2001, 1, 10 je m.w.N.

[589] Siehe Erwägungsgründe 5–7 ECRL, ABl. EG 2000, Nr. L 178, S. 1 f.

[590] A.A. *Spindler*, in: Spindler/Schmitz/Geis, TDG, § 4 TDG, Rn. 70.

[591] *Fischer*, StGB, Vor §§ 3–7, Rn. 1; *Lackner/Kühl*, StGB, Vor §§ 3–7, Rn. 1; *Satzger*, Internationales und Europäisches Strafrecht, § 3, Rn. 4.

Die grundsätzliche Funktionsweise des Herkunftslandprinzips – der gegenseitigen Anerkennung nationaler Regelungen durch die anderen Mitgliedstaaten – spricht ebenfalls dafür, den Verweis auf das innerstaatliche Recht des Niederlassungsstaates ohne Beschränkung auf das materielle Strafrecht zu interpretieren. Die gegenseitige Anerkennung unter den Mitgliedstaaten bedeutet aus völkerrechtlicher Sicht ein durch den Binnenmarkt überhöhtes Abwehrinteresse des Herkunftsstaates gegenüber dem Eingriffsinteresse der übrigen Mitgliedstaaten. Ist also durch die Koordinierung unter den Mitgliedstaaten der Wille des Herkunftsstaates zum entscheidenden erklärt, so muss auch sein Wille respektiert werden, einen bestimmten Sachverhalt nicht seinen Gesetzen zu unterwerfen. Diese Gefahr hat der Richtliniengeber gesehen und ist ihr mit einem Hinweis auf die allgemeine Verantwortung des Herkunftsstaates gegenüber der Gemeinschaft in Erwägungsgrund 22 und einem Verfahren der Zusammenarbeit in Art. 19 ECRL entgegengetreten. Aus Art. 20 ECRL geht zudem nicht hervor, dass die Herkunftsländer zur durchgängigen Sicherung der Anwendung ihres materiellen Rechts verpflichtet sein sollen, sondern nur, dass sie das im Zuge der Richtlinienumsetzung erlassene Recht durchsetzen müssen.

Da weder der Wortlaut noch die Systematik oder der Sinn und Zweck für eine das Strafanwendungsrecht ausschließende Verweisung des Herkunftslandprinzips sprechen und der in den Begründungen niedergelegte Wille des Richtliniengebers sowie der nationalen Gesetzgeber sich nicht zu diesem Problem positionieren, ist für den Bereich des Strafrechts anzunehmen, dass das Strafanwendungsrecht mit in den Regelungsbereich des Herkunftslandprinzips fällt. Ist nach den Regelungen des Herkunftslandprinzips Deutschland zuständig, muss sich der Rechtsanwender in einem zweiten Schritt fragen, ob die Fallkonstellation nach deutschem internationalem Strafrecht zur Anwendung des nationalen Strafrechts führt. Insoweit wird auf die Ausführungen unter B.II. verwiesen.

IV. Resümee

Die vor jeder Aufnahme von Ermittlungen von den Strafverfolgungsbehörden zu beantwortende Frage nach ihrer Zuständigkeit ist abhängig von der Anwendbarkeit deutschen Strafrechts im konkreten Einzelfall und in Konstellationen mit Auslandsbezügen häufig besonders schwierig. Aufgrund des regelmäßig bereits technisch bedingten grenzüberschreitenden Informationsaustauschs im Internet ist die Antwort auf die Frage nach der Zuständigkeit der Strafverfolgungsbehörden in Fällen von im Internet begangenen Straftaten besonders brisant. Zu unterscheiden ist zwischen Inlandstaten mit Auslandsbezug und reinen Auslandstaten. Letztere weisen regelmäßig keine internetspezifischen Besonderheiten auf, sodass das deutsche Strafrecht unter Berücksichtigung der §§ 5, 6, 7 StGB bei Vorliegen der entspre-

chenden Voraussetzungen anwendbar ist und die Strafverfolgungsbehörden in diesen Fällen ihre Ermittlungen aufnehmen müssen.

Anders ist die Sachlage bei Inlandstaten mit Auslandsbezug. In diesen Fällen ist das deutsche Strafrecht nach dem Territorialitätsprinzip anwendbar, wenn der Täter in Deutschland körperlich gehandelt hat oder ein tatbestandlicher Erfolg in Deutschland eingetreten ist. Ein Erfolg i.S.d. § 9 Abs. 1, 3. Var. StGB ist unter Berücksichtigung des Völkerrechts durch Abwägung der Interessen von eingreifendem und abwehrendem Staat zu ermitteln und liegt nur bei Eintritt von tatbestandsmäßigen Verletzungen und konkreten Gefährdungen vor. Einer über dieses Auslegungsergebnis hinausgehenden weiteren Einschränkung der Strafanwendungsvorschriften bedarf es aus völkerrechtlicher Sicht nicht. Allein rechtspolitische Erwägungen können im Wege einer einschränkenden gesetzlichen Neuregelung zu einer weitergehenden Begrenzung führen.

In Sonderkonstellationen, in denen ein im EU-Ausland niedergelassener geschäftsmäßig handelnder Diensteanbieter einen Sachverhalt verwirklicht, der in den koordinierten Bereich der E-Commerce-Richtlinie fällt, ist in Abkehr zu den vorgenannten Grundsätzen bei Inlandstaten mit Auslandsbezug das sogenannte Herkunftslandprinzip beachtlich. Der Diensteanbieter hat nach diesem Prinzip grundsätzlich nur das an seinem Niederlassungssitz geltende Recht zu berücksichtigen. Die als Einzelfallausnahme konzipierte Vorschrift des § 3 Abs. 5 TMG führt nicht zu einem generellen Ausschluss des Strafrechts aus dem Anwendungsbereich des Herkunftslandprinzips. Soweit nach dem Prinzip deutsches Recht zur Anwendung kommt, bleibt in einem zweiten Schritt jedoch weiterhin zu überprüfen, ob nach nationalem Strafanwendungsrecht deutsches Recht anwendbar ist.

Teil 3

Territoriale Reichweite der Ermittlungsbefugnisse deutscher Strafverfolger

Von der vorstehend beantworteten Frage nach der Kompetenz zur Anwendung des nationalen Strafrechts auf Internetsachverhalte mit Auslandsbezug streng zu unterscheiden[1] ist die nach der sogenannten Ausübungskompetenz eines Staates für Ermittlungsmaßnahmen. Nach Letzterer bestimmt sich, ob und inwieweit eigene Ermittlungsbehörden Hoheitsakte auf fremdem Staatsgebiet vornehmen dürfen oder aber die Beamten zu Hoheitsakten berechtigt sind, deren Auswirkungen sich nicht auf das eigene Staatsgebiet beschränken, wenngleich die ermittelnden Beamten ihr Territorium zu keinem Zeitpunkt physisch verlassen haben.

I. Allgemeine Grenzen der Ausübungskompetenz

Die Bestimmung der territorialen Reichweite der Befugnisse nationaler Strafverfolger ist besonders für die Ermittlungsarbeit im Internet virulent, weil die Fälle zunehmen, in denen Beweismaterial im Ausland zu finden ist.[2] Gleichwohl ist heute noch weitgehend ungeklärt, inwieweit die Strafverfolger mit den ihnen zur Verfügung gestellten Ermittlungsbefugnissen den neuartigen Kriminalitätsphänomenen im „Netz der Netze" angemessen entgegentreten können.

Klassische Rechtshilfeverfahren sind zumeist derart zeitaufwändig, dass eine Vielzahl von digitalen Spuren für Beweiszwecke schon verloren ist,[3] wenn der ersuchte Staat – sofern er überhaupt tätig wird – beginnt, die Beweise zu sichern. Selbst unter Berücksichtigung der zum Teil bereits in Gang gesetzten Beschleunigung der Rechtshilfe, insbesondere durch die Einrichtung eines sogenannten 24/7-Netzwerks, für welches die sich beteiligenden Staaten jeweils eine Kontaktstelle benennen, „die an sieben Wochentagen 24 Stunden täglich zur Verfügung steht, um für Zwecke der Ermittlungen oder Verfahren in Bezug auf Straftaten in

---

[1] *Spang-Hanssen*, Cyberspace & International Law, S. 270 f.

[2] BMI/BMJ, Erster Periodischer Sicherheitsbericht, S. 203; *Gercke*, StraFo 2009, 271, 271; *Seitz*, Strafverfolgungsmaßnahmen im Internet, S. 355.

[3] Z.B. weil Verkehrsdaten nur für eine bestimmte Zeit gespeichert werden dürfen oder weil der Täter die Daten nur für eine kurze Zeitspanne zugänglich macht, vgl. auch *Gercke*, MMR 2008, 291, 293 ff.; *ders.*, StraFo 2009, 271, 272; *Meininghaus*, Zugriff auf E-Mails, S. 178; *Seitz*, Strafverfolgungsmaßnahmen im Internet, S. 356.

Zusammenhang mit Computersystemen und -daten oder für die Erhebung von Beweismaterial in elektronischer Form für eine Straftat unverzüglich für Unterstützung zu sorgen“,[4] ist nicht immer eine hinreichend schnelle Bearbeitung der Anträge gewährleistet. Die Schnelligkeit der Veränderung der Beweislage bei Computerdaten in globalen Netzwerken wirft daher die Frage auf, in welcher Weise die Strafverfolger bereits abseits des Rechtshilfewegs den Herausforderungen der Verfolgung grenzüberschreitender Datennetzkriminalität erfolgreich begegnen können.

Das deutsche Strafprozessrecht unterscheidet nicht ausdrücklich zwischen im Inland belegenen Beweismitteln und solchen im Ausland, sondern verlangt vielmehr von der Staatsanwaltschaft im Ermittlungsverfahren gemäß § 160 StPO und vom Gericht in der Hauptverhandlung gemäß § 244 Abs. 2 StPO eine umfassende Erforschung des wahren Sachverhalts. Auch das Internet selbst setzt den Ermittlungsmöglichkeiten der Strafverfolgungsbehörden aufgrund seiner Staatsgrenzen ignorierenden technischen Infrastruktur faktisch keine räumlichen Grenzen. Dennoch sind die deutschen Strafverfolgungsbehörden bei ihren Ermittlungsmaßnahmen grundsätzlich auf das eigene Staatsgebiet beschränkt. Nach dem völkerrechtlichen Grundsatz der Achtung der Gebietshoheit als Ausfluss des Gebots der Achtung der souveränen Staatengleichheit[5] darf nämlich – abseits etwaiger Genehmigungen im Einzelfall, z.B. im Wege der Rechtshilfe aufgrund von völkerrechtlichen Verträgen oder genereller Ermächtigungen durch Anerkennung bestimmter Verhaltensweisen in der Staatenpraxis als rechtmäßig – kein Staat unmittelbar auf fremdes Territorium einwirken.[6] Mit anderen Worten steht jedem Staat nur auf seinem Staatsgebiet die ausschließliche, unbeschränkte und unabhängige Hoheitsgewalt zu. Er darf sich nicht anmaßen, seine Staatsgewalt auf fremdem Territorium auszuüben.[7] Daher sind alle ihm zuzurechnenden Handlungen seiner Ermittlungsbeamten im Ausland – aber auch von Privatpersonen, die als Staatsorgane auftreten und geduldet werden, sowie von Personen, die sich zwar keine Organstellung anmaßen, deren kon-

---

[4] So die Regelung des Art. 35 Abs. 1 CCC. Allerdings wurde die Einrichtung eines solchen Netzwerkes bereits 1997 durch die G8-Staaten gefordert; siehe hierzu Principles and Action Plan to Combat High-Tech Crime, No. 1 Action Plan.

[5] Siehe hierzu die Ausführungen unter Teil 1, I. und II.

[6] American Law Institute, Restatement Foreign Rel. Law 2nd, § 20, comment b, § 25; dass., vol. 1 Restatement Foreign Rel. Law 3rd, § 432, comment b; *Daum*, Grenzverletzungen und Völkerrecht, S. 37 f.; *Doehring*, Völkerrecht, Rn. 88 f.; *Geiger*, Grundgesetz und Völkerrecht mit Europarecht, S. 247 f., 312; *Ipsen*, Völkerrecht, § 23, Rn. 67, 69; *Proelß*, in: Graf Vitzthum/Bothe, Völkerrecht, 5. Abschnitt, Rn. 16; *Rehbinder*, Extraterritoriale Wirkungen des deutschen Kartellrechts, S. 394; *Rudolf*, in: BerDGesVölkR 11, S. 7, 33; *Sahlfeld*, Die Veränderung der Ausübung von Staatsgewalt, S. 75; *Schwörer*, wistra 2009, 452, 453; *Siegrist*, Hoheitsakte auf fremdem Staatsgebiet, S. 10 f.; *Spang-Hanssen*, Cyberspace & International Law, S. 267; *Stein/v. Buttlar*, Völkerrecht, Rn. 537.

[7] Vgl. American Law Institute, vol. 1 Restatement Foreign Rel. Law 3rd, § 433 Abs. 1a; *Germann*, Gefahrenabwehr und Strafverfolgung im Internet, S. 642; *Okresek*, ÖZöRV 35 (1985), 325, 332; *Schmidt*, Gefahrenabwehrmaßnahmen im Internet, S. 258; *Siegrist*, Hoheitsakte auf fremdem Staatsgebiet, S. 11; *Soiné*, NStZ 1997, 166, 167; *Spang-Hanssen*, Cyberspace & International Law, S. 273.

krete Handlung aber gleichwohl vom Heimatstaat gewünscht ist – generell völkerrechtswidrig,[8] weil diese Handlungen die Souveränitätsrechte des fremden Staates verletzen.

Auf der anderen Seite gestattet das Völkerrecht indes jedem Staat, Hoheitsakte überall dort zu setzen, wo weder ein anderer Staat seine territoriale Hoheitsgewalt ausübt noch eine völkerrechtliche Verbotsnorm besteht. Einer konkreten völkerrechtlichen Erlaubnisnorm bedarf es hierzu folglich nicht.[9]

Im Fokus der Untersuchung steht die Prüfung der völkerrechtlichen Zulässigkeit einzelner in Betracht kommender extraterritorialer Hoheitsakte im Internet (unter II.). Führt die Ermittlungsmaßnahme zu einem Eingriff in die Gebietshoheit fremder Staaten, können die Strafverfolgungsbehörden die Maßnahme abseits allgemeiner Anerkennung in der Staatenpraxis, spezieller Befugnisnormen oder Einwilligung im Einzelfall nur im Wege der internationalen Rechtshilfe vornehmen bzw. durch die Ermittlungsbehörden der betroffenen Staaten vornehmen lassen (unter III.). Ist die Ermittlungsmaßnahme auch nicht in der Staatenpraxis allgemein als völkerrechtsgemäß anerkannt, so unterliegen die unter Verstoß gegen das Gebot der Achtung der fremden Gebietshoheit gewonnenen Beweismittel regelmäßig einem Beweisverwertungsverbot (unter IV.).

II. Zulässigkeit extraterritorialer Ermittlungshandlungen

Hoheitsakte auf dem eigenen Staatsgebiet unterliegen, auch soweit sie in fremdes Staatsgebiet hineinwirken, nicht generell dem Verdikt der Völkerrechtswidrigkeit. Sie sind vielmehr nur dann unzulässig, wenn sie den Tatbestand eines völkerrechtlichen Delikts verwirklichen.[10]

Sowohl die innerstaatliche Kommunikation über das Internet (trotz potentiellen Auslandsbezugs) (nachfolgend unter A.) als auch der Abruf frei zugänglicher, aber im Ausland gespeicherter Daten (unter D.2.), sind völkerrechtlich kraft Anerkennung durch die Staatenpraxis zulässig. Dagegen greifen die Strafverfolgungsbehörden mangels Rechtfertigung grundsätzlich völkerrechtswidrig in die Gebietshoheit fremder Staaten ein, wenn sie den Fernmeldeverkehr mit ausländischen Nutzern

---

[8] *Bertele*, Souveränität und Verfahrensrecht, S. 89 f.; *Gleß*, NStZ 2000, 57; *Nagel*, Beweisaufnahme im Ausland, S. 18 f.; *Rehbinder*, Extraterritoriale Wirkungen des deutschen Kartellrechts, S. 394; *Schnigula*, DRiZ 1984, 177.

[9] *Siegrist*, Hoheitsakte auf fremdem Staatsgebiet, S. 24; *Verdross/Simma*, Universelles Völkerrecht, § 1022.

[10] *Schlochauer*, Die extraterritoriale Wirkung von Hoheitsakten, S. 41; *v. Münch*, Das völkerrechtliche Delikt, S. 65; zu weiteren Ausführungen siehe bereits oben unter Teil 1, IV.

überwachen, wenn diese Kommunikationsbeziehung gezielt am ausländischen Partner bzw. dem zu ihm führenden Telekommunikationsweg (sog. Auslandskopfüberwachung) ansetzt (unter B.). Gleiches gilt für Individualkommunikationen mit im Ausland befindlichen Nutzern über das Internet (unter C.). Auch der Abruf von im Ausland gespeicherten zugangsbeschränkten Daten erweist sich, abseits des Zugriffs mit Zustimmung des Berechtigten, als rechtswidrig, wenn für den Einzelfall keine Erlaubnis des betroffenen Staates vorliegt oder das Eingriffsinteresse des extraterritorial handelnden Staates hinter dem des betroffenen Staates zurückbleibt (unter D.3.). Der Upload von Daten auf Server im Inland, insbesondere zur Fahndung, ist dagegen ohne spezielle Ermächtigungsgrundlage zulässig und nur dann völkerrechtswidrig, wenn die Fahndung gezielt auf die Suche nach einer sich im Ausland aufhaltenden Person ausgerichtet ist und folglich vornehmlich Internetnutzer im Ausland anspricht. Starten die Strafverfolger bereits ihren Fahndungsaufruf auf Servern im Ausland, greifen sie ebenfalls rechtswidrig in die Gebietshoheit fremder Staaten ein (unter E.).

A. Innerstaatliche Kommunikation

Nutzen die Strafverfolgungsbehörden das Internet für ihre Ermittlungen, könnte schon die bloße Kommunikation über das Computernetz aufgrund der grenzüberschreitenden Übertragungswege der Daten ohne spezielle Erlaubnisnorm völkerrechtswidrig sein.

1. Eingriff in die Gebietshoheit fremder Staaten

Bereits das Kommunizieren zweier Nutzer, die sich in ein und demselben Staat aufhalten, über das Internet kann nämlich Berührungspunkte zu anderen Staaten aufweisen, weil die Übertragung der Daten im Internet im Wesentlichen nach Effektivitätsgesichtspunkten erfolgt und daher nur eingeschränkt vorhersehbar ist.[11] Selbst eine innerstaatliche Kommunikation kann daher über Router im Ausland geleitet werden. Würde die systemimmanent zufällige Leitung der Kommunikationsdaten über Ländergrenzen hinweg aufgrund ihres Auslandsbezugs zwangsläufig zur Verletzung des Völkerrechts führen, wäre jede Verwendung des Internet seitens staatlicher Stellen potentiell völkerrechtswidrig. Dass die bloße Kommunikation über das globale Computernetz ohne Ausübung von Zwang erfolgt und die Beamten eine Auslandsberührung nicht zielgerichtet herbeiführen, spricht – wie bereits zuvor näher erörtert[12] – nicht zwingend gegen einen Ausschluss völker-

---

[11] *Germann*, Gefahrenabwehr und Strafverfolgung im Internet, S. 64 f.; *Hunt/Thompson*, Windows NT TCP/IP Netzwerk-Administration, S. 13.

[12] Siehe hierzu die näheren Ausführungen unter Teil 1, III.

rechtswidrigen hoheitlichen Handelns mit Wirkung auf fremdem Staatsgebiet, da ein hoheitliches Handeln keine Anwendung von Zwang erfordert und ein völkerrechtliches Delikt nicht zwingend ein Verschulden voraussetzt. Auch eine Unterscheidung in einen hoheitlich geprägten Datenabruf und eine nicht hoheitliche Datenübertragung[13] führt nicht weiter, weil dabei ein einheitlicher technischer Vorgang unnatürlich aufgespalten würde. Einem Flug über fremdes Staatsterritorium kann schließlich auch nicht mit dem Argument, der bloße Überflug verfolge kein konkret hoheitliches Ziel, der Charakter einer Verletzung der Gebietshoheit abgesprochen werden. Zudem beruht jede Übertragung von Daten auf einem vorhergehenden Abruf, ist also von diesem kausal veranlasst. Tatsächlich liegt folglich eine Einwirkung auf das Territorium fremder Staaten vor, wenn die Daten über Rechner im Ausland transportiert werden, weil die Strafverfolgungsbehörden hiermit Rechnerprozesse auf fremdem Staatsgebiet in Gang setzen.

2. Ausnahmslose Rechtfertigung des Eingriffs

Der Eingriff in das Gebot der Achtung der Gebietshoheit ist hier aber gerechtfertigt, sodass die Datenübertragung keinen unzulässigen extraterritorialen Hoheitsakt darstellt. Die kommunizierenden Beamten können den Weg der von ihnen ausgetauschten Daten nämlich nicht immer beeinflussen; die Auslandsberührung ist in diesen Fällen vornehmlich durch die technische Infrastruktur des Computernetzes bedingt. Eine unmittelbare Beeinträchtigung des fremden Hoheitsgebiets in Form des gezielten Zugriffs auf fremdes Staatsgebiet liegt nicht vor. Die Verwendung des Internet zu Kommunikationszwecken dient in den Fällen innerstaatlicher Kommunikation letztlich allein der Regelung von Verhältnissen im Inland. Die u.U. gegebene extraterritoriale Wirkung auf dem Gebiet eines fremden Staates ist weder im konkreten Einzelfall immer bekannt noch bezweckt und intensiv, sondern stellt lediglich einen mit zumutbaren Mitteln nicht abzustellenden Reflex dar, der einzig durch ausnahmsloses Beenden der Nutzung des Internet zu beseitigen wäre. Eine solche Einschränkung der staatlichen Hoheitsgewalt, die sich auf die Regelung innerstaatlicher Verhältnisse bezieht, auf dem eigenen Territorium stattfindet und nur unerhebliche Auswirkungen auf fremdes Territorium mit sich bringt, verlangt jedoch auch das Völkerrecht den Staaten nicht ab.[14]

So waren sich die Staaten beispielsweise bereits bei der Ausstrahlung von Radiowellen einig, dass dies auch über Staatsgrenzen hinweg grundsätzlich völkerrechtlich zulässig sei,[15] zumal die Ausbreitung der Funkwellen technisch bedingt

---

[13] So *Valerius*, Ermittlungen der Strafverfolgungsbehörden, S. 153 f.

[14] *Germann*, Gefahrenabwehr und Strafverfolgung im Internet, S. 643; ähnlich *Schmidt*, Gefahrenabwehrmaßnahmen im Internet, S. 259, für Sperrverfügungen gegenüber Providern in Deutschland.

[15] *Blumenwitz*, in: Gepperth, Freedom of Information, S. 34 ff.; *Engel*, RabelsZ 49 (1985), 90, 100; *Frowein*, in: BerDGesVölkR 19, S. 1, 8 f.; *Simma*, in: BerDGesVölkR 19, S. 39, 48 f.

nicht ohne Weiteres an der Landesgrenze eines Staates abgebrochen werden kann. Im Zuge der technischen Weiterentwicklung hin zum Satellitendirektfernsehen stellten die Staaten die Sendefreiheit nur insoweit infrage, als sie mit einer zielgerichteten Ausstrahlung von Sendungen auf fremdes Staatsgebiet eine politische Einflussnahme befürchteten, der sie nicht mehr in zumutbarem wirtschaftlichem und technischem Umfang durch Störsender begegnen konnten.[16] Nach Verteilung der Frequenzbereiche einigten sich die Staaten jedoch gleichwohl auf die grundsätzliche Zulässigkeit der Ausstrahlung von Satellitendirektfernsehen.[17] Zwar stand bei der Auseinandersetzung über die Verwendung der grenzüberschreitenden Rundfunk- und Satellitentechnik zumeist das Menschenrecht der Freiheit der Meinungsäußerung (Art. 10 EMRK)[18] im Mittelpunkt der Diskussionen,[19] auf welches sich die Strafverfolgungsbehörden bei ihrer Ermittlungsarbeit nicht beziehen können.[20] Die grundsätzliche Anerkennung der Zulässigkeit von technikbedingten Grenzüberschreitungen durch elektromagnetische Wellen in der Staatenpraxis vollzog sich aber unabhängig von der Berufung auf dieses grundlegende Menschenrecht.

Daraus folgt für die Verwendung des Internet zu innerstaatlichen Kommunikationszwecken, dass der Transport der Daten, der weder auf eine Grenzüberschreitung gerichtet ist noch einen im Ausland befindlichen Kommunikationspartner erreichen soll, aufgrund der Anerkennung der Staaten und der gelebten Staatenpraxis (in der wohl jeder Staat durch seine Bediensteten selbst das weltweite Computernetz zur Kommunikation nutzt) nicht völkerrechtswidrig ist. Dies gilt auch und insbesondere für leitungsgebundene Übertragungen von Daten.[21] Indiz hierfür ist, dass fast alle Staaten der Welt mit der Unterzeichnung und Ratifizierung des Inter-

---

[16] *Frowein*, in: BerDGesVölkR 19, S. 1, 10 ff.; siehe des Weiteren zur Entwicklung *Engel*, RabelsZ 49 (1985), 90, 91 ff., 101 ff.

[17] *Frowein*, in: BerDGesVölkR 19, S. 1, 11 f.

[18] Art. 10 EMRK lautet: „(1) Jede Person hat das Recht auf freie Meinungsäußerung. Dieses Recht schließt die Meinungsfreiheit und die Freiheit ein, Informationen und Ideen ohne behördliche Eingriffe und ohne Rücksicht auf Staatsgrenzen zu empfangen und weiterzugeben. Dieser Artikel hindert die Staaten nicht, für Radio-, Fernseh- oder Kinounternehmen eine Genehmigung vorzuschreiben. (2) Die Ausübung dieser Freiheiten ist mit Pflichten und Verantwortung verbunden; sie kann daher Formvorschriften, Bedingungen, Einschränkungen oder Strafdrohungen unterworfen werden, die gesetzlich vorgesehen und in einer demokratischen Gesellschaft notwendig sind für die nationale Sicherheit, die territoriale Unversehrtheit oder die öffentliche Sicherheit, zur Aufrechterhaltung der Ordnung oder zur Verhütung von Straftaten, zum Schutz der Gesundheit oder der Moral, zum Schutz des guten Rufes oder der Rechte anderer, zur Verhinderung der Verbreitung vertraulicher Informationen oder zur Wahrung der Autorität und der Unparteilichkeit der Rechtsprechung."

[19] *Blumenwitz*, in: Gepperth, Freedom of Information, S. 13 ff.; *Simma*, in: BerDGesVölkR 19, S. 39, 49 ff.

[20] *Germann*, Gefahrenabwehr und Strafverfolgung im Internet, S. 643 f.

[21] Ebenda, S. 645.

nationalen Fernmeldevertrags (IFV)[22] bzw. mit dem Beitritt zu Konstitution und Konvention der Internationalen Fernmeldeunion,[23] die an die Stelle des IFV treten,[24] jedem beigetretenen Staat das Recht zugestanden haben, über die internationalen öffentlichen Fernmeldedienste Nachrichten auszutauschen.[25] Die Völkerrechtmäßigkeit der innerstaatlichen Kommunikation unter Inanspruchnahme im Ausland ansässiger Telekommunikationsunternehmen ergibt sich zwar nicht unmittelbar aus den angesprochenen Regeln, weil diese nur das „Wie" des Nachrichtenaustauschs regeln, aber der Beitritt der Staaten zu den Rechtsakten erklärt zumindest deren Bereitschaft zur Duldung des Nachrichtenaustauschs.

Die Regelungen des Weltpostvertrags (WPostVertr)[26], der in Art. 1 Abs. 1[27] die Freiheit des Durchgangs von Sendungen im gesamten Weltpostvereinsgebiet gewährleistet, können indes nicht zur Begründung einer Staatenpraxis bei der Datenübermittlung herangezogen werden,[28] da der Transport der Daten über Computernetze fremder Staaten nicht wie im Postverkehr vorhersehbar fremdes Staatsgebiet berührt und nur unkörperliche Objekte betrifft.[29]

B. Inländische Fernmeldeverkehrsüberwachung mit Beteiligung ausländischer Nutzer

Ein völkerrechtswidriger Eingriff in die Gebietshoheit fremder Staaten könnte aber vorliegen, wenn die Strafverfolgungsbehörden gezielt Kommunikations-

---

[22] In Deutschland umgesetzt durch das Gesetz zu dem Internationalen Fernmeldevertrag vom 6.11.1982 (Internationaler Fernmeldevertrag-Gesetz = IntFernmeldVertrG) vom 4.3.1985, BGBl. 1985 II, S. 425 ff., im Anschluss hieran ist der Internationale Fernmeldevertrag selbst abgedruckt.

[23] Umgesetzt durch das Gesetz zu der Konstitution und der Konvention der Internationalen Fernmeldeunion vom 22.12.1992 sowie den Änderungen der Konstitution und der Konvention der Internationalen Fernmeldeunion vom 14.10.1994, BGBl. II 1996, S. 1306 ff.; zu den Verträgen siehe BGBl. II 1996, S. 1316 ff. und S. 1340 ff.

[24] Die Regelungen des IFV gelten nur noch im Verhältnis zu den Staaten, die nicht der Konstitution der internationalen Fernmeldeunion und der Konvention der internationalen Fernmeldeunion vom 22.12.1992 beigetreten sind.

[25] Art. 18 Satz 1 IFV bzw. Art. 39, 40 Konvention der Internationalen Fernmeldeunion.

[26] Weltpostvertrag vom 14. September 1994, BGBl. II 1998, S. 2135 ff.

[27] Art. 1 Abs. 1 WPostVertr lautet: „Die Freiheit des Durchgangs, die in Artikel 1 der Satzung als Grundsatz verankert ist, verpflichtet jede Postverwaltung, die ihr von einer anderen Verwaltung übergebenen Kartenschlüsse und Briefsendungen des offenen Durchgangs stets auf dem schnellsten Wege weiterzuleiten, den sie für ihre eigenen Sendungen benutzt. Diese Verpflichtung gilt auch für Luftpostbriefsendungen, unabhängig davon, ob die vermittelnden Postverwaltungen an ihrer Weiterleitung beteiligt sind oder nicht. […]."

[28] Sie regeln zudem ebenso nur das „Wie" der Zustellung, die Zustellung selbst steht unter dem Vorbehalt, dass die Staaten sich hierzu bereiterklären (Art. 38 WPostVertr). Siehe hierzu auch *Bertele*, Souveränität und Verfahrensrecht, S. 98, Fn. 74.

[29] Anders wohl *Determann*, Kommunikationsfreiheit im Internet, S. 148.

vorgänge im Internet überwachen, die einen Auslandsbezug aufweisen. Hierzu müssen die Ermittlungsbeamten heute kein fremdes Staatsgebiet mehr betreten; es genügt, wenn sie sich ausschließlich im Inland belegener technischer Knotenpunkte bedienen. Diese Form der Überwachung stellt daher keinen Hoheitsakt auf fremdem Staatsgebiet dar, sondern kann lediglich ein extraterritorialer hoheitlicher Akt sein.

Bereits wegen dieser Erkenntnis lehnt ein Teil der Literatur bei der Überwachung mit Auslandsbezug ohne physische Einflussnahme auf fremdes Territorium einen Eingriff in die territoriale Integrität fremder Staaten ab und sieht die Problematik aus völkerrechtlicher Sicht als gelöst an.[30] Hierbei übersehen diese Vertreter freilich, dass selbst Hoheitsakte, die sich lediglich im Ausland auswirken, völkerrechtswidrig sein können. Entscheidend ist nämlich nicht allein der Ort der Vornahme der Ermittlungsmaßnahme, sondern auch der Ort, an dem Auswirkungen dieser Maßnahme eintreten. Das fremde Staatsgebiet wird zwar hier nicht unmittelbar verletzt, aber der Hoheitsakt könnte in seinen Wirkungen einem Hoheitsakt auf fremdem Staatsgebiet gleichkommen.[31]

1. Technischer Vergleichsfall: Auslandskopfüberwachung

Während die Überwachung der klassischen Telefonie mit dem Ausland an den sogenannten Auslandsköpfen (also an Knotenpunkten im Inland, an denen die inländischen mit den ausländischen Telekommunikationsnetzen zusammengeschaltet werden[32]) erfolgt, ist der Telekommunikationsverkehr im Internet nicht nach diesem Modell überwachbar. Der Internetverkehr mit dem Ausland wird nämlich nicht über einige wenige Knotenpunkte, sondern über eine unübersehbare Vielzahl von Leitungen abgewickelt. Praktisch kann eine vergleichbare Überwachung des Internetverkehrs aber dadurch realisiert werden, dass die Kommunikation an den großen deutschen Knotenpunkten, z.B. dem Deutschen Commercial Internet Exchange (DECIX) in Frankfurt/Main, erfasst wird.

Wie bei der Auslandskopfüberwachung geht es den Strafverfolgungsbehörden auch bei der Überwachung des Internetverkehrs an den Knotenpunkten nicht primär um die Erfassung der Kommunikationsinhalte, sondern vielmehr um die Iden-

---

[30] Antwort der Bundesregierung auf eine Kleine Anfrage von Abgeordneten, BT-Drucks. 15/5199, Antworten auf die Fragen 17–20, S. 5 f.; *Bär*, EDV-Beweissicherung im Strafverfahren, S. 60, Rn. 72; *Germann*, Gefahrenabwehr und Strafverfolgung im Internet, S. 654; *Soiné*, NStZ 1997, 166, 168; *Tiedemann*, CR 2005, 858, 862.

[31] Vgl. in diesem Zusammenhang bereits BVerfGE 100, 313, 363, wo der räumliche Schutzbereich des Fernmeldegeheimnisses für den Zugriff auf ausländischen Fernmeldeverkehr mit Überwachungsanlagen, die auf deutschem Boden stationiert sind, unter Berücksichtigung des Kontaktes zum Ausland erweitert wird.

[32] Zur rechtlichen Regelung in den §§ 3, 4 TKÜV i.V.m. § 110 TKG siehe *Reinel*, wistra 2006, 205, 206 f.; *Tiedemann*, CR 2005, 858, 859 ff.

tifizierung des inländischen Kommunikationspartners durch Analyse der transportierten Daten eines bestimmten ausländischen Absenders. Während diese Ermittlungsbeschränkung bei der Auslandskopfüberwachung allerdings technisch nicht zwingend ist, folgt sie bei der Überwachung des Internetverkehrs aus einer praktischen Notwendigkeit heraus, weil hier der erfasste Verkehr bereits aufgrund der variablen Routenführung im Internet höchstwahrscheinlich unvollständig ist und daher keine Rekonstruktion einzelner Inhalte zulässt. Die erlangte Kenntnis über inländische Kommunikationspartner erlaubt jedoch in einem weiteren Schritt deren Überwachung und damit die Ermittlung der dort anfallenden Inhalte. Sind danach Ermittlungsziel und Methodik der Auslandskopfüberwachung mit denen der Überwachung des Internetverkehrs mit dem Ausland vergleichbar, ergeben sich auch parallele völkerrechtliche Probleme, sodass sich die Stellungnahmen zur völkerrechtlichen Zulässigkeit einer Auslandskopfüberwachung auf die Zulässigkeit der oben skizzierten Überwachung des Internetverkehrs übertragen lassen.

2. Eingriff in die Gebietshoheit fremder Staaten

Anders als beim später noch näher zu untersuchenden Abruf von Daten im Ausland,[33] veranlassen die Strafverfolgungsbehörden bei der Überwachung zwar keinen eigenen datenrechnerischen Vorgang im Ausland, weil ein solcher bereits von einem Kommunikationspartner angestoßen wurde. Die Behörden knüpfen aber gleichwohl ihre Ermittlungen nicht nur reflexartig an im Ausland stattfindende Kommunikationsvorgänge an, wie dies bei der Überwachung von inländischen Teilnehmeranschlüssen der Fall wäre, sondern nutzen den Bezug zu einem individualisierten Drittstaat planmäßig aus.[34] Im Unterschied zur (völkerrechtlich unproblematischen, da langjährig anerkannten) Auswertung der im deutschen Staatsgebiet wahrnehmbaren undifferenzierten Kommunikationsströme,[35] wie sie bei der strategischen Überwachung des Auslandsverkehrs nach dem G 10 stattfindet,[36] verfolgt die Auslandskopfüberwachung bzw. die Verkehrserfassung an Internetknotenpunkten die gezielte Registrierung zumindest von Ausschnitten der an einem bestimmten ausländischen Teilnehmeranschluss geführten Kommunikation. Der Ausgangspunkt der Ermittlung ist also immer ein konkreter Anschluss in einem anderen Staat, sodass mit dieser Maßnahme eine (in seltenen Einzelfällen sogar

---

33 Siehe dazu unter Teil 3, II.D.

34 *Reinel*, wistra 2006, 205, 207.

35 Dazu gehören u.a. die in Westeuropa stattfindenden Auslandstelefonate, die fast ausnahmslos über Satelliten abgewickelt werden. Diese Satelliten strahlen ihre Datenströme aus technischen Gründen nicht auf ein Staatsgebiet beschränkt ab, sondern sind im gesamten versorgten Bereich – darunter eben auch Deutschland – zu empfangen.

36 BVerfGE 100, 313, 362; EGMR NJW 2007, 1433, 1433 (1. LS), 1435; *Badura*, FS Leisner, S. 403, 405; *Brunst*, Anonymität im Internet, S. 507 f.; *Gusy/Hueck*, NJ 1995, 461, 463; *Hochreiter*, Die heimliche Überwachung internationaler Telekommunikation, S. 93.

vollständige) Erfassung des Verkehrs des ausländischen Teilnehmeranschlusses einhergeht, die sonst nur im Wege der internationalen Rechtshilfe zu erreichen wäre.[37] Demzufolge sind die Auslandskopfüberwachung und ihr Gegenstück, die Überwachung der großen Internetknotenpunkte, in ihren Auswirkungen einer herkömmlichen, nicht inhaltsbezogenen Überwachung auf fremdem Staatsgebiet vergleichbar. Da diese Überwachung der Telekommunikation aber in allen Staaten traditionell hoheitlich ausgeübt wird, maßt sich der deutsche Staat ihm nicht zustehende Befugnisse an und greift folglich in die Gebietshoheit fremder Staaten ein.[38]

3. Fehlende generelle Rechtfertigung des Eingriffs

Eine Rechtfertigung, z.B. bereits aufgrund der Anerkennung dieser Art der Vorgehensweise durch die Staatengemeinschaft über einen gewissen Zeitraum, ist nicht ersichtlich. So war schon die Verpflichtung zur Leistung von Rechtshilfe durch eine Telefonüberwachung nach dem Europäischen Übereinkommen über die Rechtshilfe in Strafsachen (EURhÜbk)[39] selbst nach den Empfehlungen Nr. 85 (10) und Nr. 95 (13) des Europarates umstritten,[40] sodass sich die Europäische Union veranlasst sah, spezielle Vorschriften für grenzüberschreitende Überwachungsmaßnahmen zu entwickeln.[41] Der Abschluss von internationalen Vereinbarungen wie dem Übereinkommen über die Rechtshilfe in Strafsachen zwischen den Mitgliedstaaten der Europäischen Union vom 29.5.2000 (EU-RhÜbk)[42] zeigt also, dass die Staatenpraxis grundsätzlich von einem rechtswidrigen Eingriff in die Gebiets-

---

[37] Dies räumt auch die Bundesregierung ein, indem sie von einer Schnittmenge zwischen Auslandskopfüberwachung und Überwachung eines ausländischen Anschlusses im Wege der internationalen Rechtshilfe spricht, BT-Drucks. 15/5199, S. 5 f., Antwort auf Frage 19 der Kleinen Anfrage zum Thema Auslandskopfüberwachung, BT-Drucks. 15/5164.

[38] Im Ergebnis ebenso *Reinel*, wistra 2006, 205, 207.

[39] European Convention on Mutual Assistance in Criminal Matters (ETS No. 30), in Deutschland in Kraft getreten im Jahr 1977, BGBl. II 1964, S. 1369, 1386; BGBl. II 1976, 1799; BGBl. I 1982, 2071.

[40] Council of Europe, Recommendation No. (85) 10; ders., Recommendation No. (95) 13, Erläuternder Bericht, Tz. 195 f.; siehe auch zur Unanwendbarkeit der Recommendation No. (85) 10 auf Überwachungen bei Computernetzwerken auch ders., Recommendation No. (89) 9, Erläuternder Bericht, S. 91 f.

[41] Erläuternder Bericht zu dem Übereinkommen vom 29. Mai 2000 über die Rechtshilfe in Strafsachen zwischen den Mitgliedstaaten der Europäischen Union, ABl. EG 2000, Nr. C 379, S. 7, 20.

[42] Übereinkommen gemäß Artikel 34 des Vertrags über die Europäische Union – vom Rat erstellt – über die Rechtshilfe in Strafsachen zwischen den Mitgliedstaaten der Europäischen Union vom 29. Mai 2000, ABl. EG 2000, Nr. C 197, S. 3 ff.; BGBl. II 2005, S. 650 ff.; in Deutschland umgesetzt durch Gesetz zur Umsetzung des Übereinkommens vom 29. Mai 2005 über die Rechtshilfe in Strafsachen zwischen den Mitgliedstaaten der Europäischen Union vom 22.7.2005, in Kraft getreten am 8.8.2005, BGBl. I 2005, S. 2189 f.

hoheit bei der Überwachung ausländischer Anschlüsse ausgeht.[43] In den Art. 18 bis 20 EU-RhÜbk[44] sind nämlich ausdrücklich Fälle der Überwachung ausländischer

---

[43] Zur internen unveröffentlichten Richtlinie der Justizministerien von Bund und Ländern zu Zulässigkeitsanforderungen bei der Leistung von Rechtshilfe durch Telefonüberwachung vgl. *Scheller*, Ermächtigungsgrundlagen für die internationale Rechts- und Amtshilfe, S. 62 f.

[44] Art. 18 EU-RhÜbk lautet: „(1) Zum Zwecke einer strafrechtlichen Ermittlung kann eine zuständige Behörde in dem ersuchenden Mitgliedstaat in Übereinstimmung mit ihren innerstaatlichen Rechtsvorschriften an eine zuständige Behörde des ersuchten Mitgliedstaats ein Ersuchen richten um (a) Überwachung des Telekommunikationsverkehrs und dessen unmittelbare Weiterleitung an den ersuchenden Mitgliedstaat oder (b) Überwachung, Aufnahme und nachfolgende Übermittlung der Aufnahme der Telekommunikation an den ersuchenden Mitgliedstaat. (2) Ersuchen nach Absatz 1 können gestellt werden in Bezug auf die Nutzung von Telekommunikationsmitteln durch die Zielperson, wenn sich diese befindet in (a) dem ersuchenden Mitgliedstaat und der ersuchende Mitgliedstaat die technische Hilfe des ersuchten Mitgliedstaats benötigt, um die Kommunikation der Zielperson zu überwachen; (b) dem ersuchten Mitgliedstaat und die Kommunikation der Zielperson in diesem Mitgliedstaat überwacht werden kann; (c) einem dritten Mitgliedstaat, der gemäß Artikel 20 Absatz 2 Buchstabe a in Kenntnis gesetzt worden ist, und der ersuchende Mitgliedstaat die technische Hilfe des ersuchten Mitgliedstaats benötigt, um die Kommunikation der Zielperson zu überwachen. […].“

Art. 19 EU-RhÜbk lautet: „(1) Die Mitgliedstaaten stellen sicher, dass über eine Bodenstation in ihrem Hoheitsgebiet betriebene Systeme für Telekommunikationsdienste, die zum Zweck der rechtmäßigen Überwachung des Kommunikationsverkehrs einer sich in einem anderen Mitgliedstaat befindlichen Person in dessen Hoheitsgebiet nicht unmittelbar zugänglich sind, zum Zweck der rechtmäßigen Überwachung durch diesen Mitgliedstaat mittels eines bezeichneten Dienstanbieters, der sich in dessen Hoheitsgebiet befindet, unmittelbar zugänglich gemacht werden können. (2) In dem in Absatz 1 genannten Fall sind die zuständigen Behörden eines Mitgliedstaats berechtigt, für die Zwecke einer strafrechtlichen Ermittlung nach Maßgabe des geltenden innerstaatlichen Rechts und sofern sich die Zielperson im Hoheitsgebiet dieses Mitgliedstaats befindet, die Überwachung mittels eines dort befindlichen bezeichneten Diensteanbieters durchzuführen, ohne dass der Mitgliedstaat, in dessen Hoheitsgebiet sich die Bodenstation befindet, eingeschaltet wird. (3) Absatz 2 gilt auch, wenn die Überwachung gemäß einem Ersuchen nach Artikel 18 Absatz 2 Buchstabe b durchgeführt wird. (4) Dieser Artikel hindert einen Mitgliedstaat nicht, an denjenigen Mitgliedstaat, in dessen Hoheitsgebiet sich die Bodenstation befindet, ein Ersuchen um rechtmäßige Überwachung des Telekommunikationsverkehrs gemäß Artikel 18 zu stellen, insbesondere wenn es im ersuchenden Mitgliedstaat keine Vermittlungsstelle gibt.“

Art. 20 EU-RhÜbk lautet: „(1) Unbeschadet der allgemeinen Grundsätze des Völkerrechts sowie der Bestimmungen des Artikels 18 Absatz 2 Buchstabe c gelten die in diesem Artikel vorgesehenen Verpflichtungen für Überwachungsanordnungen, die von der zuständigen Behörde eines Mitgliedstaats im Zuge strafrechtlicher Ermittlungen erlassen oder genehmigt wurden; dabei muss es sich um Ermittlungen handeln, die infolge der Begehung einer spezifischen Straftat, einschließlich versuchter Straftaten, soweit diese nach dem innerstaatlichen Recht unter Strafe gestellt sind, durchgeführt werden, um die dafür Verantwortlichen festzustellen und festzunehmen, Anklage gegen sie zu erheben, sie strafrechtlich zu verfolgen oder abzuurteilen. (2) Wenn zum Zwecke einer strafrechtlichen Ermittlung die Überwachung des Telekommunikationsverkehrs von der zuständigen Behörde eines Mitgliedstaats (des „überwachenden Mitgliedstaats“) genehmigt wurde und der in der Überwachungsanordnung bezeichnete Telekommunikationsanschluss der Zielperson im Hoheitsgebiet eines anderen Mitgliedstaats (des „unterrichteten Mitgliedstaats“) genutzt wird, von dem für die Durchführung der Überwachung keine technische Hilfe benötigt

Anschlüsse sowie im Ausland befindlicher Nutzer inländischer Anschlüsse geregelt, die nach dem Erläuternden Bericht zum Übereinkommen wegen des weiten Verständnisses des Telekommunikationsbegriffes nicht nur auf klassische Telefongespräche beschränkt sind.[45]

Mit den Regelungen in den Art. 19 und 20 EU-RhÜbk haben sich die Mitgliedstaaten der Europäischen Union zudem über Konstellationen verständigt, die über den herkömmlichen Rahmen von Rechtshilfeübereinkommen hinausgehen. In Art. 19 EU-RhÜbk sind nämlich Überwachungsmaßnahmen normiert, nach denen es einem Mitgliedstaat ermöglicht wird, die Überwachung vom eigenen Gebiet ausgehend quasi per „Fernbedienung" anzustoßen. Der Mitgliedstaat, in dessen Hoheitsgebiet sich die Bodenstation befindet, welche die Kommunikation abwickelt, gibt nach Art. 19 EU-RhÜbk im Gegenzug ein Stück weit seine Kontrolle über die Überwachung der Kommunikation auf.[46] Art. 20 EU-RhÜbk wiederum betrifft Sachverhalte, in denen der überwachende Staat keine technische Unterstützung mehr durch einen ersuchten Staat benötigt, um vom eigenen Hoheitsgebiet ausgehend den Telekommunikationsverkehr der im Ausland befindlichen Zielperson zu erfassen.[47] Die genannten Vorschriften i.V.m. den Erwägungen dieses Übereinkommens belegen folglich den Bedarf einer gesonderten völkerrechtlichen Rechtfertigung,[48] auch soweit die Staaten bei den Ermittlungen das eigene Staatsgebiet nicht verlassen. Die Verfasser des EU-RhÜbk erklären in den Erwägungsgründen die allgemeinen Grundsätze des Völkerrechts für die nicht in diesem

---

wird, so hat der überwachende Mitgliedstaat den unterrichteten Mitgliedstaat von der Überwachung zu unterrichten: (a) vor der Überwachung in Fällen, in denen er bereits bei Anordnung der Überwachung davon Kenntnis hat, dass sich die Zielperson im Hoheitsgebiet des unterrichteten Mitgliedstaats befindet, oder b) in den anderen Fällen unmittelbar, nachdem er davon Kenntnis erhält, dass sich die Zielperson im Hoheitsgebiet des unterrichteten Mitgliedstaats befindet."

[45] Erläuternder Bericht zu dem Übereinkommen vom 29. Mai 2000 über die Rechtshilfe in Strafsachen zwischen den Mitgliedstaaten der Europäischen Union, ABl. EG 2000, Nr. C 379, S. 7, 20, allgemeine Einleitung zu den Regelungen der Überwachung des Telekommunikationsverkehrs; zur Einbeziehung von Internetverbindungen siehe auch *Meininghaus*, Zugriff auf E-Mails, S. 179, der Art. 20 EU-RhÜbk auf E-Mail-Konten bezieht, soweit die Nachrichten noch nicht abgerufen worden sind; *Schuster*, NStZ 2006, 657, 659 f., der sich im Rahmen des Art. 18 Abs. 5a, Abs. 2a bzw. 2c EU-RhÜbk auf Internetserver und bei Art. 20 EU-RhÜbk auf E-Mail-Konten bezieht; siehe auch *Walden*, Computer Crimes and Digital Investigations, S. 313, Rn. 5.56.

[46] *Walden*, Computer Crimes and Digital Investigations, S. 314, Rn. 5.58.

[47] Siehe hierzu die allgemeine Einleitung zu den Regelungen der Überwachung des Telekommunikationsverkehrs im Erläuternden Bericht zum EU-RhÜbk, ABl. EG 2000, Nr. C 379, S. 7, 20 ff.; sowie *Gleß*, in: Schomburg et al., Internationale Rechtshilfe in Strafsachen, Art. 19 EU-RhÜbk, Rn. 1 ff., Art. 20 EU-RhÜbk, Rn. 1 ff.; *Schuster*, NStZ 2006, 657, 659 f.

[48] *Meuters*, Leitung und Kontrolle grenzüberschreitender Ermittlungen, S. 138 f.

Übereinkommen geregelten Fälle zwar als unberührt,[49] gleichwohl verdeutlichen aber die Regelungen des EU-RhÜbk, dass jedenfalls die Vertragsstaaten keinerlei anerkannte völkerrechtliche Praxis bei den in dem Übereinkommen geregelten Konstellationen der Überwachung ausländischer Anschlüsse bzw. im Ausland befindlicher inländischer Teilnehmer erkennen konnten.

Völkerrechtlich unbedenklich ist eine vom eigenen Staatsgebiet ausgehende Überwachung der Telekommunikation mit Auslandsbezug folglich lediglich dann, wenn die Überwachung nicht ausschließlich an Auslandsanschlüssen ansetzt und damit den ausländischen Teilnehmer ebenfalls zur unmittelbaren Zielperson macht, sondern die Überwachung ausländischer Anschlüsse lediglich eine reflexartige Nebenfolge darstellt.

C. Kommunikation mit Nutzern im Ausland

Kommunizieren die Ermittlungsbehörden mit Internetnutzern im Ausland, z.B. indem sie sich mit diesen im Chat unterhalten oder per E-Mail Nachrichten austauschen, ist ebenfalls strittig, ob sie hiermit gegen das Gebot der Achtung der Gebietshoheit fremder Staaten verstoßen.

1. Eingriff in die Gebietshoheit fremder Staaten

Für die telefonische oder postalische Kontaktaufnahme mit im Ausland befindlichen Personen durch Ermittlungsbehörden ist nach dem deutschen Schrifttum wohl weitgehend anerkannt,[50] dass mit diesen Maßnahmen – selbst soweit keine unmittelbaren rechtlichen Konsequenzen angedroht werden[51] – regelmäßig ein Eingriff in die Gebietshoheit des Staates verbunden ist, in dem sich der Empfänger befindet. Dies ist folgerichtig, da auf dem fremden Staatsgebiet eine substanzielle Auswirkung eintritt, die allein durch ihren investigativen Hintergrund nur einem Hoheitsträger zustehen kann. Kann ein Staat seine Angelegenheiten aber nicht selbst zulässig auf fremdem Staatsgebiet durchsetzen, so ist er auch nicht befugt, sie unter Inanspruchnahme Dritter (hier von Kommunikationsunternehmen) vorzu-

---

[49] Siehe hierzu auch den Erläuternden Bericht zum EU-RhÜbk, ABl. EG 2000, Nr. C 379, S. 7, 24 zu Art. 20; sowie *Gleß*, in: Schomburg et al., Internationale Rechtshilfe in Strafsachen, Art. 20 EU-RhÜbk, Rn. 3.

[50] *Bertele*, Souveränität und Verfahrensrecht, S. 88 i.V.m. 93 ff.; *Ipsen*, Völkerrecht, § 23, Rn. 70; *Schnigula*, DRiZ 1984, 177; *Spatscheck*, Steuern im Internet, Rn. 304; *Storbeck*, Kriminalistik 1987, 472, 473; anders beispielsweise die amerikanische Sichtweise in American Law Institute, vol. 1 Restatement Foreign Rel. Law 3rd, § 431, comment e (i), S. 323.

[51] *Germann*, Gefahrenabwehr und Strafverfolgung im Internet, S. 645; *Siegrist*, Hoheitsakte auf fremdem Staatsgebiet, S. 177 ff.

nehmen.[52] Nach den verwaltungsinternen Anweisungen in Nr. 121 Abs. 1 Satz 1 RiVASt[53] soll die unmittelbare Kontaktaufnahme in strafrechtlichen Angelegenheiten mit Personen im Ausland daher auch nur dann zulässig sein, wenn nicht damit zu rechnen ist, dass der ausländische Staat dieses Verfahren als einen unzulässigen Eingriff in seine Hoheitsrechte beanstandet.[54] Abseits völkerrechtlicher Übereinkommen sind gemäß Nr. 121 Abs. 4 RiVASt zumindest Mitteilungen unzulässig, in denen Zwangsmaßnahmen oder Rechtsnachteile angedroht werden, durch deren Empfang Rechtswirkungen herbeigeführt, insbesondere Fristen in Lauf gesetzt werden oder der Empfänger zu einem Tun oder Unterlassen aufgefordert wird.

Die Strafverfolgungsbehörden können danach also grundsätzlich auch durch Kommunikationsbeziehungen mit ausländischen Nutzern über das Internet – z.B. durch Auskunftsersuchen per E-Mail – in die Gebietshoheit fremder Staaten eingreifen.[55] Der Staat wendet sich bei der Kommunikation über das Internet, ebenso wie bei Verwendung eines Telefons oder der Post,[56] aktiv an im Ausland befindliche Personen, indem er seinen Hoheitsakt durch Daten auf fremdes Staatsgebiet überträgt.[57] An dieser Beurteilung ändert sich selbst dann nichts, wenn – wie im Internet üblich – der Ermittlungsbeamte sich nicht als solcher zu erkennen gibt oder gar als Privatperson ermittelt, denn ein Staat darf sich nicht seiner hoheitlichen Stellung begeben, indem er die Ermittlungen „im privatrechtlichen Gewand" vornimmt.[58]

---

[52] *Bertele*, Souveränität und Verfahrensrecht, S. 97 f.; im Ergebnis ebenso *Schmidt*, Gefahrenabwehrmaßnahmen im Internet, S. 260, für Sperrverfügungsanordnungen gegenüber im Ausland ansässigen Providern.

[53] Richtlinien für den Verkehr mit dem Ausland in strafrechtlichen Angelegenheiten vom 18.9.1984 (BAnz. Nr. 176 vom 18.9.1984 i.V.m. der Beilage Nr. 47/84) i.d.F. der am 1.3.1993 in Kraft getretenen Änderungsbekanntmachung (BAnz. Nr. 40a vom 27.2.1993); abgedruckt z.B. in *Schomburg* et al., Internationale Rechtshilfe in Strafsachen; im Übrigen abrufbar unter http://www.datenbanken.justiz.nrw.de/pls/jmi/ir_rivast_start [Stand: 6.11.2013].

[54] Die Vorschriften der RiVASt stellen allerdings aufgrund ihrer fehlenden Außenwirkung als Verwaltungsvorschriften selbst keine Ermächtigungsgrundlagen dar.

[55] *Bertele*, Souveränität und Verfahrensrecht, S. 88 i.V.m. 93 ff.; *Determann*, Kommunikationsfreiheit im Internet, S. 147 f.; *Germann*, Gefahrenabwehr und Strafverfolgung im Internet, S. 649 für die Kommunikation in ausländischen Diskussionsforen, S. 652 bei Auskunftsverlangen in hoheitlicher Eigenschaft, S. 653 bei verdeckter Kommunikation, S. 653 f.; *Spatscheck/Alvermann*, wistra 1999, 333, 334; *Valerius*, Ermittlungen der Strafverfolgungsbehörden, S. 161.

[56] Zur Unzulässigkeit des direkten Kontakts mit Personen im Ausland *Schnigula*, DRiZ 1984, 177.

[57] *Determann*, Kommunikationsfreiheit im Internet, S. 147.

[58] *Bertele*, Souveränität und Verfahrensrecht, S. 80 i.V.m. 89 ff.; *Hermanns*, Völkerrechtliche Grenzen für die Anwendung kartellrechtlicher Verbotsnormen, S. 17 f.; *Schmidt*, Gefahrenabwehrmaßnahmen im Internet, S. 265 für die Kontaktaufnahme im zugangsgeschützten Chat oder Meinungsforum; *Rudolf*, in: BerDGesVölkR 11, S. 7, 35.

2. Ausnahmsweise Rechtfertigung des Eingriffs

Der Eingriff könnte jedoch infolge Anerkennung dieser Praxis durch die Staaten gerechtfertigt sein, denn dann würden die Staaten diese Ermittlungshandlungen nicht als rechtswidrigen Souveränitätseinbruch auffassen, sodass eine widerspruchslose Duldung vorläge,[59] die zu einer allgemeinen Übung und durch Anerkennung der Staaten nach einem gewissen Zeitablauf zum Gewohnheitsrecht erstarken kann.[60] Einer solchen Übung steht indes entgegen, dass die Rechtsauffassungen in diesen Konstellationen im angloamerikanischen und kontinentaleuropäischen Rechtskreis regelmäßig weit auseinanderklaffen. Während nach den im angloamerikanischen Rechtskreis zumeist vertretenen Auffassungen eine keine rechtlichen Konsequenzen androhende Kommunikation zwischen staatlichen Organen mit Personen in anderen Staaten völkerrechtlich unbedenklich sein soll, sehen die dem kontinentaleuropäischen Rechtskreis entstammenden Rechtsordnungen auch hierin regelmäßig einen Eingriff in die Gebietshoheit des betroffenen Staates.[61] Auf eine in den Grundsätzen einheitliche Staatenpraxis kann folglich nicht zurückgegriffen werden. Maßgeblich ist zudem nicht allein die Rechtsauffassung des Staates, in dem der Ermittlungsort liegt bzw. die Wirkungen der Ermittlungen eintreten, sondern der ermittelnde Staat darf nach dem Prinzip der Gegenseitigkeit gegenüber anderen Staaten nur das einfordern, was er im Gegenzug ebenfalls zu leisten bereit ist.[62] Wollte sich Deutschland also weiterhin gegen eine Kommunikation ausländischer Behörden mit Inländern zur Wehr setzen, so dürften deutsche Ermittlungsbeamte auch ohne Androhung rechtlicher Konsequenzen nicht mit im Ausland befindlichen Personen im Internet kommunizieren.

Zur Rechtfertigung von Eingriffen in die Gebietshoheit durch Kontaktaufnahme mit Personen im Ausland haben z.B. die Mitgliedstaaten der Europäischen Union in den Art. 10, 11 EU-RhÜbk[63] Regelungen zur Vernehmung per Videokonferenz

---

[59] Siehe zur Anerkennung der widerspruchslosen Duldung oder stillschweigender Einwilligung als Rechtfertigung *Geck*, in: Strupp/Schlochauer, Wörterbuch des Völkerrechts, S. 796; *Siegrist*, Hoheitsakte auf fremdem Staatsgebiet, S. 68 ff.

[60] Zu den Voraussetzungen der Herausbildung von Gewohnheitsrecht im Völkerrecht kraft anerkannter Übung und der Beschleunigung im technischen Zeitalter siehe *Doehring*, Völkerrecht, Rn. 288; *Ipsen*, Völkerrecht, § 16, Rn. 4 ff.; *Stein/v. Buttlar*, Völkerrecht, Rn. 124 ff.

[61] Siehe hierzu die Darstellungen m.w.N. bei *Nagel*, Beweisaufnahme im Ausland, S. 21; *Nordmann*, Die Beschaffung von Beweismitteln, S. 57 ff.; *Siegrist*, Hoheitsakte auf fremdem Staatsgebiet, S. 149 f. (für form- und zwangslose Ermittlungen) und S. 177 ff. (speziell für Zustellungen); *Tiedemann*, FS Bockelmann, S. 819, 819 ff.; zur Zusendung von Steuerbescheiden an eine in Deutschland lebende Person durch ausländische Behörden siehe BVerfGE 63, 343, 372.

[62] *Germann*, Gefahrenabwehr und Strafverfolgung im Internet, S. 645 f.; in diesem Sinne auch *Siegrist*, Hoheitsakte auf fremdem Staatsgebiet, S. 147.

[63] Art. 10 EU-RhÜbk lautet: „(1) Befindet sich eine Person im Hoheitsgebiet eines Mitgliedstaats und soll diese Person als Zeuge oder Sachverständiger von den Justizbehörden eines anderen Mitgliedstaats vernommen werden, so kann letzterer, sofern ein persönliches

und zur Vernehmung von Zeugen und Sachverständigen per Telefonkonferenz getroffen.[64] Der Tatsache, dass die Mitgliedstaaten der EU eine solche Regelung für notwendig erachtet haben, kann nicht nur entnommen werden, dass die Kommunikation mit im Ausland befindlichen Personen als in die jeweilige Gebietshoheit eingreifend betrachtet wird, sondern auch, dass eine einheitliche duldende bzw. erlaubende Praxis nicht existiert. Da keine Hinweise für eine spezielle, die Kommunikation im Internet betreffende andere Staatenpraxis bekannt sind,[65] ist die Kommunikation im Internet mit Nutzern im Ausland ohne spezielle Ermächtigungsnorm wegen des Eingriffs in die Gebietshoheit fremder Staaten durch deutsche Ermittlungsbehörden folglich völkerrechtswidrig.

Eine andere Beurteilung könnte allerdings in Fallkonstellationen angezeigt sein, in denen die Strafverfolgungsbehörden bei der Kommunikation davon ausgehen konnten, dass sich ihr Kommunikationspartner im Inland befindet. Anders als bei einer postalischen Adresse oder einem Festnetzanschluss weiß der Ermittlungsbeamte nämlich nicht bereits aufgrund der Kennung des Nutzers sicher, ob sich die Kennung auf einen im Ausland gelegenen Ort bezieht. Weder weist die Kennung selbst zwingend auf einen konkreten Staat hin noch muss sich der Inhaber der Kennung bei der Verwendung dieser im Inland aufhalten; vielmehr ist es z.B. möglich, dass er seine E-Mail-Adresse über einen Webmail-Zugriff im Ausland nutzt. Sprechen die Indizien für eine inländische Kennung, etwa indem eine E-Mail-Adresse auf einen inländischen Provider verweist, ist fraglich, ob die Strafverfolgungsbehörde grundsätzlich davon ausgehen darf, dass sich der Adressat im Inland aufhält, wenn ihr keine entgegenstehenden Anhaltspunkte im Zeitpunkt der Ermittlungsmaßnahme vorliegen.[66]

Erscheinen der zu vernehmenden Person in seinem Hoheitsgebiet nicht zweckmäßig oder möglich ist, darum ersuchen, dass die Vernehmung per Videokonferenz nach Maßgabe der Absätze 2 bis 8 erfolgt. (2) Der ersuchte Mitgliedstaat bewilligt die Vernehmung per Videokonferenz, wenn der Rückgriff auf Videokonferenzen den Grundprinzipien seiner Rechtsordnung nicht zuwiderläuft und er über die technischen Vorrichtungen für eine derartige Vernehmung verfügt. Verfügt der ersuchte Mitgliedstaat nicht über die technischen Vorrichtungen für eine Videokonferenz, so können ihm diese von dem ersuchenden Mitgliedstaat in gegenseitigem Einvernehmen zur Verfügung gestellt werden. […]."

Art. 11 EU-RhÜbk lautet: „(1) Befindet sich eine Person im Hoheitsgebiet eines Mitgliedstaats und soll diese Person als Zeuge oder Sachverständiger von einer Justizbehörde eines anderen Mitgliedstaats vernommen werden, so kann letzterer, sofern sein innerstaatliches Recht dies vorsieht, den erstgenannten Mitgliedstaat ersuchen, die Vernehmung per Telefonkonferenz, wie in den Absätzen 2 bis 5 vorgesehen, zu ermöglichen. (2) Eine Vernehmung per Telefonkonferenz kann nur mit Zustimmung des Zeugen oder des Sachverständigen erfolgen. (3) Der ersuchte Mitgliedstaat bewilligt die Vernehmung per Telefonkonferenz, wenn der Rückgriff auf dieses Verfahren den Grundprinzipien seiner Rechtsordnung nicht zuwiderläuft."

64 Siehe hierzu *Meuters*, Leitung und Kontrolle grenzüberschreitender Ermittlungen, S. 135 ff.

65 *Valerius*, Ermittlungen der Strafverfolgungsbehörden, S. 162.

66 Hierfür *Germann*, Gefahrenabwehr und Strafverfolgung im Internet, S. 646.

Ob allein die Unkenntnis vom Zugriff auf fremdes Staatsgebiet eine hoheitliche Handlung zu rechtfertigen vermag,[67] ist strittig.[68] Dagegen spricht, dass nach vorzugswürdiger Auffassung der Eingriff in die Gebietshoheit fremder Staaten grundsätzlich kein schuldhaftes Handeln voraussetzt.[69] Das Völkerrecht misst dem Willen des Handelnden keine primäre Bedeutung bei, sondern stellt maßgeblich auf die objektive Verletzung eines Rechts ab.[70] Andererseits zeigen die auf dokumentierte Praxisfälle zurückgehenden Vorschriften zur Staatenverantwortlichkeit, Art. 20 ff.,[71] dass unter näher genannten Umständen ein eingreifender Staat völkerrechtlich ausnahmsweise nicht verantwortlich gemacht werden kann,[72] z.B. wenn er in Fällen unabwendbarer Gewalt oder eines außer seiner Kontrolle stehenden unvorhersehbaren Ereignisses handelte, was es ihm unmöglich machte, sich völkerrechtskonform zu verhalten oder zumindest zu wissen, dass sein Verhalten nicht völkerrechtsgemäß ist (Art. 23).[73] Ein solches unvorhersehbares Ereignis liegt allerdings nicht schon vor, wenn der Amtsträger auf einen inländischen Provider aus der Top-Level-Domain „.de“ schließt, denn es ist im Internetzeitalter nicht unüblich, dass Nutzer ihre im Inland erworbenen Kennungen auch im Ausland verwenden, zumal die Erfolgsgeschichte des globalen Netzwerkes auch und gerade auf den grenzüberschreitenden Anwendungsmöglichkeiten beruht. Ein unvorhersehbares Ereignis liegt also jedenfalls nicht in jedem Fall für die Kommunikation im Internet vor.

---

[67] Dagegen *Valerius*, Ermittlungen der Strafverfolgungsbehörden, S. 157.

[68] Council of Europe, Recommendation No. (89) 9, Erläuternder Bericht, S. 87 f.; siehe auch ders., Recommendation No. (95) 13, Erläuternder Bericht, Tz. 191, wonach zumindest eine Benachrichtigung des betroffenen Staates bei Abrufen von Daten aus fremdem Hoheitsgebiet gefordert wird, selbst wenn der Handelnde zunächst gutgläubig davon ausging, der Abruf beträfe im Inland gespeicherte Daten.

[69] Siehe hierzu die Ausführungen unter Teil 1, IV.

[70] *Strupp*, Das völkerrechtliche Delikt, S. 56.

[71] Responsibility of States for Internationally Wrongful Acts (2001), ILC, A/CN 4 L. 602, Rev. 1, auch als Annex der Kenntnis nehmenden Resolution der UN-Generalversammlung (A/RES/56/83); abgedruckt in *Tomuschat*, Völkerrecht, Ordnungsnummer 9.

[72] Siehe dazu *Daum*, Grenzverletzungen und Völkerrecht, S. 43 f.; *Wilske*, Die völkerrechtwidrige Entführung und ihre Rechtsfolgen, S. 107 f.

[73] Responsibility of States for Internationally Wrongful Acts (2001); abgedruckt in *Tomuschat*, Völkerrecht, Ordnungsnummer 9; siehe zu einer früheren Fassung (Art. 31) auch YBILC 1979, vol. II, part two, S. 122.

Art. 23 Responsibility of States for Internationally Wrongful Acts lautet: “(1) The wrongfulness of an act of a State not in conformity with an international obligation of that State is precluded if the act is due to *force majeure*, that is the occurrence of an irresistible force or of an unforeseen event, beyond the control of the State, making it materially impossible in the circumstances to perform the obligation. (2) Paragraph 1 does not apply if: (a) The situation of *force majeure* is due, either alone or in combination with other factors, to the conduct of the State invoking it; or (b) The State has assumed the risk of that situation occurring.”

Im konkreten Einzelfall kann der Auslandsbezug indes unvorhersehbar sein, soweit der Staat die ihm zumutbaren Nachforschungen über den Aufenthaltsort der Person vorgenommen hat, mit der er kommunizieren will. Wenn er danach annehmen durfte, die Kommunikation erfolge im Inland, ist ihm ein Verzicht auf die Ausübung von Hoheitsgewalt nicht zuzumuten. Der Verzicht wäre nämlich gleichzeitig eine Beschränkung der innerstaatlichen Hoheitsausübung, da bei jeder innerstaatlichen Kommunikation immer die Unsicherheit verbliebe, dem Verdikt der Völkerrechtswidrigkeit zu unterliegen. Ob und inwieweit dieser Gedanke, der dem des *inevitable spill-over* bei grenzüberschreitenden Rundfunksignalen[74] vergleichbar ist, in der Staatenpraxis Niederschlag gefunden hat und die betroffenen Staaten Ermittlungen in diesen Fällen stillschweigend dulden, ist jedoch mangels dokumentierter Fälle nicht praktisch belegbar.

D. Download im Ausland gespeicherter Daten

Soweit die Frage nach einem Eingriff in das Hoheitsgebiet fremder Staaten bei Ermittlungen der Strafverfolgungsbehörden im Internet in der Literatur überhaupt angesprochen wird, steht als Maßnahme der Abruf von auf Rechnern im Ausland gespeicherten Daten im Vordergrund.[75] Wie brisant die daran hängenden praktischen Vorgänge sind, veranschaulichen nicht nur Fälle, in denen der Täter z.B. rechtsradikales Material bewusst im Ausland speichert,[76] sondern auch jene Sachverhaltskonstellationen, in denen sich der Beschuldigte z.B. auf eine Geschäftsreise oder einen Wochenendtrip mit seinem Laptop ins Ausland begibt. Gleiches gilt, wenn international tätige Unternehmen involviert sind.[77] So speichern beispielsweise weltweit agierende Provider nicht selten sämtliche Daten ihrer Kunden in verschiedenen Ländern, weswegen sogar bei einer Kommunikation ihrer deutschen Kunden über das Internet die Daten auf Servern im Ausland liegen und die Strafverfolgungsbehörden auch dann mit einem Auslandsbezug konfrontiert sein können, wenn es die Internetnutzer nicht gezielt darauf anlegen, ihre Daten im Ausland zu speichern.

---

[74] Siehe hierzu *Engel*, RabelsZ 49 (1985), 90, 97.

[75] So in den Monografien von *Bär*, Der Zugriff auf Computerdaten im Strafverfahren, S. 232 ff., 507; *Böckenförde*, Die Ermittlung im Netz, S. 206 ff.; *Germann*, Gefahrenabwehr und Strafverfolgung im Internet, S. 641 ff.; *Jofer*, Strafverfolgung im Internet, S. 190 ff.; *Meininghaus*, Zugriff auf E-Mails, S. 178 ff.; *Seitz*, Strafverfolgungsmaßnahmen im Internet, S. 397 ff.; *Valerius*, Ermittlungen der Strafverfolgungsbehörden, S. 141 ff.

[76] BfV, Rechtsextremistische Bestrebungen im Internet, S. 8; *Fromm*, in: Welp, kriminalität@net, S. 41, 42.

[77] *Seitz*, Strafverfolgungsmaßnahmen im Internet, S. 415; *Störing*, MMR 2008, 187, 188 f.

Die Datenzugriffe bereiten bei ungesicherten, also für jedermann frei zugänglichen, im Ausland gespeicherten Daten keine technischen Schwierigkeiten. Bei einer Sicherung durch eine Zugangsbeschränkung müssen die Beamten diese dagegen zunächst erst einmal überwinden.

1. Vorgelagertes Problem der Standortbestimmung des Rechners

Gemeinsam ist beiden Konstellationen aber, dass die Strafverfolgungsbehörden beim Download der Daten regelmäßig nicht ohne Weiteres wissen, wo sich der Server befindet, der ihre Anfrage durch Versendung der nachgefragten Daten beantwortet. Mindesterfordernis für eine Standortbestimmung ist die Kenntnis der IP-Adresse des Rechners,[78] von dem Daten abgerufen werden sollen. Diese Adresse erlaubt in bestimmten Grenzen die Lokalisierung des Computers, auch wenn mangels bisher uneingeschränkt verlässlicher Methoden eine Reterritorialisierung des Internet nicht hinlänglich sicher möglich ist.[79] Die IP-Adresse selbst kann z.B. durch eine Telekommunikationsüberwachung ermittelt werden.[80] Ist hierzu die Mithilfe eines ausländischen Providers nötig, steht gewöhnlich mangels spezieller Erlaubnistatbestände nur der Weg der internationalen Rechtshilfe offen.[81] Insbesondere kann der ersuchende Staat auch nach Art. 20 CCC,[82] der die Erhebung von

---

[78] Um in einem Netzwerk kommunizieren zu können, bedarf der Rechner eines Nutzers einer eindeutigen Kennung, über die er identifiziert werden kann. Diese sog. IP-Adresse vergibt der Access-Provider, über den sich der Nutzer in das Netz „einwählt", aus einem Pool ihm zugewiesener IP-Adressen. Die derzeit verwendeten IP-Adressen nach dem IPv4-Protokoll sind 32- oder 128-stellige Binärzahlen. Siehe *Cheswick/Bellowin/Rubin*, Firewalls und Sicherheit im Internet, S. 62 f.; *Germann*, Gefahrenabwehr und Strafverfolgung im Internet, S. 61, Fn. 79 und S. 66, Fn. 94; *Kyas*, Internet professionell, S. 88 f.; zur Verwendung des Internetprotokolls IPv6 und der damit verbundenen eindeutigeren Kennung aufgrund des größeren Adressraumes *Art. 29 Datenschutzgruppe*, Stellungnahme 2/2002, WP 58, S. 2 ff.

[79] *Hoeren*, MMR 2007, 3, 5 f.; *Lessig/Resnik*, Michigan Law Review, vol. 98, 1999, 395, 399; *Mitsdörffer/Gutfleisch*, MMR 2009, 731, 731 f.; *Sankol*, K&R 2008, 279, 283.

[80] So jedenfalls die Auskunft des BMI zur Frage 37 des Katalogs der SPD-Bundestagsfraktion u.a., S. 19, für die Online-Durchsuchung mittels der Remote Forensic Software für das BKA, abrufbar unter http://www.netzpolitik.org/wp-upload/fragen-onlinedurchsuchung-SPD.pdf [Stand: 6.11.2013].

[81] Hiervon geht inzident auch die G8-Gruppe in ihren Recommendations for Tracing Networked Communications Across National Borders in Terrorist and Criminal Investigations (2002) aus. Die Empfehlungen beziehen sich auf die Schaffung nationaler Rechtsgrundlagen mit dem Ziel, dass Rechtshilfeersuchen im Bereich der Überwachung netzwerkübergreifender Kommunikation erfolgreich bearbeitet werden können. Siehe auch Principles on the Availability of Data Essential to Protecting Public Safety (2002) der G8-Gruppe, worin abermals das Erfordernis internationaler Vereinbarungen für den Zugriff auf Verkehrsdaten, die in anderen Staaten gespeichert sind, zum Ausdruck kommt.

[82] Europarat, Convention on Cybercrime, 23.11.2001 (ETS No. 185), in Kraft getreten am 1.7.2004.

Art. 20 CCC lautet in deutscher Übersetzung: „(1) Jede Vertragspartei trifft die erforderlichen gesetzgeberischen und anderen Maßnahmen, um ihre zuständigen Behörden zu er-

Verkehrsdaten in Echtzeit regelt, bzw. nach dem für die Rechtshilfe bei der Erhebung von Verkehrsdaten in Echtzeit korrespondierenden Art. 33 CCC[83] nicht unmittelbar selbst einen solchen Hoheitsakt auf fremdem Staatsgebiet anordnen und vollziehen.[84] Gleiches gilt im Ergebnis für die – nicht auf klassische Telefongespräche beschränkten[85] – Art. 18 bis 20[86] EU-RhÜbk.[87] Zwar ist nach Art. 19, 20 EU-RhÜbk unter näher bestimmten Voraussetzungen auch die eigenständige Vornahme eines Hoheitsakts mit (un)mittelbarem Auslandsbezug möglich, die Regelungen betreffen aber nicht die Verpflichtung ausländischer Provider zur Mithilfe. Demgegenüber enthält Art. 4 Abs. 1 des Rahmenbeschlusses über die Europäische Beweisanordnung[88] auf Provider abzielende Verpflichtungen; diese können aber

---

mächtigen, (a) Verkehrsdaten, die mit bestimmten in ihrem Hoheitsgebiet mittels eines Computersystems übermittelten Kommunikationen in Zusammenhang stehen, durch Anwendung technischer Mittel im Hoheitsgebiet dieser Vertragspartei in Echtzeit zu erheben oder aufzuzeichnen und (b) einen Diensteanbieter im Rahmen seiner bestehenden technischen Möglichkeiten zu verpflichten, (i) solche Verkehrsdaten durch Anwendung technischer Mittel im Hoheitsgebiet dieser Vertragspartei in Echtzeit zu erheben oder aufzuzeichnen oder (ii) bei der Erhebung oder Aufzeichnung solcher Verkehrsdaten in Echtzeit mit den zuständigen Behörden zusammenzuarbeiten und diese zu unterstützen. (2) Kann eine Vertragspartei die in Absatz 1 Buchstabe a bezeichneten Maßnahmen aufgrund der in ihrer innerstaatlichen Rechtsordnung festgelegten Grundsätze nicht treffen, so kann sie stattdessen die erforderlichen gesetzgeberischen und anderen Maßnahmen treffen, um sicherzustellen, dass Verkehrsdaten, die mit bestimmten in ihrem Hoheitsgebiet übermittelten Kommunikationen in Zusammenhang stehen, durch Anwendung technischer Mittel in diesem Hoheitsgebiet in Echtzeit erhoben oder aufgezeichnet werden. […]."

[83] Art. 33 CCC lautet in deutscher Übersetzung: „(1) Die Vertragsparteien leisten einander Rechtshilfe bei der Erhebung von Verkehrsdaten in Echtzeit in Zusammenhang mit bestimmten Kommunikationen in ihrem Hoheitsgebiet, die mittels eines Computersystems übermittelt werden. Vorbehaltlich des Absatzes 2 unterliegt die Rechtshilfe den nach innerstaatlichem Recht vorgesehenen Bedingungen und Verfahren. (2) Jede Vertragspartei leistet zumindest in Bezug auf die Straftaten Rechtshilfe, bei denen die Erhebung von Verkehrsdaten in Echtzeit in einem gleichartigen inländischen Fall möglich wäre."

[84] Erläuternder Bericht zur Convention on Cybercrime, Tz. 222 und 295; in deutscher Übersetzung siehe BT-Drucks. 16/7218, S. 57 ff., 84, 95 f.

[85] Erläuternder Bericht zu dem Übereinkommen über die Rechtshilfe in Strafsachen zwischen den Mitgliedstaaten der Europäischen Union, ABl. EG 2000, Nr. C 379, S. 7, 20, der eine allgemeine Einleitung zu den Regelungen der Überwachung des Telekommunikationsverkehrs gibt; zur Einbeziehung von Internetverbindungen siehe auch *Schuster*, NStZ 2006, 657, 659 f., der sich im Rahmen des Art. 18 Abs. 5a, Abs. 2a bzw. c EU-RhÜbk auf Internetserver und bei Art. 20 EU-RhÜbk auf E-Mail-Konten bezieht.

[86] Zum Wortlaut siehe Teil 3 Fn. 44.

[87] ABl. EG 2000, Nr. C 197, S. 3 ff. Ergänzt durch den Rechtsakt des Rates vom 16. Oktober 2001 über die Erstellung – gemäß Artikel 34 des Vertrages über die Europäische Union – des Protokolls zu dem Übereinkommen über die Rechtshilfe in Strafsachen zwischen den Mitgliedstaaten der Europäischen Union, ABl. EG 2001, Nr. C 326, S. 1 ff.

[88] Rahmenbeschluss 2008/978/JI des Rates vom 18.12.2008 über die Europäische Beweisanordnung zur Erlangung von Sachen, Schriftstücken und Daten zur Verwendung in Strafsachen, ABl. EU 2008, Nr. L 350, S. 72 ff.

Art. 4 (Anwendungsbereich der Europäischen Beweisanordnung) des Rahmenbeschlusses lautet: „(1) Unbeschadet des Absatzes 2 des vorliegenden Artikels kann die Europäi-

gemäß Art. 4 Abs. 2 lit. c) des Rahmenbeschlusses nicht zur Überwachung der Telekommunikation zugunsten des Anordnungsstaates verpflichtet werden, sondern allenfalls zur schlichten Herausgabe von Computerdaten. Der Anordnungsstaat darf zudem nicht unmittelbar an ausländische Provider herantreten, da eine Beweisanordnung vom sogenannten Vollstreckungsstaat umzusetzen ist (Art. 8 Abs. 1 Rahmenbeschluss).[89] Der weitergehende Vorschlag in Art. 21 der zunächst beabsichtigten Fassung des Rahmenbeschlusses,[90] jeder Mitgliedstaat solle sicherstellen, dass sein nationales Recht Regelungen vorsieht, wonach Personen im eigenen Hoheitsgebiet Computerdaten herausgeben müssen, die sich auf für das eigene Gebiet bereitgestellte Leistungen beziehen, wenn sich die Personen zu diesen rechtmäßig Zugang mithilfe eines elektronischen Kommunikationsnetzes verschaffen können, auch soweit sich die Daten in einem Informationssystem im Hoheitsgebiet eines anderen Mitgliedstaates befinden, hat keine Aufnahme in die endgültige Fassung des Rahmenbeschlusses gefunden.

---

sche Beweisanordnung unter den in Artikel 7 genannten Bedingungen zur Erlangung von Sachen, Schriftstücken oder Daten im Vollstreckungsstaat erlassen werden, die vom Anordnungsstaat für die Zwecke der in Artikel 5 genannten Verfahren benötigt werden. Die Europäische Beweisanordnung erstreckt sich auf die in ihr angegebenen Sachen, Schriftstücke und Daten. (2) Die Europäische Beweisanordnung kann nicht erlassen werden, um von der Vollstreckungsbehörde Folgendes zu verlangen: […] c) Erlangung von Informationen in Echtzeit wie etwa durch Überwachung des Telekommunikationsverkehrs, verdeckte Überwachungsmaßnahmen oder Überwachung von Kontobewegungen; […]."

[89] Art. 8 (Übermittlung der Europäischen Beweisanordnung) des Rahmenbeschlusses lautet: „(1) Die Europäische Beweisanordnung kann an die zuständige Behörde eines Mitgliedstaats übermittelt werden, wenn die zuständige Behörde des Anordnungsstaats hinreichenden Grund zu der Annahme hat, dass sich relevante Sachen, Schriftstücke oder Daten dort befinden oder, wenn es sich um elektronische Daten handelt, diese Daten dort nach dem Recht des Vollstreckungsstaats direkt zugänglich sind. Sie wird unverzüglich von der Anordnungsbehörde an die Vollstreckungsbehörde in einer Form übermittelt, die einen schriftlichen Nachweis unter Bedingungen ermöglicht, die dem Vollstreckungsstaat die Feststellung der Echtheit gestatten. Alle weiteren amtlichen Mitteilungen erfolgen unmittelbar zwischen der Anordnungsbehörde und der Vollstreckungsbehörde. […]."

[90] Vorschlag für einen Rahmenbeschluss über die Europäische Beweisanordnung zur Erlangung von Sachen, Schriftstücken und Daten zur Verwendung in Strafverfahren, KOM(2003) 688 endg.

Art. 21 des Vorschlags lautete: „(1) Jeder Mitgliedstaat ergreift die notwendigen Maßnahmen, um sicherzustellen, dass die Europäische Beweisanordnung ohne weitere Formalitäten vollstreckt wird, wenn (a) die angeforderten Computerdaten sich in einem Informationssystem im Hoheitsgebiet eines anderen Mitgliedstaats befinden, jedoch für eine juristische oder natürliche Person im Hoheitsgebiet des Vollstreckungsstaats mit Hilfe eines elektronischen Kommunikationsnetzes rechtmäßig zugänglich sind, und (b) die Computerdaten sich auf eine Leistung beziehen, die von dieser juristischen oder natürlichen Person im Hoheitsgebiet des Vollstreckungsstaats für eine juristische oder natürliche Person im Hoheitsgebiet desselben Staats bereitgestellt werden. (2) Jeder Mitgliedstaat ergreift zudem die notwendigen Maßnahmen, um sicherzustellen, dass sein innerstaatliches Recht es einem anderen Mitgliedstaat ermöglicht, in Bezug auf Computerdaten nach Absatz 1 tätig zu werden."

Abseits dieser Schwierigkeiten und der häufig nur zeitabhängigen Vergabe der IP-Adressen[91] ist die tatsächliche Adresse eines Rechners auch nicht immer hinreichend sicher zu ermitteln, beispielsweise bei der Verwendung von Anonymisierungsdiensten,[92] Virtual Private Networks (VPN) oder der Datenabfrage über einen Proxy-Server.[93] Darüber hinaus kommt es gerade in grenznahen Gebieten bei nicht leitungsgebundenen Anschlüssen, etwa beim Zugang über UMTS, häufig zum Einloggen in ein Netz, welches zu einem Land zählt, während sich der Nutzer bereits im Nachbarland aufhält, sodass auch hier die IP-Adresse nicht auf den tatsächlichen Standort des Rechners verweisen muss.

2. Download frei zugänglicher Daten

Sind die abrufbaren Daten frei für jedermann verfügbar, ist strittig, ob die Strafverfolgungsbehörden diese ohne Inanspruchnahme von Rechtshilfe oder einer speziellen Erlaubnisnorm abrufen dürfen, wenn die Daten in auf fremdem Hoheitsgebiet gelegenen Computern gespeichert sind. Die Politik und ihnen folgend die Sicherheitsbehörden, z.B. das bei Europol angesiedelte Überwachungsprojekt

---

[91] Es ist nämlich zwischen statischen, d.h. über einen längeren Zeitraum einem konkreten Rechner zugeteilten, und dynamischen, d.h. regelmäßig nur für die Dauer einer Sitzung (Netzverbindung) zugewiesenen, IP-Adressen zu unterscheiden. Siehe hierzu *Köhntopp/Köhntopp*, CR 2000, 248, 248; *Kyas*, Internet professionell, S. 57; *Rasmussen*, CR 2002, 36, 37; *Schulz*, Die Verwaltung 1999, 137, 165 ff. Diese Unterscheidung wird allerdings mit dem vollständigen Übergang zum Internetprotokoll IPv6 wohl obsolet werden, denn dann ist der verfügbare Adressraum so groß, dass es einer dynamischen Vergabe von IP-Adressen vermutlich nicht mehr bedarf, *Raabe*, DuD 2003, 134, 134; zu den datenschutzrechtlichen Bedenken siehe *Art. 29 Datenschutzgruppe*, Stellungnahme 2/2002, WP 58, S. 6 ff.

[92] Z.B. die Anonymisierung des Nutzerrechners über mehrere Zwischenstationen unterschiedlicher sog. Anonymous-Server, siehe hierzu das Projekt AN.ON der TU Dresden; nähere Informationen im Internet unter http://www.anon.inf.tu-dresden.de [Stand: 6.11.2013] bzw. seinen Nachfolger „JonDonym", siehe hierzu unter http://www.anonym-surfen.de/ [Stand: 6.11.2013]; zur technischen Umsetzung vgl. *Federrath/Golembiewski*, DuD 2004, 486, 487; *Fritsch* et al., DuD 2005, 592, 594; *Köpsell/Miosga*, DuD 2005, 403, 403 ff.; ULD, Verkettung digitaler Identitäten, S. 160 f.

Einen anderen, dem Peer-to-Peer-Verfahren ähnlichen Ansatz zur Anonymisierung verfolgt das sog. Onion-Routing, dessen bekanntester Vertreter das Projekt „TOR" ist. Im Gegensatz zum AN.ON/JonDonym-Projekt erfolgt die Anonymisierung nicht mehr über starr vorherbestimmte Mixkaskaden, sondern über flexible und unvorhersehbare, verschiedene Anonymisierungsstationen. Zum technischen Ablauf vgl. ULD, Verkettung digitaler Identitäten, S. 161.

Vgl. zur technischen Vorgehensweise von unterschiedlichen Anonymisierungsdiensten sowie zu deren rechtlicher Bewertung auch *Brunst*, Anonymität im Internet, S. 130 ff., 383 ff.

[93] *Damker/Müller*, DuD 1997, 24, 28; *Federrath/Golembiewski*, DuD 2004, 486, 487; *Köhntopp/Köhntopp*, CR 2000, 248; zur leichten Durchbrechbarkeit der Anonymität bei Proxy-Servern vgl. aber *Federrath/Golembiewski*, DuD 2004, 486, 487; ULD, Verkettung digitaler Identitäten, S. 157.

„Check the Web“[94] oder das deutsche Gemeinsame Internetzentrum (GIZ) der Bundessicherheitsbehörden,[95] sowie die Gerichte, beispielsweise im „CompuServe“-Verfahren[96] oder im Verfahren gegen die Revisionisten *Töben*[97] und *Zündel*,[98] übergehen diese Problemstellung bisher stillschweigend. In der wissenschaftlichen Auseinandersetzung haben sich dagegen zu diesem Fragenkreis im Wesentlichen drei Ansichten herausgebildet. Nach einer Auffassung soll der Download solcher Daten nicht zu einem Eingriff in die Gebietshoheit fremder Staaten führen und daher völkerrechtlich zulässig sein,[99] während nach der Gegenauffassung der Abruf frei zugänglicher Daten gegen das Völkerrecht verstoße und grundsätzlich (wenn keine spezielle Befugnisnorm den Zugriff erlaubt) unzulässig sei.[100] Eine vermit-

---

[94] Vgl. hierzu die Pressemitteilung des BMI vom 9.5.2007 abrufbar unter http://www.bmi.bund.de/SharedDocs/Pressemitteilungen/DE/2007/05/check_the_web.html [Stand: 6.11.2013].

[95] Zur Beschreibung der Aufgaben und Arbeitsweise vgl. die Angaben des BMI unter http://www.verfassungsschutz.de/de/arbeitsfelder/af-islamismus-und-islamistischer-terrorismus/gemeinsames-internetzentrum-giz [Stand: 6.11.2013]. Vorreiter von Kontrollen im Internet waren in Deutschland vor allem das Polizeipräsidium München und das Bayerische LKA. Bereits auf der Innenministerkonferenz vom 19./20.11.1998 wurde darüber hinaus die Errichtung einer Zentralstelle für anlassunabhängige Kontrollen im Internet beim BKA beschlossen. Siehe dazu BKA, Electronic Commerce, S. 59; *Wiedemann*, Kriminalistik 2000, 229, 237 f.

[96] AG München NJW 1998, 2836 ff., aufgehoben durch Urteil des LG München I NJW 2000, 1051 ff., das jedoch gleichfalls die völkerrechtliche Problematik unbeachtet lässt.

[97] BGHSt 46, 212 ff. = BGH NJW 2001, 624 ff.

[98] LG Mannheim, Urteil vom 15.2.2007, Az.: 6 KLs 503 Js 4/96 (unveröffentlicht). Die im „Fall Zündel“ eingelegte Revision verwarf der BGH durch Beschluss vom 12.9.2007, Az.: 1 StR 337/07, HRRS 2007, Nr. 832.

[99] Im Ergebnis wohl *Bär*, EDV-Beweissicherung im Strafverfahren, S. 345, Rn. 507; *ders.*, in Wabnitz/Janovsky, Handbuch des Wirtschafts- und Steuerstrafrechts, 25. Kapitel, Rn. 23 a.E. (von einem Eingriff noch ausgehend aber *ders.*, Der Zugriff auf Computerdaten im Strafverfahren, S. 234 ff.; *ders.*, MMR 1998, 577, 579); *Böckenförde*, Ermittlungen im Netz, S. 208; im Ergebnis *Eschelbach*, in: Eberle/Rudolf/Wasserburg, Mainzer Rechtshandbuch der Neuen Medien, Kapitel XI, Rn. 161; *Germann*, Gefahrenabwehr und Strafverfolgung im Internet, S. 651 f., der grundsätzlich einen Eingriff verneint, für den Fall eines Eingriffs aber auch eine rechtfertigende Duldung annimmt, S. 652, Fn. 1501; *Graf*, in: Herrmann/Ohly, Verantwortlichkeit im Netz, S. 85, 99 f.; *Jofer*, Strafverfolgung im Internet, S. 196; *Kudlich*, JA 2000, 227, 228; so wohl auch *Schmidt*, Gefahrenabwehrmaßnahmen im Internet, S. 264 f.; *Veh*, in: Wabnitz/Janovosky, Handbuch des Wirtschafts- und Steuerstrafrechts, 22. Kapitel, Rn. 88; so wohl auch *Walden*, Computer Crimes and Digital Investigations, S. 316, Rn. 5.63.

[100] *Determann*, Kommunikationsfreiheit im Internet, S. 149 f., der allerdings differenziert zwischen zulässigen Abrufen zur allgemeinen Informationsgewinnung und rechtswidrigen Abrufen, die Bestandteil oder Vorbereitung von Maßnahmen gegen den Anbieter oder Übermittler der betreffenden Inhalte sind; *Gercke*, Rechtswidrige Inhalte im Internet, S. 171; *Gruhl*, in: Welp, kriminalität@net, S. 49, 67, 73; *Meininghaus*, Zugriff auf E-Mails, S. 179; im Ergebnis einen Eingriff in die Souveränität annehmend wohl auch *Möhrenschlager*, wistra 1991, 321, 329 (nicht differenzierend nach frei und beschränkt zugänglichen Daten); *Spatscheck*, in: Welp, kriminalität@net, S. 85, 91 f.; *Wiedemann*,

telnde Auffassung nimmt demgegenüber zwar einen Eingriff in die Gebietshoheit fremder Staaten an, sieht aber einen solchen auch abseits einer konkreten Befugnis bereits durch eine „generelle Einwilligung" des betroffenen Staates[101] oder kraft Gewohnheitsrechts als durchgängig gerechtfertigt an.[102]

a) Eingriff in die Gebietshoheit fremder Staaten

Wie bereits bei den vorhergehenden Maßnahmen herausgearbeitet, ist auch mit dem Download frei zugänglicher, im Ausland gespeicherter Daten durch Ermittlungsbeamte im Inland, sei es vom behördeneigenen Rechner oder vom Rechner eines Dritten aus,[103] ebenfalls ein Eingriff in die Gebietshoheit fremder Staaten verbunden, da die Beamten mit dem Download Rechnerprozesse im Ausland hervorrufen und damit auf das Gebiet der betroffenen Staaten selbst einwirken.[104] Gegen einen solchen Eingriff spricht entgegen anderer Ansicht[105] insbesondere nicht, dass die Staatsvertreter nach deutschem Grundrechtsverständnis nicht in die geschützten Rechte der betroffenen Computerinhaber und berechtigten Nutzer eingreifen, die mit dem freien Zugang zu den Daten auch in deren Abruf durch jedermann zugestimmt haben. Auf ein Einverständnis von Privatpersonen und juristischen Personen des Privatrechts kann es aus den oben bereits genannten Gründen[106] nämlich nicht ankommen; dieses ist mangels Dispositionsbefugnis über die staatlichen Hoheitsrechte vielmehr gegenstandslos.[107] Auch soweit sich der Hoheitsakt nicht gegen den fremden Staat als solchen richtet, sondern gegen dessen

---

Kriminalistik 2000, 229, 238 (ohne Differenzierung zwischen frei und beschränkt zugänglichen Daten).

[101] *Valerius*, Ermittlungen der Strafverfolgungsbehörden, S. 155 f.

[102] *Gercke*, StraFo 2009, 271, 273; *Seitz*, Strafverfolgungsmaßnahmen im Internet, S. 409 f.; *ders.*, IJCLP, Issue 9/2004, S. 1, 9 f.; *Sieber*, Straftaten und Strafverfolgung im Internet, C 144 f.

[103] So z.B. wenn die Ermittler nachvollziehen wollen, welche frei zugänglichen Inhalte aus dem Ausland von einem bestimmten Rechner – den sie z.B. bei einer Durchsuchung aufgefunden haben – abgerufen wurden.

[104] *Bär*, Der Zugriff auf Computerdaten im Strafverfahren, S. 234 ff.; Council of Europe, Recommendation No. (95) 13, Erläuternder Bericht, Tz. 187 ff.; *Determann*, Kommunikationsfreiheit im Internet, S. 149; *Meininghaus*, Zugriff auf E-Mails, S. 180; *Sankol*, K&R 2008, 279, 280 f.; *Seitz*, Strafverfolgungsmaßnahmen im Internet, S. 407 f.; *ders.*, IJCLP, Issue 9/2004, S. 1, 8; *Sieber*, in: Eser/Thormundsson, Old Ways and New Needs in Criminal Legislation, S. 203, 211 f. (mit dem Hinweis auf weiteren Diskussionsbedarf in Fn. 25); *ders.*, COMCRIME-Study, S. 107, mit Verweis auf besondere Situationen in Fn. 239, wobei jedoch nicht zwischen Eingriff und Rechtfertigung unterschieden wird.

[105] *Bär*, in: Wabnitz/Janovsky, Handbuch des Wirtschafts- und Steuerstrafrechts, 25. Kapitel, Rn. 23 a.E.; *Jofer*, Strafverfolgung im Internet, S. 193.

[106] Siehe hierzu die Ausführungen unter Teil 1, III.A.

[107] *Bertele*, Souveränität und Verfahrensrecht, S. 86 f.; *Gercke*, StraFo 2009, 271, 273; *Sieber*, Straftaten und Strafverfolgung im Internet, C 79; *Spatscheck/Alvermann*, IStR 2001, 33; *dies.*, wistra 1999, 333, 334; im Ergebnis, aber ohne Begründung, ebenso *Gruhl*, in: Welp, kriminalität@net, S. 49, 67, 73.

Staatsangehörige, deren Daten abgerufen werden, können die Rechte des fremden Staates verletzt sein, insbesondere wenn der Abruf Bestandteil oder Vorbereitung von Ermittlungsmaßnahmen z.B. gegen die Anbieter oder Übermittler der Inhalte ist. Überdies kann der betroffene Staat zumindest seinen Schutzanspruch gegenüber seinen Staatsangehörigen geltend machen.

b) Eingriff ausnahmslos gerechtfertigt

Der mit dem Download frei zugänglicher Daten verbundene Eingriff in die Gebietshoheit fremder Staaten ist jedoch gerechtfertigt. Eine solche Rechtfertigung lässt sich allerdings nur den Rechtsquellen entnehmen, an denen sich jeder Eingriff messen lassen muss,[108] also völkerrechtlichen Verträgen, dem Völkergewohnheitsrecht als Ausdruck einer allgemein als Recht anerkannten Übung oder den von den Kulturvölkern anerkannten allgemeinen Rechtsgrundsätzen.[109] Allein vom Standpunkt der Praktikabilität ist die völkerrechtliche Zulässigkeit des Downloads frei zugänglicher Daten, auch wenn dies für die Ermittlungsbehörden wünschenswert erscheinen mag,[110] allerdings nicht zu begründen. Aus einer solchen bloßen Wunschvorstellung erwächst nämlich noch keine Rechtfertigung, da Praktikabilitätsgründe für sich keinen völkerrechtlich anerkannten Rechtsgrund darstellen.[111]

Soweit Deutschland die Convention on Cybercrime vollständig ins nationale Recht umgesetzt hat, ergibt sich eine Rechtfertigung zum Abruf frei zugänglicher Inhalte für die Strafverfolger aus dem Tatbestand des Art. 32 Buchstabe a)[112] CCC.[113] Dort ist bestimmt, dass eine Vertragspartei ohne die Genehmigung einer

---

[108] *Gercke*, StraFo 2009, 271, 272; *Seitz*, Strafverfolgungsmaßnahmen im Internet, S. 408; *ders.*, IJCLP, Issue 9/2004, S. 1, 8 f.

[109] Zu den Rechtsquellen siehe *Ipsen*, Völkerrecht, 3. Kapitel, Rn. 2.

[110] So *Graf*, in: Herrmann/Ohly, Verantwortlichkeit im Netz, S. 85, 99 f.

[111] *Seitz*, Strafverfolgungsmaßnahmen im Internet, S. 408; *ders.*, IJCLP, Issue 9/2004, S. 1, 9.

[112] Art. 32 CCC lautet in deutscher Übersetzung: „Eine Vertragspartei darf ohne die Genehmigung einer anderen Vertragspartei (a) auf öffentlich zugängliche gespeicherte Computerdaten (offene Quellen) zugreifen, gleichviel, wo sich die Daten geographisch befinden, oder (b) auf gespeicherte Computerdaten, die sich im Hoheitsgebiet einer anderen Vertragspartei befinden, mittels eines Computersystems in ihrem Hoheitsgebiet zugreifen oder diese Daten empfangen, wenn sie die rechtmäßige und freiwillige Zustimmung der Person einholt, die rechtmäßig befugt ist, die Daten mittels dieses Computersystems an sie weiterzugeben."

[113] *Bär*, BKA-Herbsttagung 2007, S. 14, der allerdings ohne auf das Erfordernis der Umsetzung einzugehen ohne Weiteres auf Art. 32 Buchstabe a) CCC verweist; *Gercke*, StrafFo 2009, 271, 272; *Sankol*, K&R 2008, 279, 281; *Spatscheck*, in Welp, kriminalität@net, S. 85, 92. Siehe auch die Regelung in Art. 6 Abs. 5 im Stanford Draft einer International Convention to Enhance Protection form Cyber Crime and Terrorism, abgedruckt in *Sofaer/Goodman*, The Transnational Dimension of Cyber Crime and Terrorism, S. 249 ff. und *Sofaer*, in Sofaer/Goodman, The Transnational Dimension of Cyber Crime and Terrorism, S. 221, 235.

anderen Partei selbstständig auf öffentlich zugänglich gespeicherte Computerdaten (offene Quellen) zugreifen darf, unabhängig davon, wo sich die Daten geografisch befinden.[114] Jeder Staat, welcher der Konvention beigetreten ist und diese umgesetzt hat, kann sich aufgrund eigener Verpflichtung zur Gewährung des Abrufrechts ebenfalls auf dieses vereinbarte Recht nach dem Grundsatz der Gegenseitigkeit berufen.

Abseits der Regelung in Art. 32 CCC ist aber fraglich, ob sich eine Rechtfertigung zum Download frei zugänglicher Daten nicht bereits aus international anerkanntem Gewohnheitsrecht ergibt.[115] Dafür spricht, dass die Mehrheit der Staaten bereits vor der Verabschiedung der Convention on Cybercrime bis heute frei zugängliche Inhalte – auch wenn diese im Ausland gespeichert waren – abgerufen haben. Dies verdeutlichen die zahlreichen Beispiele der anlassunabhängigen Recherchen von Behörden im Internet,[116] die bisher – soweit bekannt – nicht auf die Gegenwehr anderer Staaten getroffen sind. So beauftragte beispielsweise die Innenministerkonferenz durch Beschluss vom 19./20.11.1998 nach § 2 Abs. 1 und Abs. 2 Nr. 1, i.V.m. § 7 Bundeskriminalamtgesetz (BKAG) das Bundeskriminalamt mit der zentralen Wahrnehmung von anlassunabhängigen Recherchen in Datennetzen, in deren Folge eine Zentralstelle für anlassunabhängige Recherchen in Datennetzen (ZaRD) im Januar 1999 eingerichtet wurde, die weltweit im Internet tätig wird. Vergleichbare Recherchen nehmen u.a. auch US-amerikanische FBI-Beamte[117] und Ermittler der Serious Organised Crime Agency (SOCA) Großbritanniens[118] vor.

Mit dieser gelebten Staatenpraxis korrespondieren allerdings nicht ausnahmslos die Darlegungen des Meinungsstands der Staaten in internationalen Vorschlägen und Konventionen. So sprachen beispielsweise die Verfasser der OECD-Studie zur

---

[114] Siehe hierzu auch den Erläuternden Bericht für die CCC, Tz. 293 f. sowie die Denkschrift zur Umsetzung der CCC ins nationale Recht, BT-Drucks. 16/7218, S. 55.

[115] Im Ergebnis so *Gercke*, StraFo 2009, 271, 273; *Valerius*, Ermittlungen der Strafverfolgungsbehörden, S. 155 f.; *Seitz*, Strafverfolgungsmaßnahmen im Internet, S. 409 f.; angedacht bereits durch *Sieber*, in: Eser/Thormundsson, Old Ways and New Needs in Criminal Legislation, S. 203, 212, Fn. 25; *ders.*, COMCRIME-Study, S. 107, Fn. 239; a.A. *Spatscheck*, in: Welp, kriminalität@net, S. 85, 92.

[116] Für Deutschland vgl. die Darstellung der Entwicklung bei *Ziercke*, BKA-Herbsttagung 2007, S. 4.

[117] Zur Rechtsgrundlage für anlassunabhängige Recherchen siehe die Attorney General's Guidelines for domestic FBI operations, dort Abschnitt V.A. Nr. 4+9, S. 31 f., abrufbar unter http://www.justice.gov/ag/readingroom/guidelines.pdf [Stand: 6.11.2013]. Siehe auch die Richtlinien des US Justizministeriums „Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations", unter I., C, S. 15 ff., abrufbar unter http://www.justice.gov/criminal/cybercrime/docs/ssmanual2009.pdf [Stand: 6.11.2013].

[118] Die SOCA ist im Jahr 2006 aus der gleichzeitig aufgelösten National High-Tech Crime Unit hervorgegangen; zu ihren Grundlagen und Aufgaben siehe den Serious Organised Crime and Police Act 2005, abrufbar unter http://www.legislation.gov.uk/ukpga/2005/15/contents [Stand: 6.11.2013].

Analyse der Rechtspolitik bei der Bekämpfung der Computerkriminalität zwar bereits 1986 das praktische Bedürfnis grenzüberschreitender Datenabrufe an, ließen aber offen, ob nationale Strafverfolger mit solchen Transfers gegen das Völkerrecht verstoßen.[119] Die Autoren der Resolution der AIDP[120] vom XVth International Congress of Penal Law in Rio de Janeiro 1994 hielten dagegen für eine grenzüberschreitende Durchsuchung und Beschlagnahme in vernetzten Computersystemen internationale Vereinbarungen für erforderlich.[121] Ausdrücklich auch auf im Ausland frei zugänglich gespeicherte Daten bezogen sich 1995 die Verfasser der Recommendation (95) 13 des Europarats. Diese befanden, dass der Abruf freier Quellen, auch wenn die Daten im Ausland gespeichert sind, zulässig sein sollte.[122] Zugleich hielten sie im Erläuternden Bericht jedoch fest, dass selbst in Fällen des Abrufs frei zugänglicher, extraterritorial gespeicherter Daten nicht vollständig geklärt sei, ob der direkte Zugriff ohne gesonderte völkerrechtliche Erlaubnisnorm zulässig sei.[123]

Unmissverständlich für die Zulässigkeit des selbstständigen grenzüberschreitenden Abrufs frei zugänglicher Daten abseits einer besonderen Autorisation sprach sich indes die für High-Tech-Kriminalität zuständige Arbeitsgruppe der G8-Staaten in Nr. 7[124] des Statement of Principles 1997[125] aus. Sie wiederholte diese Auffassung zwei Jahre später.[126] Vor dem Hintergrund, dass die Mitglieder der Gruppe die führenden Industrienationen[127] sind, kommt dieser Zulässigkeitserklärung besondere Bedeutung zu. Weniger eindeutig ist 2001 aber wieder der Erläuternde

---

119 OECD, Computer-related Crime: Analysis of Legal Policy, S. 68.

120 Association Internationale de Droit Pénal.

121 AIDP, International Review of Penal Law, vol. 66 (1995) No. 1/2, S. 61, Tz. 23c.

122 Siehe hierzu Principle No. 17, Recommendation No. (95) 13: "The power to extend a search to other computer systems should also be applicable when the system is located in a foreign jurisdiction, provided that immediate action is required. In order to avoid possible violations of state sovereignty or international law, an unambiguous legal basis for such extended search and seizure should be established. Therefore, there is an urgent need for negotiating international agreements as to how, when and to what extent such search and seizure should be permitted."

123 Council of Europe, Recommendation No. (95) 13, Erläuternder Bericht, Tz. 190; in ders., Recommendation No. (89) 9, Erläuternder Bericht, S. 87 f., finden sich hingegen nur Ausführungen zum Abruf von zugangsgeschützten Daten.

124 Principle No. 7 lautet: "Transborder electronic access by law enforcement to publicly available (open source) information does not require authorization from the State where the data resides."

125 G8-Gruppe, Principles and Action Plan to Combat High-Tech Crime, 1997.

126 G8-Gruppe, Principles on transborder access to stored computer data, 1999, Principle No. 6 (a): "Notwithstanding anything in these Principles, a State need not obtain authorization from another State when it is acting in accordance with its national law for the purpose of: (a) accessing publicly available (open source) data, regardless of where the data is geographically located […]."

127 Kanada, Frankreich, Deutschland, Italien, Japan, Großbritannien, USA und Russland.

Bericht der Convention on Cybercrime, in dem es zum grenzüberschreitenden Zugriff auf Computerdaten heißt, dass sich die Verfasser entschieden, „in Art. 32 des Übereinkommens nur solche Situationen aufzuführen, bezüglich derer alle der Auffassung waren, dass eine einseitige Vorgehensweise akzeptierbar sei".[128] Die Formulierung „akzeptierbar" könnte hier nahe legen, dass die Vertragsstaaten für den Bereich des Abrufs im Ausland gespeicherter, öffentlich verfügbarer Daten eine gesonderte Regelung für erforderlich hielten. Andererseits kann der Wortlaut aber auch allein dem Umstand geschuldet sein, dass sich die Verfasser des Übereinkommens mangels hinreichender Erfahrungen auf eine umfassende rechtsverbindliche Regelung für den grenzüberschreitenden Zugriff auf gespeicherte Daten im Übrigen nicht einigen konnten. Angesichts des bereits über einen längeren Zeitraum unwidersprochen praktizierten grenzüberschreitenden Zugriffs auf offene Quellen spricht mehr dafür, dass die Verfasser der Konvention, zumindest für den Abruf freier Quellen, ihre Ermittlungsarbeit lediglich deklaratorisch auf ein geschriebenes rechtliches Fundament stellen wollten, also eine solche Grundlage nicht als konstitutiv erachteten.

Durch die intensive internationale behördliche Nutzung des Zugriffs auf frei zugängliche Daten im Internet, die ohne Protest der betroffenen Länder geblieben ist, und die insbesondere für den technologischen Bereich durchaus lange Dauer dieser Staatenpraxis[129] ist zudem wohl nicht mehr nur eine Rechtfertigung aufgrund genereller Einwilligung gegeben.[130] Es liegt vielmehr eine von gemeinsamer Rechtsauffassung getragene ständige Übung vor, die sich durch Anerkennung der Staaten zum Gewohnheitsrecht[131] entwickelt hat.[132] Folglich können aufgrund einer staatenübergreifenden anerkannten Übung Ermittlungsbeamte allgemein zugängliche Daten über das Internet, auch soweit diese auf ausländischen Servern gespeichert sind, im Einklang mit dem Völkerrecht abrufen.

Der Umstand, dass der Zugriff auf frei abrufbare Daten durch die Strafverfolgungsbehörden nicht lediglich privaten wirtschaftlichen Interessen, sondern Strafverfolgungszwecken dient und das Internet auf einfache Weise eine Vielzahl an unbemerkten Abrufen von Informationen erlaubt,[133] vermag diese rechtliche Beur-

---

[128] Erläuternder Bericht zur Convention on Cybercrime, Tz. 293.

[129] Zu den Voraussetzungen der Herausbildung von Gewohnheitsrecht im Völkerrecht kraft anerkannter Übung und der Beschleunigung im technischen Zeitalter siehe *Doehring*, Völkerrecht, Rn. 288; *Stein/v. Buttlar*, Völkerrecht, Rn. 12 ff.

[130] *Valerius*, Ermittlungen der Strafverfolgungsbehörden, S. 158.

[131] Zu den Voraussetzungen der Entstehung von Völkergewohnheitsrecht vgl. *Spang-Hanssen*, Cyberspace & International Law, S. 218 ff.

[132] *Gercke*, StraFo 2009, 271, 273; *Seitz*, Strafverfolgungsmaßnahmen im Internet, S. 409 f.; *ders.*, IJCLP, Issue 9/2004, S. 1, 9 f.

[133] So die Argumentation von *Bär*, Der Zugriff auf Computerdaten im Strafverfahren, S. 193 f., der allerdings eine Online-Abfrage bei freiwilliger Gestattung wieder in Betracht ziehen will; *ders.*, CR 1995, 227, 234; in diesem Sinne auch *Determann*, Kommunikationsfreiheit im Internet, S. 149 f., der deshalb differenziert zwischen zulässigen Abfragen zur

teilung nicht zu ändern. Gerade die Tatsache, dass die Staaten in Kenntnis dieser Sachlage selbst Recherchen in allgemein zugänglichen Quellen im Internet vornehmen und Downloads von allgemein zugänglichen Daten durch andere Staaten nicht entgegentreten, begründet die Legitimation. Da Staaten selbst dafür Sorge tragen, was sie fremden Ermittlungsbehörden gestatten und welche Übung sie so entstehen lassen, greift der Vorwurf der Aushebelung des formellen Territorialitätsprinzips durch Verwendung neuer Kommunikationsmedien[134] nicht durch.

3. Download von Daten, die einer Zugangsbeschränkung unterliegen

Für Ermittlungen im Strafverfahren wesentlich interessanter sind zumeist aber Daten, die nicht für jedermann zugänglich sind, sondern auf die nur ausgewählte Personen zugreifen können. Strafverfolger können sich zugangsgeschützte Daten aus dem Ausland verschaffen, indem sie diese mit Zustimmung des Berechtigten herunterladen oder den Zugangsschutz selbst durchbrechen oder umgehen.

Der Abruf im Ausland gespeicherter, zugangsbeschränkter Daten durch die Strafverfolgungsbehörden ist nach überwiegender Meinung ohne eine spezielle Ermächtigungsnorm völkerrechtswidrig,[135] da die Ermittlungsbeamten in die Gebietshoheit des Staates, in dem die Daten gespeichert sind, mangels hinreichender Ermächtigungsgrundlage rechtswidrig eingreifen. Vereinzelt werden allerdings Überlegungen angestellt, ob z.B. der Abruf zugangsgeschützter Daten zulässig sein könnte, wenn der Zugangsberechtigte in den Abruf einwilligt[136] oder die Strafver-

---

allgemeinen Innformationsgewinnung und rechtswidrigen Abrufen, die Bestandteil oder Vorbereitung von Maßnahmen gegen die Anbieter oder Übermittler der betreffenden Inhalte sind.

[134] So *Ditz*, DStR 2004, 2038, 2024.

[135] LG Hamburg StV 2009, 70,71; *Bär*, Der Zugriff auf Computerdaten im Strafverfahren, S. 234 ff.; *ders.*, in: Wabnitz/Janovsky, Handbuch des Wirtschafts- und Steuerstrafrechts, 25. Kapitel, Rn. 23, *ders.*, MMR 1998, 577, 579; *ders.*, EDV-Beweissicherung im Strafverfahren, S. 345, Rn. 507; *Brodowski*, JR 2009, 402, 410; Council of Europe, Recommendation No. (89) 9, Erläuternder Bericht, S. 87 ff.; ders., Recommendation No. (95) 13, Erläuternder Bericht, Tz. 187 ff.; *Eschelbach*, in: Eberle/Rudolf/Wasserburg, Mainzer Rechtshandbuch der Neuen Medien, Kapitel XI, Rn. 161; *Gaede*, StV 2009, 96, 101 f.; *Gercke*, StraFo 2009, 271, 272 f.; *Germann*, Gefahrenabwehr und Strafverfolgung im Internet, S. 653 f.; *Graf*, in: Herrmann/Ohly, Verantwortlichkeit im Netz, S. 85, 99 f.; *Jofer*, Strafverfolgung im Internet, S. 196; *Meininghaus*, Zugriff auf E-Mails, S. 179 ff.; *Möhrenschlager*, wistra 1991, 321, 329 (nicht differenzierend nach frei und beschränkt zugänglichen Daten); *Schantz*, KritV 2007, 310, 328; *Schmidt*, Gefahrenabwehrmaßnahmen im Internet, S. 264 f.; *Seitz*, Strafverfolgungsmaßnahmen im Internet, S. 417 ff.; *Sieber*, in: Eser/Thormundsson, Old Ways and New Needs in Criminal Legislation, S. 203, 211 f.; *ders.*, in: Cheswick/Bellovin, Firewalls und Sicherheit im Internet, S. 283, 303 f.; *ders.*, The International Emergence of Criminal Information Law, S. 49; *ders.*, Straftaten und Strafverfolgung im Internet, C 145; *Spatscheck*, StraFo 2000, 1, 7 (ohne Differenzierung zwischen frei und beschränkt zugänglichen Daten); *Wiedemann*, Kriminalistik 2000, 229, 238 (ohne Differenzierung zwischen frei und beschränkt zugänglichen Daten).

[136] Council of Europe, Recommendation No. (95) 13, Erläuternder Bericht, S. 69, Tz. 190.

folger nicht wissen, dass sie Daten im Ausland abrufen.[137] Nach der Gegenauffassung findet aufgrund fehlender physischer Anwesenheit der Ermittlungsbehörden auf dem fremden Staatsgebiet ein Souveränitätseingriff hingegen grundsätzlich nicht statt. Die Zugriffe der Ermittlungsbehörden sollen aber nicht über das Maß hinausgehen dürfen, welches dem Nutzungsberechtigten selbst zusteht.[138]

a) Abruf mit Zustimmung des Berechtigten

Rufen die Strafverfolger im Ausland gespeicherte Daten mit Zustimmung des Berechtigten ab, so durchbrechen oder umgehen sie den Zugangsschutz zumindest nicht eigenmächtig. Eine völkerrechtliche Konfliktlage entsteht erst gar nicht, wenn die Ermittler lediglich die Daten aus dem Ausland wahrnehmen, die ein inländischer Nutzer schon – und sei es nur in den Arbeitsspeicher – heruntergeladen hat.[139] In diesen Fällen greifen die Strafverfolger nämlich nicht in ein fremdes Hoheitsgebiet ein, denn sie führen weder selbst datenrechnerische Vorgänge im Ausland herbei noch ist ihnen das Handeln des Nutzers – soweit nicht von ihnen veranlasst – zurechenbar.

aa) Eingriff in die Gebietshoheit fremder Staaten

Anders liegt der Sachverhalt hingegen, wenn die Ermittler selbst die im Ausland gespeicherten, zugangsgeschützten Daten abrufen oder Dritte hierzu veranlassen. In diesen Fällen greifen sie in die Gebietshoheit des betroffenen fremden Staates ein bzw. ist ihnen das Handeln des Dritten als Eingriff zurechenbar; der Eingriff selbst liegt im Auslösen von datenrechnerischen Vorgängen im Ausland. Die hiermit einhergehende Verletzung der Gebietshoheit des fremden Staates entfällt auch nicht dadurch, dass der Berechtigte in den Abruf eingewilligt hat, denn er selbst kann nicht über die Souveränitätsrechte des vom Abruf betroffenen Staates disponieren.

bb) Rechtfertigung des Eingriffs in engen Grenzen

Der Eingriff ist jedoch innerhalb der Grenzen der speziellen Ermächtigungsnormen der Convention on Cybercrime gerechtfertigt. Aus Art. 19 Abs. 2 CCC,[140] der

---

137 Ebenda, S. 69 f., Tz. 191; *Sieber*, COMCRIME-Study, S. 107, Fn. 239.

138 *Ehlscheid*, in: v. Briel/Ehlscheid, Steuerstrafrecht, § 3, Rn. 493.

139 Council of Europe, Recommendation No. (89) 9, Erläuternder Bericht, S. 87; ders., Recommendation No. (95) 13, Erläuternder Bericht, Tz. 187; *Seitz*, IJCLP, Issue 9/2004, S. 1, 3, Fn. 6.

140 Art. 19 Abs. 2 CCC lautet in deutscher Übersetzung: „Jede Vertragspartei trifft die erforderlichen gesetzgeberischen und anderen Maßnahmen, um sicherzustellen, dass ihre Behörden, wenn sie ein bestimmtes Computersystem oder einen Teil davon nach Absatz 1 Buchstabe a durchsuchen oder in ähnlicher Weise darauf Zugriff nehmen und Grund zu der Annahme haben, dass die gesuchten Daten in einem anderen Computersystem oder einem

die erweiterte Durchsuchung und Sicherstellung räumlich entfernter Speichermedien von einem aufgefundenen System aus zum Gegenstand hat, ergibt sich eine Befugnis zum eigenständigen Vollzug des Abrufs von Daten aus dem Ausland zwar noch nicht. Diese Regelung bezieht sich nämlich nur auf solche Computersysteme, die sich „im Hoheitsgebiet der betreffenden Vertragspartei" befinden.[141] Für Staaten, welche der Convention on Cybercrime beigetreten sind und die Regelungen in ihr nationales Recht transformiert haben, folgt die Ermächtigung zum Abruf im Ausland gespeicherter zugangsbeschränkter Daten mit Zustimmung des Betroffenen aber aus Art. 32 Buchstabe b) CCC.[142] Hiernach ist ein Vertragsstaat berechtigt, „auf gespeicherte Computerdaten, die sich im Hoheitsgebiet einer anderen Vertragspartei befinden, mittels eines Computersystems in [seinem] Hoheitsgebiet [zu]zugreifen oder diese Daten [zu] empfangen, wenn [er] die rechtmäßige und freiwillige Zustimmung der Person einholt, die rechtmäßig befugt ist, die Daten mittels dieses Computersystems an [ihn] weiterzugeben".[143] Agieren die Strafverfolger innerhalb der von Art. 32 Buchstabe b) CCC vorgegebenen Grenzen, sind sie also ermächtigt, auch zugangsgeschützte Daten eigenständig aus den fraglichen Staaten abzurufen.[144]

Die Befugnis der Ermittler nach Art. 32 Buchstabe b) CCC ist allerdings recht eng geschnitten. Es reicht nämlich nicht aus, dass der Dritte selbst auf die Daten im Ausland rechtmäßig zugreifen kann. Der Berechtigte muss vielmehr auch die Zu-

---

Teil davon im Hoheitsgebiet der betreffenden Vertragspartei gespeichert sind, und diese Daten von dem ersten System aus rechtmäßig zugänglich oder verfügbar sind, die Durchsuchung oder den ähnlichen Zugriff rasch auf das andere System ausdehnen können."

[141] Siehe hierzu den Erläuternden Bericht für die CCC, Tz. 192 f., 195; *Bär*, EDV-Beweissicherung im Strafverfahren, S. 342, Rn. 500; *Sankol*, K&R 2008, 279, 282. So auch bereits die Vorlage für Art. 19 Abs. 2 CCC aus den Empfehlungen des Europarates, Council of Europe, Recommendation No. (95) 13, Anhang I. No. 3; siehe hierzu ferner den Erläuternden Bericht für Recommendation No. (95) 13, Tz. 80. Die Beschränkung auf das eigene Hoheitsgebiet verkennt dagegen der DAV, Stellungnahme Nr. 41/2007, S. 26, 29, wenn er annimmt, die Durchsuchung nach Art. 19 Abs. 2 CCC dürfe auch auf das Gebiet sämtlicher Vertragsstaaten ausgedehnt werden.

[142] Vgl. auch die Regelung in Art. 6 Abs. 5 im Stanford Draft einer International Convention to Enhance Protection from Cyber Crime and Terrorism, abgedruckt in *Sofaer/Goodman*, The Transnational Dimension of Cyber Crime and Terrorism, S. 249 ff. Art. 6 Abs. 5 lautet: "States Parties shall be free to engage in reasonable, electronic methods of investigation of conduct covered by Articles 3 and 4 of this Convention, over which they have jurisdiction to prosecute under Article 5, even if such conduct results in the transfer of electronic signals into the territory of other States Parties. A State Party aware that its investigative efforts will likely result in such transfers of electronic signals shall as soon as practicable inform all affected States Parties of such efforts." Siehe hierzu auch *Sofaer*, in: Sofaer/Goodman, The Transnational Dimension of Cyber Crime and Terrorism, S. 221, 235.

[143] Siehe hierzu auch den Erläuternden Bericht für die CCC, Tz. 294 sowie die Denkschrift zur Umsetzung der CCC ins nationale Recht, BT-Drucks. 16/7218, S. 55.

[144] *Gaede*, StV 2009, 96, 101 f.; *Gercke*, StrafFo 2009, 271, 273; *Meininghaus*, Zugriff auf E-Mails, S. 179; *Seitz*, Strafverfolgungsmaßnahmen im Internet, S. 415 f.

stimmung zum Zugriff auf die Daten durch die Ermittler rechtmäßig erteilen dürfen. Wer eine zur Weitergabe von Daten „rechtmäßig befugte Person" ist, kann je nach den Umständen, der Art der Person und dem jeweils anwendbaren Recht unterschiedlich sein.[145]

Fraglich ist dabei insbesondere, ob die zustimmungsberechtigte Person sich im Hoheitsgebiet der agierenden Strafverfolger aufhalten muss oder ob die Verfolger auch Personen im Ausland um eine Zustimmung ersuchen können. Für eine enge Sichtweise spricht, dass bereits das Ersuchen um Zustimmung gegenüber einer Person im Ausland zu einem weiteren Eingriff in die Souveränität des ausländischen Staates führen kann. Die deutsche Denkschrift zur Umsetzung der Konvention geht dementsprechend von einer Begrenzung auf befugte Personen im Inland aus.[146] Der Erläuternde Bericht zur Konvention verhält sich hierzu indes nicht ausdrücklich, stellt aber für die Bestimmung der „rechtmäßig befugten Person" auf das jeweils anwendbare Recht ab[147] und legt damit ebenfalls eine Eingrenzung auf Personen im Inland nahe. Allerdings muss der Berechtigte i.S.d. der Vorschrift nicht notwendig der von der Maßnahme unmittelbar Betroffene sein, denn nach dem Erläuternden Bericht kann z.B. auch der Provider als Zugangsberechtigter von den Strafverfolgern angesprochen werden.[148]

Weitere Schwierigkeiten können sich in der Praxis bei der Anwendung der Befugnis nach Art. 32 Buchstabe b) CCC dann ergeben, wenn keine gesetzlichen Spezialvorschriften für die Ermächtigung Dritter zur Weitergabe der jeweiligen Daten existieren. In diesen Konstellationen ist die Zulässigkeit des Abrufs der extraterritorial gespeicherten Daten nämlich von im konkreten Einzelfall für gewöhnlich nur eingeschränkt verlässlich aufzuklärenden Absprachen zwischen dem Berechtigten und demjenigen abhängig, der die Regeln für die Zugangsverteilungen festlegt. Vereinbaren diese Personen sogar, dass Dritten, insbesondere Strafverfolgungsbehörden, der Zugriff generell nicht gestattet werden darf, kann die Befugnis der Ermittler gänzlich leerlaufen, wenn nicht als Auffangtatbestände gesetzlich bestimmte Weitergabebefugnisse bestehen.

Abseits dieses Problemkreises ist der Umfang der Ermächtigung nach Art. 32 Buchstabe b) CCC aber auch deswegen beschränkt, weil der Betroffene den Zugang nicht nur zu gewähren berechtigt sein, sondern in der konkreten Situation diesen auch tatsächlich gewähren muss. Für eine solch enge Auslegung spricht, dass Art. 32 Buchstabe b) CCC die Einholung der Zustimmung fordert. Sowohl der

---

145 So der Erläuternde Bericht zur CCC, Tz. 294.

146 BT-Drucks. 16/7218, S. 55.

147 Erläuternder Bericht zur CCC, Tz. 294.

148 Ebenda; siehe hierzu auch *Meininghaus*, Zugriff auf E-Mails, S. 179, nach dem der Provider jedoch regelmäßig ausscheidet, da dieser aus seinem Verhältnis zu der Person, welche die Daten auf den Speicher ablegt, kein Recht habe, über die Daten zu verfügen; *Seitz*, Strafverfolgungsmaßnahmen im Internet, S. 415; *ders.*, IJCLP, Issue 9/2004, 1, 14.

Erläuternde Bericht zur Konvention als auch die Denkschrift zur Umsetzung der Vorgaben stellen daher auf eine eingeholte bzw. erteilte Zustimmung ab.[149] Der Berechtigte muss ferner dem Abruf freiwillig zustimmen. Damit scheidet eine zwangsfreie Durchsetzung des Zugangs bereits dann aus, wenn der Berechtigte gesetzlich verpflichtet ist, den Zugang zu gewähren.[150] In diesen Fällen beruht die Zugangsgewährung nämlich regelmäßig nicht mehr primär auf dem freien Willen, sondern auf der gesetzlichen Verpflichtung.

Ob sich neben der Rechtfertigung aus Art. 32 Buchstabe b) CCC schon eine allgemeine Befugnis zum Download im Ausland gespeicherter Daten mit Zustimmung des Berechtigten aus international anerkanntem Gewohnheitsrecht ergibt, ist zweifelhaft. Für eine solche spricht zwar, dass die angesprochene Regelung in der Convention on Cybercrime auf eine breite internationale Zustimmung bedeutender Staaten zurückgeht.[151] Auch nach Ansicht der G8-Gruppe[152] ist ein Rechtshilfeverfahren für diese Ermittlungsmaßnahmen nicht erforderlich. Es ist aber nicht belegt, inwieweit sich ebenfalls die Nichtunterzeichnerstaaten mit einer solchen Verfahrensweise einverstanden erklären. Hierbei ist insbesondere zu berücksichtigen, dass nach den Grundsätzen des Völkerrechts eine Privatperson gerade nicht eigenständig über das Recht zum Eingriff in ein fremdes Hoheitsgebiet disponieren kann, sondern allein der betroffene Staat. Eine Einwilligung Privater hat also abseits völkerrechtlicher Verträge für sich genommen überhaupt keinen Einfluss auf die Beurteilung der Eingriffssituation. Gegen eine allgemeinverbindliche, gewohnheitsrechtlich anerkannte Übung spricht zudem, dass schon allein die bei der Regelung des Art. 32 Buchstabe b) CCC aufgezeigten Schwierigkeiten der Bestimmung und Ausübung der Berechtigung selbst innerhalb des Regelungsgegenstands zu keiner vollständig klaren Ermittlungssituation beitragen. Daher kann ein Abruf mit Zustimmung des Berechtigten ohne eine spezielle Ermächtigungsnorm nur in Ausnahmefällen zulässig sein.[153]

---

[149] Erläuternder Bericht zur CCC, Tz. 294; Denkschrift zur Umsetzung der CCC ins deutsche Recht, BT-Drucks. 16/7218, S. 55.

[150] *Seitz*, Strafverfolgungsmaßnahmen im Internet, S. 415 f.; *ders.*, IJCLP, Issue 9/2004, 1, 14 f.

[151] Dahingehend argumentierend *Seitz*, Strafverfolgungsmaßnahmen im Internet, S. 416; *ders.*, IJCLP, Issue 9/2004, 1, 15.

[152] G8-Gruppe, Principles on transborder access to stored computer data, 1999, Principle No. 6 (b). Principle No. 6 (b) lautet: "Notwithstanding anything in these Principles, a State need not obtain authorization from another State when it is acting in accordance with its national law for the purpose of: […] (b) accessing, searching, copying, or seizing data stored in a computer system located in another State, if acting in accordance with the lawful and voluntary consent of a person who has the lawful authority to disclose to it that data."; siehe zur Ansicht des US Justizministeriums auch die Richtlinien „Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations" unter I., C., S. 15 ff., abrufbar unter http://www.justice.gov/criminal/cybercrime/docs/ssmanual2009.pdf [Stand: 6.11.2013].

[153] Zur Bestimmung der Ausnahmefälle im Folgenden unter Teil 3, II.D.3.b)bb).

b) Eigenständige Durchbrechung des Zugangsschutzes

Häufig werden die Strafverfolger freilich ohnehin auf zugangsgeschützte Daten treffen und sich entweder keine Zustimmung eines Berechtigten zum Zugriff beschaffen können oder ggf. aus ermittlungstaktischen Gründen eine solche gar nicht einholen wollen.

aa) Schwerer Eingriff in die Gebietshoheit fremder Staaten

Entsprechend den obigen Ausführungen liegt beim Zugriff auf im Ausland gespeicherte, zugangsgeschützte Daten durch die Strafverfolgungsbehörden ein Eingriff in die Gebietshoheit fremder Staaten vor. Der Download von Daten unter Überwindung eines Zugangsschutzes durch die Ermittlungsbehörden hat gegenüber dem Zugriff auf frei zugängliche Daten einen noch viel stärker hervortretenden hoheitlichen Charakter. Die Behörden greifen gegen den mit der Beschränkung nach außen dokumentierten Willen der Berechtigten auf die Daten zu, was traditionell hoheitlichem Handeln vorbehalten ist. Dies gilt insbesondere, wenn der Staat des Speicherorts, wie z.B. Deutschland in § 202a Abs. 1 StGB den unberechtigten Zugang zu Daten unter Überwindung einer besonderen Zugangssicherung unter Strafe gestellt hat.

bb) Ausnahmsweise Rechtfertigung des Eingriffs

Völkerrechtlich zulässig sind solche Zugriffe nur, wenn die Handlungen der Ermittlungsbeamten gerechtfertigt wären, also entweder völkerrechtliche Verträge sie zum Download zugangsgeschützter Daten ermächtigen würden, es nach dem Völkergewohnheitsrecht eine allgemein anerkannte Übung für den beschriebenen Zugriff gäbe oder von den Kulturvölkern allgemein anerkannte Rechtsgrundsätze ein solches Vorgehen rechtfertigen würden.

Eine Rechtfertigung kraft völkerrechtlicher Verträge, insbesondere in Form der Convention on Cybercrime, liegt nicht vor. Die Regelungen in Art. 32 CCC betreffen nur den grenzüberschreitenden Zugriff auf gespeicherte Computerdaten mit Zustimmung des Berechtigten oder auf öffentlich zugängliche Daten. Die Verfasser der Konvention wollten nach den Ausführungen in Nr. 293 des Erläuternden Berichts den Zugriff auf geschützte Daten gegen den Willen des Berechtigten nicht regeln, sondern solche Fälle offen lassen, bis mehr Erfahrungen vorlägen und diskutiert wären. Aus dem Übereinkommen über Computerkriminalität lassen sich daher, insbesondere unter Berücksichtigung von Art. 39 Abs. 3 CCC, der bestimmt, dass das „Übereinkommen […] andere Rechte, Beschränkungen, Pflichten und Verantwortlichkeiten einer Vertragspartei unberührt [lässt]“, weder Ansätze für noch gegen eine Zulässigkeit des Zugriffs auf geschützte Quellen destillieren.[154]

---

[154] Ebenso *Gercke*, StraFo 2009, 271, 273; *Seitz*, Strafverfolgungsmaßnahmen im Internet, S. 418; *ders*., IJCLP, Issue 9/2004, 1, 16.

Einen direkten Zugriff auf zugangsgeschützte, im Ausland gespeicherte Daten vom Inland aus erlauben auch die Bestimmungen des Rahmenbeschlusses über die Vollstreckung von Entscheidungen und über die Sicherstellung von Vermögensgegenständen oder Beweismitteln[155] nicht. Zwar entfällt nach Art. 3 Abs. 2 des Rahmenbeschlusses für Sicherstellungsentscheidungen,[156] u.a. auch bei Straftaten der Cyberkriminalität, in Rechtshilfeverfahren die Prüfung der beiderseitigen Strafbarkeit, sodass die Sicherstellungsentscheidung des ersuchenden Staates gemäß Art. 5 Abs. 1[157] unmittelbar anerkannt wird, gleichwohl nimmt aber der ersuchte Staat immer noch eigenständig die erforderlichen Maßnahmen auf seinem Hoheitsgebiet selbst vor. Eine unmittelbare Ausübung von Hoheitsgewalt auf fremdem Staatsgebiet rechtfertigt Art. 5 Abs. 1 hingegen nicht. Abseits multi- und bilateraler Verträge kommt für den konkreten Einzelfall als ausdrückliche Erlaubnis daher nur eine Einwilligung in Betracht, welche die Strafverfolger auf dem normalen, regelmäßig förmlichen Weg der internationalen Rechtshilfe erlangen können.[158]

Fraglich ist, ob sich neben einer solchen ausdrücklichen Erlaubnis im Ausnahmefall eine Rechtfertigung aus dem Völkergewohnheitsrecht herleiten lässt. Eine allgemein anerkannte Übung, nach der die Staaten damit einverstanden sind, dass Ermittlungsbehörden über Computernetze unter Überwindung von Zugangssperren auf im Ausland gespeicherte Daten zugreifen, ist mangels entsprechender dokumentierter Staatenpraxis nicht nachweisbar. Im Gegenteil, in international angelegten Studien sowie in Vorschlägen internationaler Vereinigungen und Organisationen finden sich sogar Hinweise darauf, dass die Staaten den eigenmächtigen grenzüberschreitenden Abruf zugangsgeschützter Daten generell als unzulässigen

---

155 Rahmenbeschluss 2003/577/JI des Rates vom 22. Juli 2003 über die Vollstreckung von Entscheidungen über die Sicherstellung von Vermögensgegenständen oder Beweismitteln in der Europäischen Union, ABl. EU 2003, Nr. L 196, S. 45 ff.; zu den Umsetzungsbemühungen vgl. den Gesetzentwurf der Bundesregierung BT-Drucks. 16/6563.

156 Art. 3 Abs. 2 des Rahmenbeschlusses 2003/577/JI lautet: „(2) Bei folgenden nach dem Recht des Entscheidungsstaats definierten Straftaten erfolgt keine Überprüfung des Vorliegens der beiderseitigen Strafbarkeit, wenn sie im Entscheidungsstaat mit einer Freiheitsstrafe im Höchstmaß von mindestens drei Jahren bedroht sind: […] Cyberkriminalität […]."

157 Art. 5 Abs. 1 des Rahmenbeschlusses 2003/577/JI lautet: „(1) Die zuständige Justizbehörde des Vollstreckungsstaats erkennt jede nach Artikel 4 übermittelte Sicherstellungsentscheidung ohne weitere Formalität an und trifft unverzüglich die erforderlichen Maßnahmen für deren unmittelbare Vollstreckung auf dieselbe Weise wie bei einer von einer Behörde des Vollstreckungsstaats erlassenen Sicherstellungsentscheidung, es sei denn, die betreffende Behörde beschließt, einen der Gründe für die Versagung der Anerkennung oder der Vollstreckung nach Artikel 7 oder einen der Gründe für den Aufschub nach Artikel 8 geltend zu machen. […]."

158 Siehe für die internationale Rechtshilfe die Ausführungen unter Teil 3, III.

völkerrechtswidrigen Eingriff in fremde Souveränitätsrechte betrachten.[159] Soweit in der Literatur auf praktische Fälle des Fernzugriffs auf geschützte Daten hingewiesen wird,[160] sind dies Einzelfälle, aus denen sich jedenfalls speziell für das in Rede stehende Vorgehen keine allgemein anerkannte Übung herleiten lässt bzw. gerade im Gegenteil aufgrund von Einsprüchen gegen das Vorgehen, das Berufen auf die eigene Souveränität deutlich wird.

Zu überlegen bleibt daher nur, ob und ggf. wann im Einzelfall die Überwindung von Zugriffssperren nach den allgemeinen Grundsätzen des Völkerrechts[161] gerechtfertigt sein könnte.[162] Dem Gebot der Achtung der Gebietshoheit kommt, wie die vorhergehenden Durchbrechungen bei den bereits dargestellten Maßnahmen verdeutlicht haben, nicht der Charakter eines ausnahmslosen Rechtsprinzips zu. Zwar resultiert das Verbot des Eingriffs in das Hoheitsgebiet fremder Staaten aus dem grundsätzlichen Abwehrinteresse des im Kern seiner Souveränität betroffenen Staates, sodass ohne Einwilligung im Einzelfall oder aufgrund eines multilateralen Vertrags kaum Fallgestaltungen denkbar sind, in denen dieses Abwehrinteresse überwogen wird mit der Folge, dass keine Ausnahmefälle existieren, die im Verlaufe der Zeit regelmäßig genug hätten auftreten können, um eine gängige einschränkende Praxis begründen zu können. Dennoch sind Konstellationen – auch mit Blick auf die Regeln zur Staatenverantwortlichkeit, insbesondere Art. 20 ff.[163] – denkbar, in denen der eingreifende Staat für die Verletzung der fremden Gebietshoheit nicht verantwortlich ist. Dies ist namentlich dann der Fall, wenn die Interessen des eingreifenden Staates gegenüber dem Abwehrinteresse des betroffenen

---

[159] Council of Europe, Recommendation No. (95) 13, Erläuternder Bericht für Recommendation No. (95) 13, Tz. 80, 187 ff.; *Sieber*, COMCRIME-Study, S. 107; United Nations, Manual on the prevention and control of computer-related crime, Tz. 264 ff.

[160] Siehe *Koops/Brenner*, in: dies., Cybercrime and Jurisdiction, S. 1, 3; *Seitz*, Strafverfolgungsmaßnahmen im Internet, S. 419 ff.; *ders.*, IJCLP, Issue 9/2004, 1, 2 ff.; *Walden*, Computer Crimes and Digital Investigations, S. 320 f., Rn. 5.76 ff., die den Fall *United States ./. Gorshkow & Ivanov* beschreiben, in dem das FBI Rechner und Dateien von Hackern in Russland durchsuchte und aufgefundene Daten in die USA online übertrug, was zu diplomatischen Spannungen führte. Zur vom FBI auf einem italienischen Rechner eingesetzten Spyware CIPAV (Computer and Internet Protocol Address Verifier) siehe auch die eidesstattliche Erklärung des U.S. FBI Special Agent *Norman B. Sanders, Jr.* vor dem U.S. District Court, Western District of Washington, abrufbar unter http://www.politechbot.com/docs/fbi.cipav.sanders.affidavit.071607.pdf [Stand: 6.11.2013].

[161] Diese gehören zur Rechtsquelle des Völkergewohnheitsrechts, weil sie ihren Ursprung in den internationalen Beziehungen haben und nicht wie die von den Kulturvölkern allgemein anerkannten Rechtsgrundsätze lediglich Prinzipien sind, die zumindest in den meisten nationalen Rechtsordnungen zu finden sind, also keinem primären völkerrechtlichen Rechtserzeugungsverfahren entstammen. Siehe hierzu *Doehring*, Völkerrecht, Rn. 408; *Ipsen*, Völkerrecht, § 17, Rn. 1; *Stein/v. Buttlar*, Völkerrecht, Rn. 161.

[162] Gegen eine solche Rechtfertigung außerhalb gesetzlicher Eingriffsgrundlagen *Meininghaus*, Zugriff auf E-Mails, S. 180 ff.; ihm folgend *Gercke*, StrafFo 2009, 271, 273.

[163] Responsibility of States for Internationally Wrongful Acts (2001), ILC, A/CN 4 L. 602, Rev. 1, auch als Annex der kenntnisnehmenden Resolution der UN-Generalversammlung (A/RES/56/83); abgedruckt in *Tomuschat*, Völkerrecht, Ordnungsnummer 9.

Staates zumindest gleichwertig sind.[164] Wie bereits bei der Regelungskompetenz eines Staates für Sachverhalte mit Auslandsbezug dargestellt,[165] ist die Befugnis der Staaten, bei Auslandsbezügen tätig zu werden, nur beschränkt durch die im konkreten Fall entgegenstehenden Interessen anderer Staaten. Das Eingriffsinteresse ist dem Abwehrinteresse des anderen Staates gegenüberzustellen und die Interessen sind gegeneinander abzuwägen.[166]

Dass die danach infrage kommenden Fälle eines zumindest gleichwertigen Eingriffsinteresses bei Eindringen in fremdes Hoheitsgebiet selten sind, zeigt bereits die auf Einzelfälle beschränkte dokumentierte Staatenpraxis.[167] Aus rechtlicher Sicht müssen diese Fälle ebenfalls vereinzelte Ausnahmen bleiben, weil das Abwehrinteresse eben immer auch eine Frage des Bestands des betroffenen Staats an sich und damit sehr hoch anzusetzen ist. Jede hoheitliche Einflussnahme von außen untergräbt nicht nur die staatliche Autorität, sondern führt zu Rechtsunsicherheiten und einem politischen Handlungsdruck, der Spielräume einengt. Gemessen hieran müssen die Eingriffsinteressen eine Qualität erreichen, wie sie z.B. bei Bedrohungen des Bestandsinteresses des zugreifenden Staates (also insbesondere bei Staatsschutzdelikten) zum Ausdruck kommt. Auch Fälle, in denen die Verweigerung staatlichen Schutzes zu einer schweren Erschütterung der inneren Stabilität führte (etwa bei massiver offener Unterstützung terroristischer oder krimineller Organisationen aus dem Ausland), können ein hinreichendes Interesse begründen. Der Schutz von Individualgütern hingegen, die nicht im unmittelbaren Interesse eines Staates stehen, ergibt nur dort ein ausreichendes Eingriffsinteresse, wo besondere staatliche Schutzverpflichtungen bestehen. Dies kann etwa der Schutz des unmittelbar bedrohten Lebens,[168] der sich aus der Menschenrechtskonvention[169] ableiten lässt,[170] sein.

---

[164] Siehe zur Überwindung entgegenstehender Interessen bei Gleichwertigkeit die Ausführungen unter Teil 2, II.C.4.a)cc)(3)(d)(bb).

[165] Siehe hierzu die Ausführungen unter Teil 2, II.C.4.a)cc)(3).

[166] Insoweit widersprüchlich *Schantz*, KritV 2007, 310, 328 f., der die abwägenden Ausnahmevorschriften der Art. 20 ff. und 49 ff. der UN-Resolution A/RES/56/93 anführt, aber gleichwohl eine Abwägung bestreitet.

[167] So sollen z.B. US-amerikanische Behörden bei der Vereitelung der Anschlagsversuche mit Autobomben in Deutschland im September 2007 sog. Online-Durchsuchungen auch auf fremdem Staatsgebiet durchgeführt haben. Siehe hierzu *Miriam Lau*, Deutscher Terrorkampf mit US-Methoden, Die Welt, 6.9.2007, abrufbar unter http://www.welt.de/politik/deutschland/article1163552/Deutscher_Terrorkampf_mit_US-Methoden.html [Stand: 6.11.2013].

[168] Siehe hierzu auch Art. 1 Abs. 7 des Gemeinsamen Standpunkts vom 27.5.1999 – vom Rat aufgrund von Artikel 34 des Vertrags über die Europäische Union festgelegt – zu den Verhandlungen im Europarat über das Übereinkommen über Cyber-Kriminalität, ABl. EG 1999, Nr. L 142, S. 1, 2.

[169] Konvention zum Schutze der Menschenrechte und Grundfreiheiten vom 4. November 1950 in der Fassung der Bekanntmachung vom 17. Mai 2002 (BGBl. II 2002, S. 1055 ff.), zuletzt geändert durch Gesetz zu dem Protokoll Nr. 14 vom 13.5.2004 zur

E. Upload von Daten als Souveränitätsverletzung

Neben dem untersuchten Download kennzeichnet der Upload von Daten durch die Strafverfolgungsbehörden im Internet ebenfalls einen wichtigen Teil der Ermittlungsarbeit im Computernetzwerk; so finden sich beispielsweise auf Webseiten Fahndungsaufrufe nach bestimmten Personen oder es wird um Mithilfe bei der Aufklärung von Straftaten gebeten. Da der Abruf dieser Fahndungsaufrufe wiederum nicht auf das eigene Staatsgebiet beschränkt ist, könnte hiermit abermals ein rechtfertigungsbedürftiger Eingriff in die Gebietshoheit fremder Staaten verbunden sein.

1. Inländische Fahndungsaufrufe auf Servern im eigenen Staatsgebiet

Nach zutreffender überwiegender Ansicht ist das Einstellen solcher Daten durch die Ermittlungsbehörden auf Host-Servern im eigenen Staatsgebiet in den Fällen, in denen die inländische Bevölkerung zur Mithilfe angesprochen wird, völkerrechtlich nicht zu beanstanden.[171] Mit diesen Maßnahmen treten die Ermittlungsbehörden nämlich nicht in Konkurrenz zur Hoheitsmacht anderer Staaten, sondern beziehen sich primär auf die Regelung innerstaatlicher Angelegenheiten. Der Upload der Daten durch die Strafverfolgungsbehörden auf inländische Server unterscheidet sich überdies von den bereits dargestellten Maßnahmen insbesondere dadurch, dass der Auslandsbezug überhaupt erst durch Internetnutzer im Ausland aktiv hergestellt werden kann. Für die Zurechnung dieses Zugriffs zum einstellenden Staat müssen jedoch Umstände hinzutreten, die darauf schließen lassen, dass ein solcher Abruf auch gewollt war.[172] Die allein mit der Einstellung der Daten u.U. verbundenen Auswirkungen auf fremdes Staatsgebiet stellen nur einen schlicht unvermeidbaren Reflex der Ausübung eigener Hoheitsgewalt auf eigenem Staatsgebiet dar. Mit dem Upload der Daten auf im Inland gehostete Webseiten treten die Ermittlungsbehörden außerdem weder mit Behörden des Auslands derart in Kontakt, dass sie diese um Mithilfe bei einem Strafverfahren ersuchen, noch wenden sie sich unmittelbar an ausländische Privatpersonen.[173] Vergleichbar mit der Ausstrahlung einer Fahn-

---

Konvention zum Schutz der Menschenrechte und Grundfreiheiten über die Änderung des Kontrollsystems der Konvention (BGBl. II 2006, S. 138 ff.).

[170] Siehe dazu etwa den von *Seitz*, Strafverfolgungsmaßnahmen im Internet, S. 419 ff. angeführten praktischen Fall, in welchem das US-amerikanische FBI auf geschützte Daten auf einem in Russland befindlichen Server zugriff, um die Gefahr massenhafter Flugzeugangriffe abzuwehren.

[171] *Germann*, Gefahrenabwehr und Strafverfolgung im Internet, S. 649 f.; *Marberth-Kubicki*, Computer- und Internetstrafrecht, S. 264, Rn. 560; *Meseke*, FS Herold, S. 505, 528; *Seitz*, Strafverfolgungsmaßnahmen im Internet, S. 427; *Soiné*, NStZ 1997, 166, 167; *Valerius*, Ermittlungen der Strafverfolgungsbehörden, S. 160 f.; KMR-*Wankel*, § 131a, Rn. 4.

[172] *Valerius*, Ermittlungen der Strafverfolgungsbehörden, S. 160.

[173] *Soiné*, NStZ 1997, 166, 167.

dung in einer Fernsehsendung, welche ebenfalls durch Personen im Ausland empfangen werden kann, oder einem Fahndungsaufruf in einer Zeitung, die desgleichen in anderen Staaten erhältlich ist, ist auch mit der Internetfahndung kein rechtswidriger Eingriff in die Gebietshoheit verbunden.[174]

Soweit vereinzelt die Fahndung über das Internet nicht nur als Öffentlichkeitsfahndung, sondern stets auch als eine internationale Fahndung angesehen wird,[175] sodass ein rechtfertigungsbedürftiger Eingriff in die Gebietshoheit fremder Staaten mit der Maßnahme einherginge, kann dem nicht zugestimmt werden. Gegen die Charakterisierung jeder Internetfahndung als internationale Fahndung i.S.d. der Anlage F der Richtlinien für Straf- und Bußgeldverfahren (RiStBV) spricht, dass weder die Verwendung des Internet zur Fahndung noch die ggf. mehrsprachige Ausgestaltung des Aufrufs in einer multikulturellen Gesellschaft allein stichhaltige Indizien für die Vermutung sind, die Person werde im Ausland gesucht.[176] Nur soweit die Ermittlungsbehörden annehmen, dass sich die gesuchte Person im Ausland befindet, und ein Auslieferungsersuchen bei Ermittlung des Gesuchten vorbereiten, ist von einer internationalen Fahndung i.S.d. Richtlinien über die internationale Fahndung nach Personen einschließlich der Fahndung nach Personen im Schengener Informationssystem[177] zu sprechen.

2. Internationale Fahndungsaufrufe auf Servern im eigenen Staatsgebiet

Richtet sich die Fahndung auf ein Aufspüren der gesuchten Person oder des Gegenstands im Ausland, ändert sich dagegen die rechtliche Beurteilung, da in diesen Konstellationen primär auch ausländische Personen um Mithilfe gebeten werden. Die Fahndung wirkt sich dann trotz Einstellens der Daten auf einen inländischen Server auch wesentlich im Ausland aus, sodass in diesen Konstellationen der extraterritoriale Hoheitsakt völkerrechtlich rechtfertigungsbedürftig ist. Die Abrufe der Fahndungsaufrufe aus dem Ausland sind nicht mehr zufällig und unvermeidbar, sondern vielmehr maßgeblich auf den Auslandsbezug zurückzuführen, sodass sich die Wirkung der Ermittlungsmaßnahme über die Staatsgrenzen hinweg nicht allein aufgrund des Grenzen ignorierenden Computernetzes ergibt, sondern zielgerichtet ausgenutzt wird. Bereits bei dem grenzüberschreitenden Rundfunk und später dem Satellitendirektfernsehen hat die völkerrechtliche Literatur zwischen *inevitable spill-over* und *intended spill-over* differenziert.[178] Während die

---

174 *Valerius*, Ermittlungen der Strafverfolgungsbehörden, S. 160; KMR-*Wankel*, § 131a, Rn. 4.

175 *Pätzel*, NJW 1997, 3131, 3132.

176 *Bär*, CR 1997, 422, 429; *Valerius*, Ermittlungen der Strafverfolgungsbehörden, S. 160 f.

177 Anlage F der RiStBV, für das Land Brandenburg: Allgemeine Verordnung vom 21.2.1994, ABl. Bbg. 1994, S. 78 ff.

178 Siehe hierzu *Engel*, RabelsZ 49 (1985), 90, 97.

Staaten grenzüberschreitende Sendungen so lange als aus Souveränitätssicht irrelevant einstuften, wie sie technisch unvermeidbar auch auf fremdes Staatsgebiet übertragen wurden *(inevitable spill-over)*, stießen die Fälle des *intended spill-over*, bei denen Sendungen gezielt auch auf das Ausland abgestrahlt wurden und deren Inhalt nicht mehr nur vornehmlich innerstaatliche Belange des Sendestaats betrafen, hingegen vermehrt auf Widerstand.[179] Daraus folgt für die Fahndung über das Internet in den Fällen der Suche nach Personen im Ausland, dass sich diese Maßnahme auf fremdes Staatsgebiet auswirkt, insbesondere die innerstaatliche Sicherheit und Ordnung der betroffenen fremden Staaten berührt. Der mit der Ermittlungshandlung einhergehende Eingriff bedarf folglich der Rechtfertigung. Spezielle Ermächtigungsgrundlagen stehen für einen solchen Eingriff jedoch nicht zur Verfügung.

3. Fahndungsaufrufe auf Servern im Ausland

Der Eingriff in die Gebietshoheit fremder Staaten vertieft sich noch weiter, wenn sich der Fahndungsaufruf nicht nur an ein weltweites Publikum richtet, sondern er auch noch auf ausländischen Servern publiziert wird. Soweit deutsche Behörden mit dem Gedanken spielen, für ihre Aufrufe z.B. im Ausland gehostete Web-2.0-Plattformen wie YouTube oder Myspace nutzen zu wollen,[180] müssen sie ein solches Vorhaben auf eine völkerrechtlich hinreichende Ermächtigungsgrundlage stellen. Sie können völkerrechtsgemäß nicht eigenständig ihren Aufruf zur Fahndung auf im Ausland von Privaten gehostete Server einstellen. Mangels spezieller Regelungen bleibt ihnen auch hier nur der Weg der Rechtshilfe. Fraglich ist jedoch, inwieweit die Rechtshilfe eine Einstellung von Fahndungsaufrufen auf privaten Webseiten ermöglicht. Zum einen können nämlich auf dem Weg der internationalen Rechtshilfe nur fremde staatliche Behörden um Hilfe gebeten werden und zum anderen würde eine erfolgreiche Einstellung des Fahndungsaufrufs voraussetzen, dass die ersuchte Behörde Private im Zweifelsfall verpflichten könnte, ausländische Fahndungsaufrufe zu publizieren. Als weiterer Problemkreis kommt hinzu, dass die ersuchende Behörde Aufrufe auf fremden Servern privater Dritter nicht mehr selbst beeinflussen, insbesondere diese nicht mehr selbstständig beenden kann. Damit vertieft sich jedoch der ohnehin bei einer internationalen Fahndung schon schwere Eingriff in das Persönlichkeitsrecht des Betroffenen erneut exorbitant, nicht zuletzt vor dem Hintergrund, dass einmal eingestellte Inhalte sich kaum mehr entfernen lassen.

---

[179] Ebenda, 90, 99 ff.

[180] *Löffel*, Internet-Surfer gehen auf Patrouille, Frankfurter Rundschau vom 17.3.2007.

III. Internationale Rechtshilfe

Soweit die Strafverfolgungsbehörden mit den vorgenannten Ermittlungsmaßnahmen in die Gebietshoheit fremder Staaten eingreifen und nicht bereits aufgrund von Völkergewohnheitsrecht generell oder aus einer konkreten Ermächtigungsnorm oder Einwilligung heraus im Einzelfall gerechtfertigt sind, müssen sie den Weg der internationalen Rechtshilfe beschreiten. Einen allgemeinen Grundsatz der Pflicht zur Leistung von Rechtshilfe enthält das Völkerrecht zwar nicht. Jeder Staat kann aber von sich aus, auch ohne hierzu gesondert verpflichtet zu sein, freiwillig Rechtshilfe leisten.[181] Praktisch kommt die Staatengemeinschaft zudem nicht umhin, sich gemeinsam den mit transnationalen Kriminalitätsformen verbundenen Herausforderungen an die Strafverfolgung durch Gewährung gegenseitiger Hilfe zu stellen, da alle Staaten über kurz oder lang zunehmend mit grenzüberschreitenden Straftaten konfrontiert sind. Bei der Bekämpfung der Datennetzkriminalität kommt hinzu, dass schon aufgrund der Grenzen ignorierenden Arbeitsweise von Computernetzen die Strafverfolgungsbehörden zur Zusammenarbeit gezwungen sind.[182] Voraussetzung für die erfolgreiche Leistung von Rechtshilfe ist allerdings, dass nicht zuletzt durch Harmonisierung sowohl das materielle Recht als auch das Prozessrecht vereinheitlicht wird,[183] denn die Gewährung der Hilfe ist für gewöhnlich davon abhängig, dass zum einen die Tat auch nach dem Recht des ersuchten Staates strafbar ist und zum anderen, dass der ersuchte Staat selbst die ersuchte Ermittlungshandlung nach nationalem Recht legal vornehmen darf.[184]

Obwohl jeder Staat freiwillig Rechtshilfe leisten kann, ohne hierzu gesondert verpflichtet zu sein,[185] ist die Gewährung von Rechtshilfe aufgrund vertraglicher Übereinkommen gleichwohl am verbreitetsten.

Die wichtigsten rechtlichen Regelwerke hierfür sind systematisiert nach ihrem Ursprung, u.a. die Übereinkommen des Europarates, wozu insbesondere das Europäische Übereinkommen über die Rechtshilfe in Strafsachen (EuRhÜbk)[186] zählt,

---

[181] *Nagel*, Beweisaufnahme im Ausland, S. 72 f.; *Schuster*, Verwertbarkeit im Ausland gewonnener Beweise, S. 26, 116; *Schwörer*, wistra 2009, 452, 453.

[182] *Putnam/Elliott*, in: Sofaer/Goodman, Transnational Dimension of Cyber Crime and Terrorism, S. 35, 35 f.; *Sofaer/Goodman*, in: dies., Transnational Dimension of Cyber Crime and Terrorism, S. 1, 33; United Nations, Manual on the prevention and control of computer-related crime, Tz. 268 ff.

[183] AIDP, International Review of Penal Law, vol. 66 (1995), No. 1/2, 60, Tz. 22; Council of Europe, Extraterritorial criminal jurisdiction, S. 32; *Sieber*, COMCRIME-Study, S. 133; *ders.*, The international handbook on computer crime, S. 114. Siehe auch *Putnam/Elliott*, in: Sofaer/Goodman, Transnational Dimension of Cyber Crime and Terrorism, S. 35, 53; *Walden*, Computer Crimes and Digital Investigations, S. 328 f., Rn. 5.101.

[184] Siehe zu dadurch in der Praxis verursachten Problemen auch BMI/BMJ, Erster Periodischer Sicherheitsbericht, S. 203 f.

[185] *Nagel*, Beweisaufnahme im Ausland, S. 72 f.; *Schuster*, Verwertbarkeit im Ausland gewonnener Beweise, S. 26, 116.

[186] European Convention on Mutual Assistance in Criminal Matters (ETS No. 30), in Deutschland in Kraft getreten im Jahr 1977, BGBl. II 1964, S. 1369, 1386; BGBl. II 1976,

welches Vorschriften für den Rechtshilfeverkehr der Justizbehörden vor allem der europäischen Staaten enthält, sowie die Konvention zum Schutze der Menschenrechte und Grundfreiheiten (EMRK),[187] in der vorwiegend die Prinzipien eines rechtsstaatlichen und fairen Verfahrens niedergelegt sind. Das für die Bekämpfung der Datennetzkriminalität wohl bedeutendste internationale Regelwerk ist jedoch die Convention on Cybercrime (CCC),[188] welche auch Nichtmitgliedstaaten des Europarates zur Unterzeichnung offensteht und nicht zuletzt daher ebenfalls durch andere intergouvernementale Organisationen beworben wird.[189] Das Übereinkommen über Computerkriminalität weicht die strengen Regeln der traditionellen Rechtshilfe zum Teil auf, erlaubt aber gleichwohl prinzipiell keine eigenständigen grenzüberschreitenden Ermittlungen der Strafverfolgungsbehörden.[190]

Aus dem Rechtskreis der Europäischen Union sind am bedeutsamsten das Schengener Durchführungsübereinkommen (SDÜ)[191] der Schengen-Staaten, welches sich vornehmlich mit der Zusammenarbeit der polizeilichen Behörden befasst, das Übereinkommen über die Rechtshilfe zwischen den Mitgliedstaaten der Euro-

---

1799; BGBl. I 1982, S. 2071. Ergänzt wurde das EuRhÜbk durch zwei Zusatzprotokolle (ETS No. 99, 182). Zu den Herausforderungen der Rechtshilfeleistung in Anwendung des EuRhÜbk auf die grenzüberschreitende Datennetzkriminalität siehe Council of Europe, Recommendation No. (89) 9, Erläuternder Bericht, S. 91 ff.; ders., Recommendation No. (95) 13, Erläuternder Bericht, Tz. 194 ff.; OECD, Computer-related Crime: Analysis of Legal Policy, S. 68.

187 Convention for the Protection of Human Rights and Fundamental Freedoms (ETS No. 5); Konvention zum Schutze der Menschenrechte und Grundfreiheiten vom 4.11.1950 in der Neufassung vom 17.5.2002, BGBl. II 2002, S. 1055 ff., zuletzt geändert durch Gesetz zu dem Protokoll Nr. 14 vom 13.5.2004 zur Konvention zum Schutze der Menschenrechte und Grundfreiheiten über die Änderung des Kontrollsystems der Konvention (BGBl. II 2006, S. 136 ff.).

188 Europarat, ETS No. 185.

189 Siehe hierzu beispielsweise den Aufruf zum Beitritt zur Convention on Cybercrime durch die G8-Gruppe in dem 2002 überarbeiteten Katalog G8 Recommendations on Transnational Crime, Part IV, Section D, No. 2; die Unterstützung durch die Organisation der Amerikanischen Staaten (OSA) 2004 im final report of the fifth meeting of ministers of justice or of ministers or attorneys general of the Americas (REMJA-V), Anhang 1, Schlussfolgerungen und Vorschläge der REMJA-V, unter IV, 8, abrufbar unter http://www.oas.org/juridico/english/ministry_of_justice_v.htm [Stand: 6.11.2013]; sowie die Empfehlung von Interpol in der Resolution zum Abschluss der 6th International Conference on Cyber Crime 2005, abrufbar unter http://www.interpolitex.ru/en/news/-security/21840.html [Stand: 6.11.2013]. Vgl. aber auch die Überlegungen innerhalb der UN zur Konzipierung einer UN-Konvention zur Bekämpfung von Computerkriminalität, Eleventh United Nations Congress on Crime Prevention and Criminal Justice, Bangkok, 18–25 April 2005, Report of the Eleventh United Nations Congress on Crime Prevention and Criminal Justice, Dokument: A/CONF.203/18, S. 90, Tz. 338.

190 Siehe hierzu die Anmerkungen in der Denkschrift zur Ratifizierung der Convention on Cybercrime, BT-Drucks. 16/7218, S. 52; *Möhrenschlager*, in: Welp, kriminalität@net, S. 97, 110.

191 Übereinkommen zur Durchführung des Übereinkommens von Schengen vom 19.6.1990, BGBl. II 1993, S. 1010, 1902, zuletzt geändert durch Verordnung Nr. 1160/2005 des Europäischen Parlaments und des Rates vom 6.7.2005, ABl. EG 2005, Nr. L 191, S. 18.

päischen Union (EU-RhÜbk),[192] welches die zwischen den Mitgliedern der Union bereits geltenden Rechtshilfeverträge ergänzen soll, und der Rahmenbeschluss über den Europäischen Haftbefehl, der das Auslieferungsrecht im Sinne des Grundsatzes der gegenseitigen Anerkennung novelliert.[193] Ferner sind für Strafverfahren der Rahmenbeschluss über die Vollstreckung von Entscheidungen und über die Sicherstellung von Vermögensgegenständen oder Beweismitteln,[194] der Rahmenbeschluss über die Europäische Beweisanordnung[195] sowie der Rahmenbeschluss über den Schutz personenbezogener Daten im Rahmen der polizeilichen und justiziellen Zusammenarbeit in Strafsachen[196] zu nennen, während weitere Vorschläge für Rahmenbeschlüsse, welche die Zusammenarbeit auch der Strafverfolgungsbehörden erleichtern,[197] immer noch ihrer Verabschiedung harren.

Daneben sind insbesondere zahlreiche bilaterale Abkommen und nationale Regelungen von Wichtigkeit, wie beispielsweise das Gesetz über die Internationale Rechtshilfe in Strafsachen (IRG),[198] das vor allem die Leistung von Rechtshilfe für ausländische Strafverfahren ohne Verpflichtung in einem völkerrechtlichen Vertrag zum Regelungsgegenstand hat, und die Richtlinien für den Verkehr mit dem Ausland in strafrechtlichen Angelegenheiten (RiVASt),[199] welche die zwischen den

---

[192] ABl. EG 2000, Nr. C 197, S. 3 ff. Ergänzt durch den Rechtsakt des Rates vom 16.10.2001 über die Erstellung – gemäß Artikel 34 des Vertrages über die Europäische Union – des Protokolls zu dem Übereinkommen über die Rechtshilfe in Strafsachen zwischen den Mitgliedstaaten der Europäischen Union, ABl. EG 2001, Nr. C 326, S. 1 ff.

[193] Rahmenbeschluss des Rates vom 13.6.2002 über den Europäischen Haftbefehl und die Übergabeverfahren zwischen den Mitgliedstaaten (2002/584/JI), ABl. EG 2002, Nr. L 190, S. 5 ff.; umgesetzt mit Gesetz vom 20.7.2006, BGBl. I 2006, S. 1721 ff.

[194] Rahmenbeschluss 2003/577/JI des Rates vom 22.7.2003 über die Vollstreckung von Entscheidungen über die Sicherstellung von Vermögensgegenständen oder Beweismitteln in der Europäischen Union, ABl. EU 2003, Nr. L 196, S. 45 ff.; zu den Umsetzungsbemühungen vgl. den Gesetzentwurf der Bundesregierung BT-Drucks. 16/6563.

[195] Rahmenbeschluss 2008/978/JI des Rates vom 18.12.2008 über die Europäische Beweisanordnung zur Erlangung von Sachen, Schriftstücken und Daten zur Verwendung in Strafverfahren, ABl. EU 2008, Nr. L 350, S. 72 ff.; näher zur Europäischen Beweisanordnung *Roger*, GA 2010, 27 ff.

[196] Rahmenbeschluss 2008/977/JI des Rates über den Schutz personenbezogener Daten, die im Rahmen der polizeilichen und justiziellen Zusammenarbeit in Strafsachen verarbeitet werden, ABl. EU 2008, Nr. L 350, S. 60 ff.

[197] So z.B. der Vorschlag der Kommission für einen Rahmenbeschluss des Rates über den Austausch von Informationen nach dem Grundsatz der Verfügbarkeit, KOM(2005) 490 endg.

[198] BGBl. I 1982, S. 2071 i.d.F. der Bekanntmachung vom 27.6.1994, BGBl. I 1994, S. 1537 ff.

[199] Richtlinien für den Verkehr mit dem Ausland in strafrechtlichen Angelegenheiten vom 18.9.1984 (BAnz. Nr. 176 vom 18.9.1984 i.V.m. der Beilage Nr. 47/84) i.d.F. der am 1.3.1993 in Kraft getretenen Änderungsbekanntmachung (BAnz. Nr. 40a vom 27.2.1993); abgedruckt z.B. in *Schomburg* et al., Internationale Rechtshilfe in Strafsachen; im Übrigen abrufbar unter http://www.datenbanken.justiz.nrw.de/pls/jmi/ir_rivast_start [Stand: 6.11.2013].

Landesregierungen und der Bundesregierung vereinbarten – lediglich behördenintern geltenden – Verwaltungsvorschriften enthalten.

Welche Voraussetzungen die Strafverfolgungsbehörden beim Beschreiten des Weges der internationalen Rechtshilfe beachten müssen, wem die Leitung und Kontrolle grenzüberschreitender Ermittlungen obliegt und welche Hindernisse bei der Zusammenarbeit grenzüberschreitender Strafverfolgung zu bewältigen sind, kann insbesondere in der Kommentarliteratur,[200] umfangreichen Monografien[201] und der Rechtsprechung[202] verfolgt werden und wird daher hier nicht näher vertieft, um den Rahmen der Arbeit nicht zu sprengen.

IV. Verwertungsverbot für völkerrechtswidrig erlangte Beweise

Verstoßen die Strafverfolgungsbehörden nach den obigen Ausführungen bei der Durchführung von Ermittlungsmaßnahmen im Internet gegen das Gebot der Achtung der Gebietshoheit fremder Staaten und steht ihnen kein Rechtfertigungsgrund zur Seite, handeln sie zugleich auch gegen geltendes nationales Recht, da das in Rede stehende Gebot als allgemeine Regel des Völkerrechts gemäß Art. 25 Satz 1 GG Bestandteil des Bundesrechts ist.

Ob die erhobenen Beweise in diesen Konstellationen gleichwohl verwertbar sind, ist strittig.[203] Während insbesondere die Rechtsprechung ein Verwertungsverbot bei Verstoß gegen völkerrechtliche Pflichten oder bei der Verletzung von Rechtshilfevorschriften regelmäßig verneint,[204] sehen Stimmen in der Literatur auch bei Verletzung allgemeiner Grundsätze des Völkerrechts oder Verstoß gegen Normen von Rechtshilfeübereinkommen ein Verwertungsverbot grundsätzlich als gegeben oder doch zumindest naheliegend an.[205]

---

[200] *Schomburg* et al., Internationale Rechtshilfe in Strafsachen.

[201] *Meuters*, Leitung und Kontrolle grenzüberschreitender Ermittlungen; *Nagel*, Beweisaufnahme im Ausland; *Schädel*, Die Bewilligung internationaler Rechtshilfe; *Scheller*, Ermächtigungsgrundlagen für die internationale Rechts- und Amtshilfe.

[202] Siehe die Übersicht bei *Schmidt*, NStZ-RR 2005, 161 ff.

[203] So auch Council of Europe, Recommendation No. (89) 9, Erläuternder Bericht, S. 88.

[204] BGH NStZ 1984, 563; NStZ 1985, 464; NJW 1990, 1801; anders bei ausdrücklich verweigerter Rechtshilfe BGH NJW 1987, 2168, 2171.

[205] DAV Stellungnahme Nr. 41/2007, S. 30, allerdings sehr verallgemeinert; *Eschelbach*, in: Eberle/Rudolf/Wasserburg, Mainzer Rechtshandbuch der Neuen Medien, Kapitel XI, Rn. 161; *Gleß*, NStZ 2000, 57, 58; *Harings*, Grenzüberschreitende Zusammenarbeit der Polizei- und Zollverwaltungen, S. 280 ff. (differenzierend nach der Verletzung völkerrechtlicher Normen, welche die Rechtsposition des Betroffenen nach innerstaatlichem

Mit der Verwertung von Beweisen im deutschen Strafverfahren nimmt das Gericht selbst einen Hoheitsakt vor, der sich nach deutschem Recht richtet.[206] Eine – über Art. 25 Satz 1 GG auch für nationale Gerichte unmittelbar geltende – allgemeine Regel des Völkerrechts, nach der unter Verstoß gegen völkerrechtliche Gebote gewonnene Beweismittel generell nicht im nationalen Strafverfahren verwertet werden dürfen, gibt es wohl nicht.[207] Soweit Art. 29, 34, 35[208] der Resolution A/RES/56/83 der UN-Generalversammlung zur Staatenverantwortlichkeit[209] eine völkerrechtliche Pflicht des verletzenden (deutschen) Staates normieren, die von ihm zu verantwortende völkerrechtswidrige Situation zu beseitigen, besteht diese Pflicht nur gegenüber dem dies geltend machenden verletzten Völkerrechtssubjekt und nicht gegenüber Individuen, wie aus Art. 42[210] der genannten Resolution folgt.

Recht beeinträchtigen, S. 282); *Heine*, HRRS 2009, 540, 546; *Marberth-Kubicki*, Computer- und Internetstrafrecht, S. 294, Rn. 625; *Meininghaus*, Zugriff auf E-Mails, S. 182; *Schuster*, Verwertbarkeit im Ausland gewonnener Beweise, S. 135 ff. (zum Verstoß gegen Normen von Rechtshilfeübereinkommen); siehe auch *Seitz*, Strafverfolgungsmaßnahmen im Internet, S. 404, der allerdings das Problem des Verwertungsverbots nur anspricht, aber nicht entscheidet; *Spatscheck*, Steuern im Internet, Rn. 312 ff.; *Spatscheck/Alvermann*, wistra 1999, 333, 334; *Tiedemann*, FS Bockelmann, S. 819, 830; ebenfalls ein Beweisverwertungsverbot bei einer rechtswidrigen Telefonüberwachung von Konsularbeamten allerdings ohne nähere Begründung annehmend BVerfG NJW 1990, 1799.

206 *Böse*, ZStW 114 (2002), 148, 149; *Scheller*, Ermächtigungsgrundlagen für die internationale Rechts- und Amtshilfe, S. 95; *Schuster*, Verwertbarkeit im Ausland gewonnener Beweise, S. 96.

207 BVerfG NJW 1986, 1427, 1428 für den Fall der völkerrechtswidrigen Entführung einer Person; *Stuckenberg*, in: Menzel et al., Völkerrechtssprechung, S. 307, ebenfalls anhand des Falls einer völkerrechtswidrigen Entführung.

208 Art. 29 (Fortbestehen der Erfüllungspflicht) lautet: „Die Rechtsfolgen einer völkerrechtswidrigen Handlung nach diesem Teil berühren nicht die fortbestehende Verpflichtung des verantwortlichen Staates zur Erfüllung der verletzten Verpflichtung."

Art. 34 (Formen der Wiedergutmachung) lautet: „Die volle Wiedergutmachung des durch eine völkerrechtswidrige Handlung verursachten Schadens erfolgt durch Restitution, Schadenersatz und Genugtuung, entweder einzeln oder in Verbindung miteinander, in Übereinstimmung mit diesem Kapitel."

Art. 35 (Restitution) lautet: „Ein für eine völkerrechtswidrige Handlung verantwortlicher Staat ist verpflichtet, Restitution zu leisten, das heißt den vor der Begehung der Handlung herrschenden Zustand wiederherzustellen, sofern und soweit die Restitution a) nicht tatsächlich unmöglich ist; b) nicht mit einer Belastung verbunden ist, die außer allem Verhältnis zu dem Nutzen steht, der durch Restitution anstelle von Schadenersatz entsteht."

209 Die Resolution ist in deutscher Sprache abrufbar unter http://www.static.unigraz.at/fileadmin/rewi-institute/Voelkerrecht/Schulung/Fotos_von_der_Schulung/A_56_83_deutsch_ilc_staaten.pdf [Stand: 6.11.2013].

210 Art. 42 (Geltendmachung der Verantwortlichkeit durch einen verletzten Staat) lautet: „Ein Staat ist berechtigt, als verletzter Staat die Verantwortlichkeit eines anderen Staates geltend zu machen, wenn die Verpflichtung, die verletzt wurde, a) allein diesem Staat gegenüber besteht oder b) gegenüber einer Gruppe von Staaten, die diesen Staat einschließt, oder gegenüber der gesamten internationalen Gemeinschaft, und die Verletzung der Verpflichtung i) speziell diesen Staat betrifft oder ii) so beschaffen ist, dass sie die Lage aller

Fraglich ist daher, ob und wann ein Verwertungsverbot nach nationalem Recht vorliegt. Die Strafprozessordnung normiert u.a. mit § 136a Abs. 3 Satz 2, § 69 Abs. 3, § 100c Abs. 5 Satz 3 StPO nur einige wenige Beweisverbote selbst. Unstreitig bestehen daneben aber auch ungeschriebene Verbote, welche die im Untersuchungsgrundsatz nach § 244 Abs. 2 StPO niedergelegte gerichtliche Pflicht zur umfassenden Sachverhaltsaufklärung unter Heranziehung aller erreichbaren und erforderlichen Beweismittel beschränken. Das Strafprozessrecht schreibt keine Wahrheitserforschung um jeden Preis vor.[211] Die Ermittlung der Wahrheit muss vielmehr mit der grundgesetzlichen Werteordnung im Einklang stehen. Dies kann in Einzelfällen jedoch nur mittels einer Durchbrechung des Untersuchungsgrundsatzes im Wege von Beweisverboten – hier durch ein Beweisverwertungsverbot – gewährleistet werden. Die Annahme eines Beweisverwertungsverbots steht der Pflicht des Staates zur effektiven Strafverfolgung nicht entgegen.[212]

Abseits der gesetzlich geregelten Verwertungsverbote sind die Voraussetzungen für ein Verbot der Beweisverwertung in Rechtsprechung und Lehre umstritten.[213] Einigkeit besteht nur dahingehend, dass nicht jeder Verfahrensverstoß ein Beweisverwertungsverbot hervorruft.[214] Nach wohl h.M. ist in Erweiterung der sogenannten Rechtskreistheorie des BGH[215] bei der Prüfung des Vorliegens eines Verwertungsverbots eine Abwägung zwischen dem staatlichen Interesse an der Strafverfolgung im Einzelfall und dem Individualinteresse des Bürgers bezüglich der Wahrung seiner Rechte vorzunehmen.[216] Dabei soll der Strafverfolgung grundsätzlich Vorrang einzuräumen sein.[217]

Danach scheint ein Verbot der Verwertung von völkerrechtswidrig gewonnenen Beweisen nicht in Betracht zu kommen, weil die Pflichtverletzung nicht primär den Rechtskreis des Angeklagten berührt, sondern den der zwischenstaatlichen Beziehungen.[218] Das Gebot der Achtung der fremden Gebietshoheit schützt die Souverä-

---

anderen Staaten, gegenüber denen die Verpflichtung besteht, hinsichtlich der weiteren Erfüllung der Verpflichtung grundlegend ändert."

[211] BGH NJW 1960, 1580, 1582; NJW 1983, 1570, 1571; NZV 1992, 242, 243; NJW 1999, 959, 961; *Landau*, NStZ 2007, 121, 129.

[212] BGH NJW 2007, 2269, 2273, Rn. 32; *Brüning*, HRRS 2007, 250, 254; *Landau,* NStZ 2007, 121, 128 f.

[213] Zum Streitstand vgl. statt vieler zusammenfassend *Schuster*, Verwertbarkeit im Ausland gewonnener Beweise, S. 51 ff.

[214] BGHSt 11, 213, 214; 38, 214, 219; KK-StPO-*Fischer*, Einl., Rn. 137.

[215] BGHSt 11, 213, 214 ff.; ausführlich hierzu *Wolter*, Festgabe 50 Jahre BGH, S. 963, 983 ff.

[216] BVerfGE 43, 238, 250; BGHSt 19, 325, 332 f.; 24, 125, 130; BGH NJW 2001, 528, 529; *Hellmann*, Strafprozessrecht, Rn. 784; *Rogall*, NStZ 1988, 385, 391 ff.; *Schuster*, Verwertbarkeit im Ausland gewonnener Beweise, S. 65 ff.; *Wolter*, Festgabe 50 Jahre BGH, S. 963, 993 ff.

[217] BGHSt 44, 243, 249; 51, 285, 290.

[218] BGH NStZ 1984, 563; NStZ 1985, 464; NJW 1990, 1801. Siehe hierzu auch American Society of International Law, AJIL 29 (1935), speziell Art. 16, 623, nach welchem der

nitätsinteressen der Staaten und nicht die Interessen von Individuen. Allerdings ist der Rechtskreis des Angeklagten bereits immer schon dann berührt, wenn die Justizförmigkeit des Verfahrens betroffen ist,[219] da nach dem Rechtsstaatsprinzip des Art. 20 Abs. 3 GG die vollziehende Gewalt und die Rechtsprechung an Gesetz und Recht gebunden sind, also gemäß Art. 25 Satz 1 GG auch an die allgemeinen Regelungen des Völkerrechts. Die individuelle Betroffenheit des Angeklagten in seinen Rechten kann sich zudem durch Verstoß der Strafverfolgungsbehörden gegen Regelungen in Rechtshilfeübereinkommen ergeben. Das ist zumindest dann der Fall, wenn die verletzten Regeln über das völkerrechtliche Verhältnis der Staaten zueinander hinaus auch die Rechtfertigung des Eingriffs in die Rechte des betroffenen Bürgers enthalten.[220] Nach dem sogenannten dreidimensionalen Ansatz stehen dem Betroffenen im Rechtshilfeverfahren eigene subjektive Rechte zu, welche in materielle Abwehrrechte und den Anspruch auf Beachtung der Rechtshilferegeln bei der Beweisverwertung im Strafverfahren münden.[221]

Bei Abwägung der widerstreitenden Interessen muss das Gericht zudem nicht nur die Schwere des Tatvorwurfs, sondern auch die des Verfahrensverstoßes berücksichtigen. Letzterer wiegt jedoch schwer,[222] da die allgemeinen Regeln des Völkerrechts nach Art. 25 Satz 1 und 2 GG unmittelbar im nationalen Recht gelten und dort eine Stellung sogar oberhalb von einfachen Bundesgesetzen, direkt unterhalb der Verfassung einnehmen.[223] Hinzu tritt, dass es für die völkerrechtliche Verantwortlichkeit ohne Belang ist, ob der verletzende Staat im Einklang mit seinem innerstaatlichen Recht handelt.[224]

Die Schwere des Verfahrensverstoßes resultiert, neben der sich aus der Verfassung ergebenden Ranghöhe der Regeln, ferner aus der einem völkerrechtlichen Delikt nachfolgenden Haftung.[225] Hat der eingreifende Staat nach den Haftungsregeln nämlich die Folgen seines rechtswidrigen Handelns zu beseitigen, so würde er bei Verwertung der unter Eingriff in die Gebietshoheit gewonnenen Beweismittel nicht nur eine Beseitigung verweigern, sondern vielmehr die rechtswidrige Lage

---

Staat, der eine Person unter Verletzung internationalen Rechts festgenommen hat, diese nur dann bestrafen darf, wenn der Staat, dessen Rechte verletzt wurden, zustimmt sowie Art. 43 UN-Resolution A/RES/56/83 zur Staatenverantwortlichkeit; *Schuster*, Verwertbarkeit im Ausland gewonnener Beweise, S. 135 f. zum Rechtshilfeverhältnis.

[219] *Roxin/Schünemann*, Strafverfahrensrecht, § 24, Rn. 24; *Schmidt*, JZ 1958, 596, 597.

[220] *Harings*, Grenzüberschreitende Zusammenarbeit der Polizei- und Zollverwaltungen, S. 280 f.; *Spatscheck*, Steuern im Internet, Rn. 311 f.; *Spatscheck/Alvermann*, wistra 1999, 333, 334.

[221] *Gless/Eymann*, StV 2008, 318, 321 f.; *Heine*, HRRS 2009, 540, 545.

[222] *Spatscheck*, Steuern im Internet, Rn. 313; *Spatscheck/Alvermann*, wistra 1999, 333, 334; *Tiedemann*, FS Bockelmann, S. 819, 829.

[223] BGHSt 27, 30, 31 f.; *Rojahn*, in: v. Münch/Kunig, GG, Art. 25, Rn. 55.

[224] Art. 3 UN-Resolution A/RES/56/83 zur Staatenverantwortlichkeit.

[225] Zu den Haftungsvoraussetzungen siehe *v. Münch*, Das völkerrechtliche Delikt, S. 149 ff.

perpetuieren.[226] Allerdings verfestigt sich die rechtswidrige Souveränitätsverletzung nur dann, wenn der beeinträchtigte Staat Ansprüche aus dem Eingriff in seine Rechte geltend macht; dann kann der bloße „völkerrechtliche Reflex" zu einem subjektiven Abwehrrecht des Einzelnen erstarken.[227] Verhält er sich überhaupt nicht zu dem Eingriff in seine Interessen, ergibt sich hieraus indes nur im Ausnahmefall seine nachträgliche Zustimmung und damit die Heilung der Souveränitätsverletzung. Anders als in Fällen, in denen der ersuchte Staat die Rechtshilfe bewilligt, aber einen sogenannten Spezialitätsvorbehalt[228] nicht geltend macht und damit auf eine eingeschränkte Verwertung der Beweise verzichtet,[229] fehlt es in den vorliegenden Fällen bei dem in seiner Souveränität verletzten Staat nicht nur an der Bewilligung, sondern regelmäßig bereits an der Kenntnis des Verletzungstatbestands,[230] sodass in dem Verzicht auf dessen Geltendmachung nicht zugleich die Ausübung der eigenen Souveränität gesehen werden kann. Nach dem im Völkerrecht geltenden allgemeinen Prinzip „in dubio mitius" ist im Zweifel eine souveränitätsschonende Auslegung vorzunehmen,[231] so dass an die Annahme einer konkludenten Zustimmung im Fall der eigenmächtigen Verletzung der Souveränität fremder Staaten durch extraterritorial wirkende Ermittlungen hohe Anforderungen zu stellen sind. Für gewöhnlich scheidet daher eine Heilung der Souveränitätsverletzung aus, und es tritt gleichzeitig mit der Verwertung völkerrechtswidrig erlangter Beweise eine Perpetuierung der Verletzung der Souveränität des betroffenen Staates ein. Daneben ist in die Abwägung einzustellen, ob im Einzelfall das Beweismittel überhaupt legal, also im Wege eines internationalen Rechtshilfeverfahrens, hätte erlangt werden können, was sich jedoch insbesondere in Fällen fehlender konkreter Normen in Rechtshilfeübereinkommen nur für den konkreten Einzelfall beantworten lässt. Hypothetische Überlegungen scheiden überdies aus, wenn sich die Strafverfolgungsbehörden bewusst gegen das Recht gestellt haben, denn dann ist nach zutreffender Auffassung zur Aufrechterhaltung des Rechtsstaates zwingend ein Beweisverwertungsverbot anzunehmen.[232]

Aus den oben stehenden Gründen folgt somit, dass die unter Verstoß gegen das Gebot der Achtung der fremden Gebietshoheit gewonnenen Beweismittel regelmäßig einem Beweisverwertungsverbot unterliegen, da bei der Abwägung der widerstreitenden Staats- und Individualinteressen letztere zumeist überwiegen.

---

226 *Tiedemann*, FS Bockelmann, S. 819, 826 f.

227 BGHSt 34, 344; BGH NStZ 1984, 563; 1985, 464; zu den Auswirkungen ausdrücklich verwehrter Rechtshilfe siehe BGH NJW 1987, 2168, 2171; *Heine*, HRRS 2009, 540, 545.

228 *Gleß/Eymann*, StV 2008, 318, 319.

229 *Böse*, ZStW 114 (2002), 148, 174, zum Sonderfall der Nacheile nach Art. 40 SDÜ, S. 176 ff.; *Nagel*, Beweisaufnahme im Ausland, S. 316; *Schuster*, Verwertbarkeit im Ausland gewonnener Beweise, S. 118, 138.

230 *Gercke*, StraFo 2009, 271, 274.

231 *Ipsen*, Völkerrecht, § 11, Rn. 20.

232 *Roxin*, NStZ 2007, 616, 617.

V. Resümee

Bei ihrer Ermittlungsarbeit im Internet stoßen die Strafverfolgungsbehörden häufig an die Grenzen ihrer territorialen Kompetenz aufgrund grenzüberschreitender Sachverhalte. Völkerrechtlich kraft Anerkennung durch die Staatenpraxis zulässig ist die innerstaatliche Kommunikation über das Internet, auch soweit sie bedingt durch den technischen Aufbau des „Netzes der Netze" einen potentiellen Auslandsbezug aufweist. Gleiches gilt im Ergebnis für den Abruf frei zugänglich im Ausland gespeicherter Daten. Diese dürfen die Strafverfolger nach Art. 32 Buchstabe a) CCC eigenständig von ihrem Hoheitsgebiet aus abrufen. Darüber hinaus ist ein solcher Abruf aber auch schon aufgrund Gewohnheitsrechts zulässig. Einen mangels Rechtfertigungsgrunds völkerrechtswidrigen Eingriff in die Gebietshoheit fremder Staaten nehmen die Strafverfolgungsbehörden dagegen bei der Individualkommunikation mit im Ausland befindlichen Nutzern vor. Mit der Überwachung der Kommunikation unter Beteiligung ausländischer Nutzer, die gezielt am ausländischen Partner ansetzt, ist ebenfalls ein völkerrechtswidriger Eingriff verbunden. Gleiches gilt für den Abruf von im Ausland gespeicherten zugangsbeschränkten Daten, wenn für den Einzelfall weder der Berechtigte dem Abruf zustimmt noch eine Erlaubnis des betroffenen Staates vorliegt oder ausnahmsweise das Eingriffsinteresse des Staates, dessen Beamte Maßnahmen mit extraterritorialer Wirkung vornehmen, zumindest gegenüber dem Abwehrinteresse des betroffenen Staates gleichwertig ist. Der Upload von Daten auf Host-Servern im Inland, insbesondere zur Fahndung, ist dagegen ohne spezielle Ermächtigungsgrundlage nur dann völkerrechtswidrig, wenn die Fahndung gezielt auf die Suche nach einer sich im Ausland aufhaltenden Person ausgerichtet ist und folglich vornehmlich Internetnutzer im Ausland Ziel des Aufrufs sind. Erfolgt der Fahndungsaufruf selbst bereits auf einem im Ausland zu lokalisierenden Rechner, ist die Ermittlungsmaßnahme ebenso grundsätzlich völkerrechtswidrig.

Führt die Ermittlungsmaßnahme zu einem Eingriff in die Gebietshoheit fremder Staaten, können die Strafverfolgungsbehörden die Maßnahme abseits spezieller Befugnisnormen in völkerrechtlichen Verträgen, zwischenstaatlichen Abkommen oder allgemeiner Anerkennung in der Staatenpraxis nur im Wege der internationalen Rechtshilfe gerechtfertigt vornehmen bzw. durch die Ermittlungsbehörden der betroffenen Staaten vornehmen lassen.

Beschreiten die Strafverfolgungsbehörden bei in die Gebietshoheit fremder Staaten eingreifenden Maßnahmen nicht den Weg der internationalen Rechtshilfe und ist die Ermittlungsmaßnahme auch nicht in der Staatenpraxis allgemein anerkannt oder bestehen weder Befugnisnormen noch eine Einzelermächtigung, so unterliegen die unter Verstoß gegen das Gebot der Achtung der fremden Gebietshoheit gewonnenen Beweismittel zumeist einem Beweisverwertungsverbot.

Zusammenfassung

Die Strafrechtspflege stößt aufgrund der zunehmenden Globalisierung und Internationalisierung von Straftaten an ihre territorialen Grenzen. Den mit der grenzüberschreitenden Computerkriminalität verbundenen Herausforderungen kann sich der Nationalstaat daher nur unter Berücksichtigung der überstaatlichen Rechtsordnung des Völkerrechts erfolgreich stellen.

Der völkerrechtliche Grundsatz der Achtung der Gebietshoheit gilt auch für Internetsachverhalte. Er schränkt die Befugnis zur Ausübung grenzüberschreitender Hoheitsakte ein. Völkerrechtlich generell unzulässig sind Hoheitsakte, die ohne Einwilligung durch auf fremdem Staatsgebiet physisch befindliche staatliche oder staatlich gelenkte Organe vorgenommen werden. Mit ihnen greift der handelnde Staat in die Souveränität des betroffenen Drittstaates ein. Hiervon zu unterscheiden sind die Hoheitsakte, bei denen staatliche Organe auf dem eigenen Staatsgebiet hoheitlich handeln, ihr Handeln jedoch in fremdes Staatsgebiet hineinwirkt. Ein solcher extraterritorialer Hoheitsakt ist insbesondere dann völkerrechtswidrig, wenn er die Gebietshoheit des fremden Staates unmittelbar verletzt, der Hoheitsakt in seinen Wirkungen einem Hoheitsakt auf fremdem Staatsgebiet gleichkommt oder die Sicherheit und Ordnung des fremden Staates beeinträchtigt. Sowohl die Ausdehnung des nationalen Strafrechts auf Sachverhalte mit Auslandsbezug als auch die Maßnahmen der Strafverfolgungsbehörden im Internet zählen zu dieser letzten Gruppe. Die Beamten verbleiben nämlich physisch auf dem Territorium des eigenen Staatsgebiets und nur bestimmte Wirkungen ihrer Handlungen treten auf fremdem Gebiet ein.

Die Grenzen des Spielraums nationaler Gesetzgeber und Rechtsanwender bei der Vornahme extraterritorialer Hoheitsakte verdeutlicht das Dissertationsprojekt anhand von zwei Teilbereichen: der Anwendung des deutschen Rechts auf Internetsachverhalte mit Auslandsbezug und der Bestimmung der territorialen Reichweite der Befugnisse deutscher Strafverfolgungsbehörden bei der Ermittlungsarbeit im Internet.

Ausgangspunkte der Untersuchung, inwieweit eine Kompetenz zur Anwendung des Strafrechts auf Sachverhalte mit Auslandsbezug besteht, sind die Grundsätze des internationalen Strafrechts, die mangels Spezialregelungen auch für Straftaten im Internet gelten. Die Bestimmung des Tatorts bei grenzüberschreitenden Kriminalitätsformen wurde anhand des Territorialitätsprinzips als Haupt- und Ausgangsprinzip der meisten Rechtsordnungen der Welt verdeutlicht, da es für die Ausübung von Strafgewalt weltweit anerkannt ist. Wegen der unterschiedlichen Auslegung

der Reichweite dieses Prinzips in den verschiedenen Staaten ergibt sich eine Vielzahl von positiven Kompetenzkonflikten, denen nur durch restriktive Handhabung dieser Anwendungsregel begegnet werden kann. Eine hinreichende Konfliktlösung in grenzüberschreitenden Sachverhaltskonstellationen, bei denen keine festgeschriebenen Regelungsinstrumente greifen, ist nur durch eine Abwägung der relevanten Staateninteressen möglich. Für die Ermittlung des Handlungsorts kommt die Untersuchung zu dem Ergebnis, dass dieser nur dort sein kann, wo der Täter körperlich anwesend ist. Bei der Untersuchung des Erfolgstatorts zeigt sich, dass dieser unter Berücksichtigung der völkerrechtlichen Gesichtspunkte allein begründet ist, wo tatbestandsmäßige Verletzungen und konkrete Gefährdungen – nicht jedoch abstrakte oder abstrakt-konkrete Gefährdungen – eintreten.

Für Anbieter von Informations- und Kommunikationsdiensten aus dem EU-Ausland hat das Gemeinschaftsrecht mit dem sogenannten Herkunftslandprinzip der E-Commerce-Richtlinie den Mitgliedstaaten und ihren Strafverfolgungsbehörden auf dem Gebiet des Straf- und Strafverfahrensrechts überdies spezielle Grenzen gesetzt. Dieses bereits im primären und sekundären Gemeinschaftsrecht verankerte Prinzip gilt auch im Strafrecht. Aufgrund seines bereits durch die Richtlinie selbst beschränkten Geltungsbereichs und der zahlreichen Umgehungsmöglichkeiten mangels Harmonisierung des materiellen Rechts zeigt sich zwar die geringe Tauglichkeit des Herkunftslandprinzips für das Strafrecht. Soweit es anwendbar ist, kommt ihm in Konstellationen eines Normwiderspruchs aber Vorrang vor den Regelungen des deutschen internationalen Strafrechts zu.

Der dritte Teil der Arbeit nimmt das Strafprozessrecht in den Blick und bestimmt die territoriale Reichweite nationalstaatlicher Ermittlungsbefugnisse. Den Herausforderungen der Verfolgung grenzüberschreitender Datennetzkriminalität können die Ermittler nur dann erfolgreich begegnen, wenn ihnen hinreichende Instrumente zur schnellen Beweissicherung über Staatsgrenzen hinweg zur Verfügung stehen.

Die Untersuchung zeigt, dass sowohl die innerstaatliche Kommunikation über das Internet (trotz potentiellen Auslandsbezugs) als auch der Abruf frei zugänglicher, aber im Ausland gespeicherter Daten völkerrechtlich kraft Anerkennung durch die Staatenpraxis zulässig sind. Dagegen greifen die Strafverfolgungsbehörden mangels Rechtfertigung grundsätzlich völkerrechtswidrig in die Gebietshoheit fremder Staaten ein, wenn sie mit im Ausland befindlichen Nutzern eine Individualkommunikation führen. Ebenso ist mit der Überwachung der Kommunikation mit ausländischen Nutzern ein rechtswidriger Eingriff verbunden, soweit diese Kommunikationsbeziehung gezielt am ausländischen Partner bzw. dem zu ihm führenden Telekommunikationsweg (sog. Auslandskopfüberwachung) ansetzt. Auch der Abruf von im Ausland gespeicherten zugangsbeschränkten Daten erweist sich als rechtswidrig, wenn für den Einzelfall keine Erlaubnis des betroffenen Staates vorliegt oder das Eingriffsinteresse des extraterritorial handelnden Staates hinter dem des betroffenen Staates zurückbleibt. Anders liegt es nur dann, wenn der Zugangsberechtigte in den Abruf der Daten zuvor eingewilligt hat und die betroffenen Staa-

ten dem Übereinkommen über Computerkriminalität beigetreten sind. Der Upload von Daten auf Server im Inland, insbesondere zur Fahndung, ist dagegen ohne spezielle Ermächtigungsgrundlage zulässig und nur dann völkerrechtswidrig, wenn die Fahndung gezielt auf die Suche nach einer sich im Ausland aufhaltenden Person ausgerichtet ist und folglich vornehmlich Internetnutzer im Ausland anspricht. Erfolgt der Upload ohne konkrete Einwilligung des Staates gar auf einem Server im Ausland, ist hiermit gleichfalls eine Verletzung der Gebietshoheit des betroffenen Staates verbunden.

Führt die Ermittlungsmaßnahme zu einem Eingriff in die Gebietshoheit fremder Staaten, können die Strafverfolgungsbehörden die Maßnahme abseits allgemeiner Anerkennung in der Staatenpraxis, spezieller Befugnisnormen oder Einzelermächtigungen nur im Wege der internationalen Rechtshilfe vornehmen bzw. durch die Ermittlungsbehörden der betroffenen Staaten vornehmen lassen. Beschreiten die Strafverfolger nicht den Weg der internationalen Rechtshilfe und ist die Ermittlungsmaßnahme auch nicht in der Staatenpraxis allgemein als völkerrechtsgemäß anerkannt bzw. durch spezielle Befugnisnormen oder Einzelermächtigungen gedeckt, so unterliegen die unter Verstoß gegen das Gebot der Achtung der fremden Gebietshoheit gewonnenen Beweismittel regelmäßig einem Beweisverwertungsverbot.

Literaturverzeichnis

Altenhain, Karsten, Die strafrechtliche Verantwortung für die Verbreitung missbilligter Inhalte in Computernetzen. CR 1997, 485–496.

– Europäisches Herkunftslandprinzip und nationales Strafanwendungsrecht. In: Frank Zieschang/Eric Hilgendorf/Klaus Laubenthal (Hrsg.), Strafrecht und Kriminalität in Europa. Baden-Baden 2003, S. 107–126.

Ambos, Kai, Anmerkung zu BGH, Urteil vom 30.04.1999 – 3 StR 215/98 (OLG Düsseldorf). NStZ 1999, 404.

– Völkerrechtliche Kernverbrechen, Weltrechtsprinzip und § 153f StPO – Zugleich Anmerkung zu GBA, JZ 2005, 311 und OLG Stuttgart. NStZ 2006, 117; 434–438.

American Law Institute, Restatement of the Law Second, Foreign Relations Law of the United States. St. Paul, Minnesota, 1965.

– Restatement of the Law Third, The Foreign Relations Law of the United States, vol. 1, §§ 1–488. St. Paul, Minnesota, 1987.

– Case Citations to the Restatement of the Law, Cumulative Annual Supplement for Use in 1993–1994. St. Paul, Minnesota, 1993.

American Society of International Law (under the Auspices of the Faculty of the Harvard Law School), II. Jurisdiction with Respect to Crime, Supplement to the American Journal of International Law 29 (1935), 439–635.

Arzt, Gunther, Zum Verbotsirrtum beim Fahrlässigkeitsdelikt. ZStW 91 (1979), 857–887.

Association Internationale de Droit Pénal, XVth International Congress of Penal Law, Rio de Janeiro, 4–10 September 1994, Resolutions, Section II: Computer Crimes and other Crimes against Information Technology. International Review of Penal Law vol. 66 (1995), No. 1/2.

Auer, Marietta, Neues zu Umfang und Grenzen der richtlinienkonformen Auslegung. NJW 2007, 1106–1109.

Badura, Peter, Territorialprinzip und Grundrechtsschutz. In: Josef Isensee/Helmut Lecheler (Hrsg.), Freiheit und Eigentum. Festschrift für Walter Leisner zum 70. Geburtstag. Berlin 1999, S. 403–412.

Bär, Wolfgang, Der Zugriff auf Computerdaten im Strafverfahren. Köln u.a. 1992.

– Durchsuchungen im EDV-Bereich (II). CR 1995, 227–234.

– Öffentlichkeitsfahndung im Internet. CR 1997, 422–431.

– Strafprozessuale Fragen der EDV-Beweissicherung. MMR 1998, 577–584.

– Handbuch zur EDV-Beweissicherung im Strafverfahren. Stuttgart u.a. 2007.

Bär, Wolfgang, Strafrecht in der digitalen Welt. Herbsttagung „Tatort Internet – eine globale Herausforderung für die Innere Sicherheit" des Bundeskriminalamtes in Wiesbaden vom 20.–22.11.2007, Langfassung, abrufbar unter http://www.bka.de/nn_193608/SharedDocs/Downloads/DE/Publikationen/Herbsttagungen/2007/herbsttagung2007baerLangfassung,templateId=raw,property=publicationFile.pdf/herbsttagung2007baerLangfassung.pdf [Stand: 6.11.2013].

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

Beck, Susanne, Internetbeleidigung de lege lata und de lege ferenda. Strafrechtliche Aspekte des „spickmich"-Urteils. MMR 2009, 736–740.

Beckemper, Katharina, Strafbare Beihilfe durch alltägliche Geschäftsvorgänge. Jura 2001, 163–169.

Beisel, Daniel/Heinrich, Bernd, Die Strafbarkeit der Ausstrahlung pornographischer Sendungen in codierter Form durch das Fernsehen. JR 1996, 95–96.

Bertele, Joachim, Souveränität und Verfahrensrecht. Eine Untersuchung der aus dem Völkerrecht ableitbaren Grenzen staatlicher extraterritorialer Jurisdiktion im Verfahrensrecht. Tübingen 1998.

Berz, Ulrich, Formelle Tatbestandsverwirklichung und materialer Rechtsgüterschutz. Eine Untersuchung zu den Gefährdungs- und Unternehmensdelikten. München 1986.

Biehler, Anke/Kniebühler, Roland/Lelieur-Fischer, Juliette/Stein Sibyl, Freiburg Proposal on Concurrent Jurisdictions and the Prohibition of Multiple Prosecutions in the European Union. Freiburg 2003.

Bleisteiner, Stephan, Rechtliche Verantwortlichkeit im Internet – unter besonderer Berücksichtigung des Teledienstegesetzes und des Mediendienste-Staatsvertrages –. Köln u.a. 1999.

Blumenwitz, Dieter, Freedom of information in the light of international law. In: Rainer Gepperth (Hrsg.), Freedom of Information – a Human Right. Symposium of the Hanns Seidel Foundation with the United Nations in Geneva May 1978. München 1978, S. 13–39.

Bock, Dennis, Verfahrenseinstellung bei Auslandsberührung. Die Nichtverfolgung von aus dem Ausland heraus begangenen Taten (Distanztaten) gemäß § 153c III StPO. GA 2010, 589–597.

Böckenförde, Thomas, Die Ermittlung im Netz. Möglichkeiten und Grenzen neuer Erscheinungsformen strafprozessualer Ermittlungstätigkeit. Tübingen 2003.

Bodewig, Theo, Elektronischer Geschäftsverkehr und Unlauterer Wettbewerb. GRURInt 2000, 475–483.

Boese, Oliver, Strafrechtliche Verantwortlichkeit für Verweisungen durch Links im Internet. Frankfurt a.M. 2000.

Bösch, Rainer, Die Inländerdiskriminierung. Jura 2009, 91–96.

Böse, Martin, Die Verwertung im Ausland gewonnener Beweismittel im deutschen Strafverfahren. ZStW 114 (2002), 148–182.

Braum, Stefan, Europäische Strafgesetzgebung: Demokratische Strafgesetzlichkeit oder administrative Opportunität? – Besprechung des Urteils des EuGH vom 13.09.2005, Rs C-176/03. wistra 2006, 121–126.

Brechmann, Winfried, Die richtlinienkonforme Auslegung. Zugleich ein Beitrag zur Dogmatik der EG-Richtlinie. München 1994.

Bremer, Karsten, Strafbare Internet-Inhalte in internationaler Hinsicht. Ist der Nationalstaat wirklich überholt? Frankfurt a.M. u.a. 2001.

– Radikal-politische Inhalte im Internet – ist ein Umdenken erforderlich? MMR 2002, 147–152.

Brenner, Susan W., The Next Step: Prioritizing Jurisdiction. In: Bert-Jaap Koops/Susan W. Brenner (Hrsg.), Cybercrime and Jurisdiction. A Global Survey. Den Haag 2006, S. 327–349.

Breuer, Barbara, Anwendbarkeit des deutschen Strafrechts auf exterritorial handelnde Internet-Benutzer. MMR 1998, 141–145.

Brisch, Klaus M., EU-Richtlinienvorschlag zum elektronischen Geschäftsverkehr. CR 1999, 235–244.

Brodowski, Dominik, Strafprozessualer Zugriff auf E-Mail-Kommunikation. JR 2009, 402–412.

Bröhl, Georg M., EGG – Gesetz über rechtliche Rahmenbedingungen des elektronischen Geschäftsverkehrs. Erläuterungen zum Referentenentwurf. MMR 2001, 67–71.

Bruns, Viktor, Völkerrecht als Rechtsordnung. ZaöRV Bd. 1, Teil 1 Abhandlungen (1929), 1–56.

Brunst, Phillip W., Anonymität im Internet. Rechtliche und tatsächliche Rahmenbedingungen. Zum Spannungsfeld zwischen einem Recht auf Anonymität und den Möglichkeiten zur Identifizierung und Strafverfolgung. Berlin 2009.

Brüning, Janique, Die Rechtsfolgen eines Verstoßes gegen den Richtervorbehalt. Zugleich eine Anmerkung zum Urteil des BGH vom 18. April 2007 (5 StR 546/06 = BGH HRRS 2007 Nr. 463). HRRS 2007, 250–255.

Bullinger, Martin/Mestmäcker, Ernst-Joachim, Multimediadienste. Struktur und staatliche Aufgaben nach deutschem und europäischem Recht. Baden-Baden 1997.

Bundesamt für Verfassungsschutz (Hrsg.), Rechtsextremistische Bestrebungen im Internet. Köln 2000 (zit.: BfV, Rechtsextremistische Bestrebungen im Internet).

Bundeskriminalamt (Hrsg.), Electronic Commerce. Markt der Zukunft – auch für Kriminelle? Wiesbaden 1999.

Bundesministerium des Innern/Bundesministerium der Justiz (Hrsg.), Erster Periodischer Sicherheitsbericht. Berlin 2001.

– Zweiter Periodischer Sicherheitsbericht. Berlin 2006.

Bundesministerium der Justiz (Hrsg.), Niederschriften über die Sitzungen der Großen Strafrechtskommission, 4. Bd., Allgemeiner Teil, 38. bis 52. Sitzung. Bonn 1958.

– Niederschriften über die Sitzungen der Großen Strafrechtskommission, 8. Bd., Besonderer Teil, 76. bis 90. Sitzung. Bonn 1959.

Busse-Muskala, Veit, Strafrechtliche Verantwortlichkeit der Informationsvermittler im Netz. Eine Untersuchung zur Strafbarkeit der Anbieter von Hyperlinks und Suchmaschinen. Münster 2006.

Cheswick, William R./Bellovin, Steven M./Rubin, Avi, Firewalls und Sicherheit im Internet. Schutz vor cleveren Hackern. Deutsche Übersetzung von Thomas Maus. 2. Aufl. München 2004.

Clauß, Felix, Anmerkung zu BGH, Urteil vom 12.12.2000 – 1 StR 184/00. MMR 2001, 232–233.

Collardin, Marcus, Straftaten im Internet. CR 1995, 618–622.

Conradi, Ulrich/Schlömer, Uwe, Die Strafbarkeit der Internet-Provider (I). NStZ 1996, 366–369.

Cornils, Karin, Der Begehungsort von Äußerungsdelikten im Internet. JZ 1999, 394–398.

– Die territorialen Grenzen der Strafbarkeit und Internet. In: Gerhard Hohloch (Hrsg.), Recht und Internet. Baden-Baden 2001, S. 71–84.

Council of Europe, Recommendation No. (85) 10, of the Committee of Ministers to member states concerning the practical application of the European Convention on Mutual Assistance in Criminal Matters in respect of letters rogatory for the interception of telecommunications, abrufbar unter http://www.coe.int/t/dghl/cooperation/economiccrime/organisedcrime/Rec_1985_10.pdf [Stand: 6.11.2013].

Council of Europe/European Committee on Crime Problems, Computer-related crime, Recommendation No. R (89) 9 on computer-related crime and final report of the European Committee on Crime Problems. Straßburg 1990.

– Extraterritorial criminal jurisdiction. Straßburg 1990.

Council of Europe/European Committee of Experts on Procedural Law Problems connected with Computer-related Crime, Problems of criminal procedural law connected with information technology, Recommendation No. R (95) 13 and explanatory memorandum. Straßburg 1996.

Dahm, Georg/Delbrück, Jost/Wolfrum, Rüdiger, Völkerrecht, Bd. I/1: Die Grundlagen. Die Völkerrechtssubjekte. 2. Aufl. Berlin u.a. 1989.

– Völkerrecht, Bd. I/3 – Die Formen des völkerrechtlichen Handelns. Die inhaltliche Ordnung der internationalen Gemeinschaft. 2. Aufl. Berlin 2002.

Damker, Herbert/Müller, Günther, Verbraucherschutz im Internet. DuD 1997, 24–29.

Daum, Brigitte, Grenzverletzungen und Völkerrecht. Eine Untersuchung der Rechtsfolgen von Grenzverletzungen in der Staatenpraxis und Folgerungen für das Projekt der International Law Commission zur Kodifizierung des Rechts der Staatenverantwortlichkeit. Frankfurt a.M. 1999.

Delmas-Marty, Mireille/Vervaele, John A.E. (Hrsg.), The Implementation of the Corpus Juris in the Member States. Penal Provisions for the Protection of European Finances, vol. 1. Antwerpen u.a. 2000.

Derksen, Roland, Strafrechtliche Verantwortung für in internationalen Computernetzen verbreitete Daten mit strafbarem Inhalt. NJW 1997, 1878–1885.

Dethloff, Nina, Europäisches Kollisionsrecht des unlauteren Wettbewerbs. JZ 2000, 179–185.

Determann, Lothar, Kommunikationsfreiheit im Internet. Freiheitsrechte und gesetzliche Beschränkungen. Baden-Baden 1999.

Deutscher, Jörg, Die Kompetenzen der Europäischen Gemeinschaften zur originären Strafgesetzgebung. Frankfurt a.M. u.a. 2000.

Ditz, Xaver, Reichweite des digitalen Datenzugriffs der Finanzverwaltung im nationalen und internationalen Konzern. DStR 2004, 2038–2042.

Doehring, Karl, Die Teilung Deutschlands als Problem der Strafanwendung, Der Staat Bd. 4 (1965), S. 259–278.

– Völkerrecht. Ein Lehrbuch. 2. Aufl. Heidelberg 2004.

Duden, Das große Wörterbuch der deutschen Sprache in acht Bänden. Wissenschaftlicher Rat und die Mitarbeiter der Dudenredaktion unter der Leitung von Günther Drosdowski (Hrsg.), Bd. 3. 2. Aufl. Mannheim u.a. 1993.

– Das Fremdwörterbuch. Wissenschaftlicher Rat der Dudenredaktion (Hrsg.). 6. Aufl. Mannheim u.a. 1997.

Eberle, Carl-Eugen/Rudolf, Walter/Wasserburg, Klaus (Hrsg.), Mainzer Rechtshandbuch der Neuen Medien. Heidelberg 2003 (zit.: *Bearbeiter*, in: Eberle/Rudolf/Wasserburg, Mainzer Rechtshandbuch der Neuen Medien).

Ebermayer, Ludwig/Eichelbaum, Julius/Lobe, Adolf/Rosenberg, *Werner*, Leipziger Kommentar zum Strafgesetzbuch. Großkommentar. 1. Aufl. Berlin u.a. 1920 (zit.: LK-StGB[1]-*Bearbeiter*).

Eisele, Jörg, Internationale Bezüge des Strafrechts. JA 2000, 424–429.

– Einflussnahme auf nationales Strafrecht durch Richtliniengebung der Europäischen Gemeinschaft. JZ 2001, 1157–1165.

– Jurisdiktionskonflikte in der Europäischen Union: Vom nationalen Strafanwendungsrecht zum Europäischen Kollisionsrecht? ZStW 125 (2013), 1–33.

Engel, Christoph, Das Völkerrecht des Telekommunikationsvorgangs. RabelsZ 49 (1985), 90–120.

Epping, Volker, Die Novellierung im Bereich des Rüstungsexportrechts. RIW 1991, 461–470.

Ernst, Stefan, Rechtliche Fragen bei der Verwendung von Hyperlinks im Internet. NJW-CoR 1997, 224–228.

Eser, Albin, Das „Internationale Strafrecht" in der Rechtsprechung des Bundesgerichtshofes. In: Claus-Wilhelm Canaris/Andreas Heldrich/Karsten Schmidt/Claus Roxin/Gunter Widmaier (Hrsg.), 50 Jahre Bundesgerichtshof. Festgabe aus der Wissenschaft, Bd. IV: Strafrecht, Strafprozeßrecht. München 2000, S. 3–28.

Eurojust, Jahresbericht 2003, abrufbar unter: http://www.eurojust.europa.eu/doclibrary/corporate/eurojust%20Annual%20Reports/Annual%20Report%202003/Annual-Report-2003-DE.pdf) [Stand: 6.11.2013].

Faßbender, Kurt, Zu Inhalt und Grenzen des rundfunkrechtlichen Sendestaatsprinzips. AfP 2006, 505–512.

Federrath, Hannes/Golembiewski, Claudia, Speicherung von Nutzungsdaten durch Anonymisierungsdienste im Internet. Welche strafprozessualen Vorschriften zur Überwachung der Telekommunikation sind auf Anonymisierungsdienste anwendbar? DuD 2004, 486–490.

Fetzer, Thomas/Groß, Thomas, Die Pupino-Entscheidung des EuGH – Abkehr vom intergouvernementalen Charakter der EU? – Erwiderung auf Herrmann. EuZW 2005, 436; 550–551.

Fezer, Karl-Heinz/Koos, Stefan, Das gemeinschaftsrechtliche Herkunftslandprinzip und die e-commerce-Richtlinie. Zur dringenden Notwendigkeit einer Harmonisierung des Wettbewerbsrechts in den Mitgliedstaaten der Europäischen Union als einer gemeinschaftsrechtlichen Aufgabe. IPRax 2000, 349–354.

Finke, Thorsten, Die strafrechtliche Verantwortung von Internet-Providern. Tübingen 1998.

Fischer, Thomas, Strafgesetzbuch und Nebengesetze. 60. Aufl. München 2013.

Frenz, Walter, Handbuch Europarecht, Bd. 1: Europäische Grundfreiheiten. Berlin u.a. 2004.

Freund, Wolfgang, Die Strafbarkeit von Internetdelikten. Eine Analyse am Beispiel pornographischer Inhalte. Wien 1998.

Fritsch, Lothar/Rossnagel, Heiko/Schwenke, Matthias/Stadler, Tobias, Die Pflicht zum Angebot anonym nutzbarer Dienste. Eine technische und rechtliche Zumutbarkeitsbetrachtung. DuD 2005, 592–596.

Fröhlinger, Margot, Der Richtlinienvorschlag zum elektronischen Geschäftsverkehr. In: Josef Drexl/Karl F. Kreuzer/Dieter H. Scheuing/Ulrich Sieber (Hrsg.), Europarecht im Informationszeitalter. Baden-Baden 2000, S. 9–21.

Fromm, Heiz, Extremismus im Internet. In: Jürgen Welp (Hrsg.), kriminalität@net. Beiträge zur 13. Alsberg-Tagung 2001 in Berlin und zur Verleihung des Max-Alsberg-Preises an die Redaktion der Zeitschrift Strafverteidiger. Baden-Baden 2003, S. 41–47.

Frowein, Jochen A., Das Problem des grenzüberschreitenden Informationsflusses und des „domain réservé". In: Berichte der Deutschen Gesellschaft für Völkerrecht, Heft 19, Das Problem des grenzüberschreitenden Informationsflusses und des „domain réservé" (Free Flow of Information Across Boundaries and the „domain réservé"). 16. Tagung in Köln vom 5. bis 7. April 1979. Karlsruhe 1979, S. 1–38 (zit.: *Frowein*, in: BerDGesVölkR 19).

G8-Gruppe, Principles and Action Plan to Combat High-Tech Crime, 1997, abrufbar unter http://www.coe.int/t/dg1/legalcooperation/economiccrime/cybercrime/Documents/Points%20of%20Contact/24%208%20Communique_en.pdf [Stand: 6.11.2013].

– Principles on transborder access to stored computer data, 1999, abrufbar unter http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/documents/points%20of%20contact/24%208%20Principles%20on%20Transborder%20Access%20to%20Stored%20Computer%20Data_en.pdf [Stand: 6.11.2013].

– Recommendations on Transnational Crime, 2002, abrufbar unter http://www.inmlex.ro/arhiva/fisiere/pag_34/det_352/1010.doc [Stand: 6.11.2013].

– Recommendations for Tracing Networked Communications Across National Borders in Terrorist and Criminal Investigations, 2002, abrufbar unter http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/documents/points%20of%20contact/24%208%20Recommendations%20for%20Tracing%20Networked%20Communications%20Acros_en.pdf [Stand: 6.11.2013].

– Principles on the Availability of Data Essential to Protecting Public Safety, 2002, abrufbar unter http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/documents/points%20of%20contact/24%208%20Principles%20of%20Data%20Availability_en.pdf [Stand: 6.11.2013].

Gaede, Karsten, Der grundrechtliche Schutz gespeicherter E-Mails beim Provider und ihre weltweite strafprozessuale Überwachung. Zugleich Besprechung zu LG Hamburg, Beschl. vom 8.1.2008 – 619 Qs 1/08. StV 2009, 96–102.

Geiger, Rudolf, Grundgesetz und Völkerrecht mit Europarecht. 6. Aufl. München 2013.

Gercke, Björn, Zur Zulässigkeit sog. Transborder Searches – Der strafprozessuale Zugriff auf im Ausland gespeicherte Daten. StraFo 2009, 271–274.

Gercke, Marco, Rechtswidrige Inhalte im Internet. Eine Diskussion ausgewählter Rechtsfelder des Internet-Strafrechts unter Berücksichtigung strafprozessualer Aspekte. Köln 2000.

– Die Entwicklung der Rechtsprechung zum Internetstrafrecht in den Jahren 2000 und 2001. ZUM 2002, 283–288.

– „Cyberterrorismus" – Aktivitäten terroristischer Organisationen im Internet. Die Möglichkeiten und Grenzen legislativer Ansätze zur Bekämpfung von Aktivitäten terroristischer Gruppen im Internet. CR 2007, 62–68.

– Die Bekämpfung der Internetkriminalität als Herausforderung für die Strafverfolgungsbehörden. MMR 2008, 291–298.

– Impact of the Lisbon Treaty on Fighting Cybercrime in the EU. CRi 2010, 75–80.

Germann, Michael, Gefahrenabwehr und Strafverfolgung im Internet. Berlin 2000.

Germann, O.A., Rechtsstaatliche Schranken im internationalen Strafrecht. SchwZStR 1954, 237–252.

Gleß, Sabine, Zur Verwertung von Erkenntnissen aus verdeckten Ermittlungen im Ausland im inländischen Strafverfahren. NStZ 2000, 57–62.

Gleß, Sabine/Eymann, Stephanie, „Nachträgliches Verwertungsverbot" und internationale Beweisrechtshilfe. StV 2008, 318–325.

Götting, Bert, Das Tatortprinzip im Internet anhand des Beispiels der Volksverhetzung. Kriminalistik 2007, 615–620.

Grabitz, Eberhard/Hilf, Meinhard (Hrsg.), Das Recht der Europäischen Union, Bd. I, EUV/EGV, Stand 24. Ergänzungslieferung, September 2004. München (zit.: *Bearbeiter*, in: Grabitz/Hilf, Bd. I).

Grabitz, Eberhard/Hilf, Meinhard/Nettesheim, Martin (Hrsg.), Das Recht der Europäischen Union, Bd. I, EUV/EGV, Stand 50. Ergänzungslieferung, Mai 2013. München (zit.: *Bearbeiter*, in: Grabitz/Hilf/Nettesheim, Bd. I).

Graf, Jürgen P., Internet: Straftaten und Strafverfolgung. DRiZ 1999, 281–286.

– Strafrechtsschutz im Internet. In: Peter W. Heermann/Ansgar Ohly (Hrsg.), Verantwortlichkeit im Netz. Wer haftet wofür? Stuttgart u.a. 2003, S. 85–101.

Graf Vitzthum, Wolfgang/Bothe, Michael (Hrsg.), Völkerrecht. 5. Aufl. Berlin u.a. 2010 (zit.: *Bearbeiter*, in: Vitzthum/Bothe, Völkerrecht).

Graham, James Alexander, Der virtuelle Raum – sein völkerrechtlicher Status, JurPC Web-Dok. /1999, Abs. 1–47, abrufbar unter http://www.jurpc.de/aufsatz/19990035.htm [Stand: 6.11.2013].

Graul, Eva, Abstrakte Gefährdungsdelikte und Präsumtionen im Strafrecht. Berlin 1991.

Greiner, Arved, Die Verhinderung verbotener Internetinhalte im Wege polizeilicher Gefahrenabwehr. Hamburg 2001.

Gröseling, Nadine/Höfinger, Frank, Computersabotage und Vorfeldkriminalisierung. Auswirkungen des 41. StrÄndG zur Bekämpfung der Computerkriminalität. MMR 2007, 626–630.

Gruhl, Jens, „Grenzenlose" Ermittlungen im Internet? In: Jürgen Welp (Hrsg.), kriminalität@net. Beiträge zur 13. Alsberg-Tagung 2001 in Berlin und zur Verleihung des Max-Alsberg-Preises an die Redaktion der Zeitschrift Strafverteidiger. Baden-Baden 2003, S. 49–83.

Gusy, Christoph/Hueck, Ingo J., Fernmeldegeheimnis für Auslandsgespräche? Grundrechtsschutz und Grundrechtsreichweite. NJ 1995, 461–465.

Haft, Fritjof/Eisele, Jörg, Zur Einführung: Rechtsfragen des Datenverkehrs im Internet. JuS 2001, 112–120.

Hannich, Rolf (Hrsg.), Karlsruher Kommentar zur Strafprozessordnung mit GVG, EGGVG und EMRK. 7. Aufl. München 2013 (zit.: KK-StPO-*Bearbeiter*).

Haratsch, Andreas/Koenig, Christian/Pechstein, Matthias, Europarecht. 8. Aufl. Tübingen 2012.

Harings, Lothar, Grenzüberschreitende Zusammenarbeit der Polizei- und Zollverwaltungen und Rechtsschutz in Deutschland. Berlin 1998.

Heghmanns, Michael, Anmerkung zu LG München I, Urteil vom 17.11.1999 – 20 Ns 465 Js 173158/95. ZUM 2000, 463–466.

– Strafrechtliche Verantwortlichkeit für illegale Inhalte im Internet. JA 2001, 71–78.

– Internationales Strafrecht. JA 2001, 276–280.

– Straftaten im Rahmen elektronischer Kommunikation, insbesondere im Internet, Kapitel VI, Abschnitt 2. In: Hans Achenbach/Andreas Ransiek (Hrsg.), Handbuch Wirtschaftsstrafrecht. 2. Aufl. Heidelberg 2008, S. 461–485 (zit.: *Heghmanns*, in: Achenbach/Ransiek, HWSt^{2}).

– Straftaten im Rahmen elektronischer Kommunikation, insbesondere im Internet, 6. Teil, 2. Kapitel. In: Hans Achenbach/Andreas Ransiek (Hrsg.), Handbuch Wirtschaftsstrafrecht,. 3. Aufl. Heidelberg 2013, S. 816–853 (zit.: *Heghmanns*, in: Achenbach/Ransiek, HWSt^{3}).

Heimgartner, Stefan, Die internationale Dimension von Internetstraffällen – Strafhoheit und internationale Rechtshilfe in Strafsachen. In: Christian Schwarzenegger/Oliver Arter/Florian S. Jörg (Hrsg.), Internet-Recht und Strafrecht, 4. Tagungsband. Bern 2005, S. 117–150.

Heine, Günter, Beweisverbote und Vökerrecht: Die Affäre Liechtenstein in der Praxis. HRRS 2009, 540–547.

Heinrich, Bernd, Der Erfolg beim abstrakten Gefährdungsdelikt. GA 1999, 72–84.

– Anmerkung zu KG, Urteil vom 16.03.1999 – (5) 1 Ss 7/98 (8/89). NStZ 2000, 533–534.

Hellmann, Uwe, Strafprozessrecht. 2. Aufl. Berlin u.a. 2006.

Henrich, Andreas, Das passive Personalitätsprinzip im deutschen Strafrecht. Freiburg 1994.

Hermanns, Ferdinand, Völkerrechtliche Grenzen für die Anwendung kartellrechtlicher Verbotsnormen. Köln 1969.

Herrmann, Christoph, Richtlinienumsetzung durch die Rechtsprechung. Berlin 2003.

– Anmerkung zu EuGH, Urteil vom 16.06.2005 – C-105/03 (Maria Pupino). EuZW 2005, 436–438.

Heß, Marco, Die Verantwortlichkeit von Diensteanbietern für Informationen im Internet nach der Novellierung des Teledienstegesetzes. Münster 2005.

Hilgendorf, Eric, Überlegungen zur strafrechtlichen Interpretation des Ubiquitätsprinzips im Zeitalter des Internets. NJW 1997, 1873–1878.

– Zur Anwendbarkeit des § 5 TDG auf das Strafrecht. NStZ 2000, 518–522.

– Die Neuen Medien und das Strafrecht. ZStW 113 (2001), 650–680.

– Nationales oder transnationales Strafrecht? Europäisches Strafrecht, Völkerstrafrecht und Weltrechtsgrundsatz im Zeitalter der Globalisierung. In: Horst Dreier/Hans Forkel/Klaus Laubenthal (Hrsg.), Raum und Recht. Festschrift 600 Jahre Würzburger Juristenfakultät. Berlin 2002, S. 333–356.

– Tendenzen und Probleme einer Harmonisierung des Internetstrafrechts auf Europäischer Ebene. In: Christian Schwarzenegger/Oliver Arter/Florian S. Jörg (Hrsg.), Internet-Recht und Strafrecht, 4. Tagungsband. Bern 2005, S. 257–298.

Hinterseh, Sven, Die strafrechtliche Verantwortlichkeit für Pornographie im Internet: Ein Beitrag zum Thema „Datennetzkriminalität". JurPC 1996, 460–473.

Hirsch, Hans Joachim, Gefahr und Gefährlichkeit. In: Fritjof Haft/Winfried Hassemer/Ulfried Neumann/Wolfgang Schild/Ulrich Schroth (Hrsg.), Strafgerechtigkeit. Festschrift für Arthur Kaufmann zum 70. Geburtstag. Heidelberg 1993, S. 545–563.

Hochreiter, Monika, Die heimliche Überwachung internationaler Telekommunikation. Eine rechtsvergleichende Untersuchung zur Rechtsstaatlichkeit der Arbeit von Auslandsnachrichtendiensten in Deutschland und dem Vereinigten Königreich unter besonderer Berücksichtigung der Europäischen Menschenrechtskonvention. München 2002.

Hoeren, Thomas, Vorschlag für eine EU-Richtlinie über E-Commerce. Eine erste kritische Analyse. MMR 1999, 192–199.

– Zoning und Geolocation – Technische Ansätze zu einer Reterritorialisierung des Internet. MMR 2007, 3–6.

– Das Telemediengesetz. NJW 2007, 801–806.

Hoeren, Thomas/Sieber, Ulrich, Handbuch Multimedia-Recht. Rechtsfragen des elektronischen Geschäftsverkehrs, Stand 24. Ergänzungslieferung, Dezember 2009. München 2010 (zit.: *Bearbeiter*, in: Hoeren/Sieber, Handbuch Multimedia-Recht).

Holthausen, Dieter, Entgegnungen zum Beitrag von Pottmeyer „Die Strafbarkeit von Auslandstaten nach dem Kriegswaffenkontroll- und dem Außenwirtschaftsrecht" (NStZ 1992, 57 ff.). NStZ 1992, 268–269.

Holznagel, Bernd, Meinungsfreiheit oder Free Speech im Internet. Unterschiedliche Grenzen tolerierbarer Meinungsäußerungen in den USA und Deutschland. AfP 2002, 128–133.

Hoombrecher, Lars, Grundzüge und praktische Fragen des Internationalen Strafrechts – Teil 1: Strafanwendungsrecht und Internationale Rechtshilfe. JA 2010, 637–645.

Hörnle, Tatjana, Anmerkung zu BGH, Urteil vom 12.12.2000 – 1 StR 184/00. NStZ 2001, 309–311.

– Pornographische Schriften im Internet: Die Verbotsnormen im deutschen Strafrecht und ihre Reichweite. NJW 2002, 1008–1013.

Hunt, Craig/Thompson, Robert Bruce, Windows NT TCP/IP Netzwerk-Administration. Köln 1999.

Institut für Internationales Recht in Kiel (Hrsg.), Entscheidungen des Ständigen Internationalen Gerichtshofes. Ausgabe in deutscher Übersetzung, Fünfter Bd. (1927). Leiden (zit.: StIGHE, Band, Seite).

Ipsen, Knut, in Zusammenarbeit mit Volker Epping, Wolff Heintschel von Heinegg, Horst Fischer, Christian Gloria, Hans-Joachim Heintze, Völkerrecht. 5. Aufl. München 2004.

Jähnke, Burkhard/Laufhütte, Heinrich Wilhelm/Odersky, Walter (Hrsg.), Leipziger Kommentar zum Strafgesetzbuch. Großkommentar. 11. Aufl., §§ 19–21, 10. Lieferung. Berlin u.a. 1993 (zit.: LK-StGB[11]-*Bearbeiter*).

Jakobs, Günther, Strafrecht, Allgemeiner Teil: Die Grundlagen und die Zurechnungslehre. 2. Aufl. Berlin u.a. 1993.

Jarass, Hans D./Pieroth, Bodo, Grundgesetz für die Bundesrepublik Deutschland. 12. Aufl. München 2012 (zit.: *Bearbeiter*, in: Jarass/Pieroth, GG).

Jennings, R.Y., Extraterritorial jurisdiction and the United States Antitrust Laws. BYIL 33 (1957), 146–175.

Jescheck, Hans-Heinrich/Weigend, Thomas, Lehrbuch des Strafrechts. Allgemeiner Teil. 5. Aufl. Berlin 1996.

Jeßberger, Florian, Anmerkung zu BGH, Urteil vom 12.12.2000 – 1 StR 184/00. JR 2001, 432–435.

Joecks, Wolfgang/Miebach, Klaus (Hrsg.), Münchener Kommentar zum Srafgesetzbuch, Bd. 1, §§ 1–37. München 2011, Bd. 4, §§ 263–358 StGB, §§ 1–8, 105, 106 JGG. München 2006 (zit.: MünchKommStGB-*Bearbeiter*).

Jofer, Robert, Strafverfolgung im Internet. Phänomenologie und Bekämpfung kriminellen Verhaltens in internationalen Computernetzen. Frankfurt a.M. u.a. 1999.

Johnson, R. David/Post, David, Law and Borders – The Rise of Law in Cyberspace. Stanford Law Review 48 (1996), 1367–1402.

Kessler, Clemens, Zur strafrechtlichen Verantwortlichkeit von Zugangsprovidern in Deutschland und der Umsetzung der E-Commerce-Richtlinie in Europa. Berlin 2003.

Kienle, Michael, Internationales Strafrecht und Straftaten im Internet. Zum Erfordernis der Einschränkung des Ubiquitätsprinzips des § 9 Abs. 1 Var. 3 StGB. Konstanz 1998.

Kindhäuser, Urs, Gefährdung als Straftat. Rechtstheoretische Untersuchungen zur Dogmatik der abstrakten und konkreten Gefährdungsdelikte. Frankfurt a.M. 1989.

Kindhäuser, Urs/Neumann, Ulfried/Paeffgen, Hans-Ulrich (Hrsg.), NomosKommentar Strafgesetzbuch, Bd. 1: §§ 1–145d. 3. Aufl. Baden-Baden 2010 (zit.: NK-StGB-*Bearbeiter*).

Kioupis, Dimitrios, Strafrecht und Internet. In: Ilias G. Anagnostopoulos (Hrsg.), Internationalisierung des Strafrechts. Baden-Baden 2003, S. 93–113.

Kitz, Volker, Das neue Recht der elektronischen Medien in Deutschland – sein Charme, seine Fallstricke. ZUM 2007, 368–375.

Kitzinger, Friedrich, Ort und Zeit der Handlung im Strafrecht. Zugleich eine Betrachtung der Erscheinungsformen des Delikts. München 1902.

Klam, Cornelia, Die rechtliche Problematik von Glücksspielen im Internet. Berlin 2002.

Klengel, Jürgen Detlef W./Heckler, Andreas, Geltung des deutschen Strafrechts für vom Ausland aus im Internet angebotenes Glücksspiel. Ein Beitrag zur Frage des Erfolgsorts bei abstrakten Gefährdungsdelikten und zugleich eine Besprechung der Entscheidung des BGH vom 12.12.2000 – 1 StR 184/00. CR 2001, 243–249.

Kluge, Friedrich (Hrsg.), Etymologisches Wörterbuch der deutschen Sprache. 25. Aufl. Berlin u.a. 2011.

Klußmann, Niels, Lexikon der Kommunikations- und Informationstechnik. 3. Aufl. Heidelberg 2001.

Koch, Arnd, Zur Strafbarkeit der „Auschwitzlüge“ im Internet – BGHSt 46, 212. JuS 2002, 123–127.

Köhntopp, Marit/Köhntopp, Kristian, Datenspuren im Internet. CR 2000, 248–257.

König, Sabine, Kinderpornografie im Internet. Eine Untersuchung der deutschen Rechtslage unter besonderer Berücksichtigung des Internationalen Strafrechts. Hamburg 2004.

Koops, Bert-Jaap/Brenner, Susan W., Cybercrime and Jurisdiction – An Introduction. In: Bert-Jaap Koops/Susan W. Brenner (Hrsg.), Cybercrime and Jurisdiction. A Global Survey. Den Haag 2006, S. 1–8.

Köpsell, Stefan/Miosga, Tobias, Strafverfolgung trotz Anonymität. Rechtliche Rahmenbedingungen und technische Umsetzung. DuD 2005, 403–409.

Körber, Florian, Rechtsradikale Propaganda im Internet – der Fall Töben. Berlin 2003.

Koriath, Heinz, Zum Streit um die Gefährdungsdelikte. GA 2001, 51–74.

Kudlich, Hans, Strafprozessuale Probleme im Internet. Rechtliche Probleme der Beweisgewinnung in Computernetzen. JA 2000, 227–234.

– Anmerkung zu BGH, Urteil vom 12.12.2000 – 1 StR 184/00 (LG Mannheim). StV 2001, 397–399.

Kudlich, Hans, Die Neuregelung der strafrechtlichen Verantwortung von Internetprovidern. – Die Änderungen des TDG durch das EGG, insb. aus strafrechtlicher Sicht. JA 2002, 798–803.

– Strafrechtliche Fragen im Internet. In: Oliver Merx/Ernst Tandler/Heinfried Hahn (Hrsg.), Multimedia-Recht für die Praxis. Berlin 2002, S. 231–260.

– Die Unterstützung fremder Straftaten durch berufsbedingtes Verhalten. Berlin 2004.

– Herkunftslandprinzip und internationales Strafrecht. HRRS 2004, 278–284.

Kühl, Kristian, Strafrecht. Allgemeiner Teil. 7. Aufl. München 2012.

Kuner, Christopher, Internationale Zuständigkeitskonflikte im Internet. CR 1996, 453–458.

Kunig, Philip, Die Bedeutung des Nichteinmischungsprinzips für das Internationale Strafrecht der Bundesrepublik Deutschland – BGHSt 27, 30. JuS 1978, 594–596.

Kunig, Philip/Uerpmann, Robert, Der Fall des Postschiffes Lotus – StIGH – Urt. v. 7.9.1927 = PCIJ Series A No. 10. Jura 1994, 186–194.

Kyas, Othmar, Internet professionell. Technologische Grundlagen & praktische Nutzung. Bonn u.a. 1996.

Lackner, Karl/Kühl, Kristian, Strafgesetzbuch mit Erläuterungen. 27. Aufl. München 2011.

Lagodny, Otto, Empfiehlt es sich, eine europäische Gerichtskompetenz für Strafgewaltkonflikte vorzusehen? Gutachten im Auftrag des Bundesministeriums der Justiz. Berlin März 2001, abrufbar unter http://www.bib.uni-mannheim.de/fileadmin/pdf/fachinfo/jura/strafgewaltskonflikte-von-lagodny.pdf [Stand: 6.11.2013].

Landau, Herbert, Die Pflicht des Staates zum Erhalt einer funktionstüchtigen Strafrechtspflege. NStZ 2007, 121–129.

Lang-Hinrichsen, Dietrich, Der Überzeugungstäter in der deutschen Strafrechtsreform. JZ 1966, 153–162.

Laufhütte, Heinrich Wilhelm/Rissing-van Saan, Ruth/Tiedemann, Klaus (Hrsg.), Leipziger Kommentar zum Strafgesetzbuch. Großkommentar. 12. Aufl., Bd. 1: Einleitung, §§ 1–31. Berlin 2007; Bd. 4: §§ 80–109k. Berlin 2007 (zit.: LK-StGB[12]-*Bearbeiter*).

Lehle, Thomas, Der Erfolgsbegriff und die deutsche Strafrechtszuständigkeit im Internet, Mikrofiche-Ausgabe. Konstanz 1999.

Lehmann, Michael, Rechtsgeschäfte und Verantwortlichkeit im Netz- Der Richtlinienvorschlag der EU-Kommission. ZUM 1999, 180–184.

Leidenmühler, Franz/Plöckinger, Oliver, Zur Zuständigkeit bei Internetdelikten. Die völker- und strafrechtliche Dimension. In: Oliver Plöckinger/Dieter Duursma/Günther Helm (Hrsg.), Aktuelle Entwicklungen im Internet-Recht. Beiträge zur zivil-, straf- und verwaltungsrechtlichen Diskussion. Wien 2002, S. 101–112.

– Zur Zuständigkeit bei Internetdelikten. Die völker- und strafrechtliche Dimension. In: Oliver Plöckinger/Dieter Duursma/Michael Mayrhofer (Hrsg.), Internet-Recht. Beiträge zum Zivil- und Wirtschaftsprivatrecht, Öffentlichen Recht und Strafrecht. Wien u.a. 2004, S. 363–374.

Lenz, Karl-Friedrich, Strafrecht und Internet. In: Albin Eser (Hrsg.), Festschrift für Haruo Nishihara zum 70. Geburtstag, 5. Bd. Beiträge in deutscher Sprache. Baden-Baden 1998, S. 467–485.

Lessig, Lawrence/Resnick, Paul, Zoning speech on the internet: a legal and technical model. Michigan Law Review 98 (1999), 395–431.

Leupold, Andreas/Bachmann, Peter/Pelz, Christian, Russisches Roulette im Internet? MMR 2000, 648–655.

Ligeti, Katalin, Strafrecht und strafrechtliche Zusammenarbeit in der Europäischen Union. Berlin 2005.

Löhnig, Martin, „Verbotene Schriften" im Internet. JR 1997, 496–498.

Loock-Wagner, Oliver, Das Internet und sein Recht. Ein problemorientierter Grundriss. Stuttgart u.a. 2000.

Lowe, A. Vaughan, Extraterritorial Jurisdiction. The Bristish Practice. RabelsZ 1988, 156–204.

Macedo, Stephen (Hrsg.), The Princeton Principles on Universal Jurisdiction. Princeton, New Jersey, 2001.

Makarov, Alexander, Das Urteil des Internationalen Gerichtshofes im Fall Nottebohm. ZaöRV 16 (1955/56), 407–426.

Malek, Klaus, Strafsachen im Internet. Heidelberg 2005.

Mankowski, Peter, Internet und Internationales Wettbewerbsrecht. GRUR Int. 1999, 909–921.

– Das Herkunftslandprinzip als Internationales Privatrecht der e-commerce-Richtlinie. ZVglRWiss 100 (2001), 137–181.

Mansdörfer, Marco, Der internationalstrafrechtliche Geltungsbereich des Geldwäschetatbestandes. HHRS 2009, 252–256.

Manssen, Gerit (Hrsg.), Telekommunikations- und Multimediarecht. Ergänzbarer Kommentar zum Telekommunikationsgesetz, Mediendienste-Staatsvertrag, Teledienstegesetz, Teledienstedatenschutzgesetz, Signaturgesetz, einschließlich Gesetzes- und Verordnungstexten und europäischen Vorschriften, Bd. 2. Berlin 2005 (zit.: *Bearbeiter*, in: Manssen, Telekommunikations- und Multimediarecht, Bd. 2).

Marberth-Kubicki, Annette, Computer- und Internetstrafrecht. 2. Aufl. München 2010.

Martin, Jörg, Strafbarkeit grenzüberschreitender Umweltbeeinträchtigungen. Zugleich ein Beitrag zur Gefährdungsdogmatik und zum Umweltvölkerrecht. Freiburg 1989.

– Grenzüberschreitende Umweltbeeinträchtigungen im deutschen Strafrecht. ZRP 1992, 19–27.

Masing, Johannes, Vorrang des Europarechts bei umsetzungsgebundenen Rechtsakten. NJW 2006, 264–268.

Maurach, Reinhart/Gössel, Karl Heinz/Zipf, Heinz, Strafrecht Allgemeiner Teil, Teilband 2: Erscheinungsformen des Verbrechens und Rechtsfolgen der Tat. Ein Lehrbuch, 7. Aufl. Heidelberg 1989.

Mayer, Franz C., Recht und Cyberspace. NJW 1996, 1782–1791.

Mayer, Patrick G., Das Internet im öffentlichen Recht. Unter Berücksichtigung europarechtlicher und völkerrechtlicher Vorgaben. Berlin 1999.

McLean, Susan, Overseas Website Operators Beware? – The International Reach of the UK Defamation Laws. Status quo and potential changes by pending Defamation Bill. CRi 2012, 141–147.

Meessen, Karl Matthias, Völkerrechtliche Grundsätze des internationalen Kartellrechts. Baden-Baden 1975.

Meininghaus, Florian, Der Zugriff auf E-Mails im strafrechtlichen Ermittlungsverfahren. Hamburg 2007.

Meng, Werner, Neuere Entwicklungen im Streit um die Jurisdiktionshoheit der Staaten im Bereich der Wettbewerbsbeschränkungen. ZaöRV 41 (1981), 469–513.

– Völkerrechtliche Zulässigkeit und Grenzen wirtschaftsverwaltungsrechtlicher Hoheitsakte mit Auslandswirkung. ZaöRV 44 (1984), 675–783.

– Extraterritoriale Jurisdiktion im öffentlichen Wirtschaftsrecht. Berlin u.a. 1993.

Menzel, Jörg/Pierlings, Tobias/Hoffmann, Jeannine (Hrsg.), Völkerrechtsprechung. Ausgewählte Entscheidungen zum Völkerrecht in Retrospektive. Tübingen 2005.

Meseke, Bodo, Ermittlung und Fahndung im Internet. In: Bundeskriminalamt (Hrsg.), Festschrift für Horst Herold zum 75. Geburtstag. Wiesbaden 1998 S. 505–532.

– Ermittlungen im Internet – Positionen und Dissonanzen. Kriminalistik 2000, 245–249.

Mestmäcker, Ernst-Joachim, Staatliche Souveränität und offene Märkte. Konflikte bei extraterritorialer Anwendung von Wirtschaftsrecht. RabelsZ 1988, 205–255.

Meuters, Stefan, Leitung und Kontrolle grenzüberschreitender Ermittlungen. Zum Verhältnis von Staatsanwaltschaft und Polizei bei der grenzüberschreitenden Zusammenarbeit in Strafsachen in der Europäischen Union. Hamburg 2004.

Meyer-Goßner, Lutz, Strafprozessordnung, Gerichtsverfassungsgesetz, Nebengesetze und ergänzende Bestimmungen. 50. Aufl. München 2007 (zit.: *Meyer-Goßner*, StPO[50]).

– Strafprozessordnung, Gerichtsverfassungsgesetz, Nebengesetze und ergänzende Bestimmungen. 55. Aufl. München 2012 (zit.: *Meyer-Goßner*, StPO[55]).

Mitsdörffer, Sven/Gutfleisch, Ulf, „Geo-Sperren" – wenn Videoportale ausländische Nutzer aussperren. Eine urheberrechtliche Betrachtung. MMR 2009, 731–735.

Möhrenschlager, Manfred, Computerstraftaten und ihre Bekämpfung in der Bundesrepublik Deutschland. wistra 1991, 321–331.

– Internationale Regelungen durch die „Cyber Crime" Konvention des Europarates. In: Jürgen Welp (Hrsg.), kriminalität@net. Beiträge zur 13. Alsberg-Tagung 2001 in Berlin und zur Verleihung des Max-Alsberg-Preises an die Redaktion der Zeitschrift Strafverteidiger. Baden-Baden 2003, S. 97–112.

Moritz, Hans-Werner, Anmerkung zu LG München I, Urteil vom 17.11.1999 – 20 Ns 465 Js 173158/95 (AG München I). CR 2000, 119–121.

– Zulassung als Anbieter, S. 158 ff.; Strafbarkeit, S. 473 ff. In: Ulrich Loewenheim/Frank A. Koch (Hrsg.), Praxis des Online-Rechts. München 2001.

Moritz, Hans-Werner/Dreier, Thomas (Hrsg.), Rechts-Handbuch zum E-Commerce. 1. Aufl. Köln 2002 (zit.: *Bearbeiter*, in: Moritz/Dreier, Rechtshandbuch zum E-Commerce[1]).

– Rechts-Handbuch zum E-Commerce. 2. Aufl. Köln 2005 (zit.: *Bearbeiter*, in: Moritz/Dreier, Rechtshandbuch zum E-Commerce[2]).

Mosler, Hermann, Völkerrecht als Rechtsordnung. ZaöRV 36 (1976), 6–49.

Nagel, Karl-Friedrich, Beweisaufnahme im Ausland. Rechtsgrundlagen und Praxis der internationalen Rechtshilfe für deutsche Strafverfahren. Freiburg 1988.

Nagler, Johannes (Hrsg.), Leipziger Kommentar zum Strafgesetzbuch. Großkommentar. 6. Aufl., 1. Lieferung, Einleitung und §§ 1–152. Berlin 1944 (zit.: LK-StGB[6]-*Bearbeiter*).

Neuhaus, Rupert, Klaus, Das Rechtsmißbrauchsverbot im heutigen Völkerstrafrecht. Eine Untersuchung zur Entwicklung und Anwendbarkeit eines Begriffes. Berlin 1984.

Nickels, Sven, Neues Bundesrecht für den E-Commerce. CR 2002, 302–309.

Niedermair, Harald, Straflose Beihilfe durch neutrale Handlungen? ZStW 107 (1995), 507–544.

Nordmann, Eberhard, Die Beschaffung von Beweismitteln aus dem Ausland durch staatliche Stellen. Berlin 1979.

O'Connor, Vivienne/Rausch, Colette/Albrecht, Hans-Jörg/Klemencic, Goran, Model Codes for Post-Conflict Criminal Justice. Washington, D.C., 2007.

Oehler, Dietrich, Internationales Strafrecht. Geltungsbereich des Strafrechts. Internationales Rechtshilferecht. Recht der Gemeinschaften. Völkerstrafrecht. 2. Aufl. Köln u.a. 1983.

– Der europäische Binnenmarkt und sein wirtschaftsstrafrechtlicher Schutz. In: Gunther Arzt/Gerhard Fezer/Ulrich Weber/Ellen Schlüchter/Dieter Rössner (Hrsg.), Festschrift für Jürgen Baumann zum 70. Geburtstag 22. Juni 1992. Bielefeld 1992, S. 561–571.

Ohly, Ansgar, Herkunftslandprinzip und Kollisionsrecht. GRURInt 2001, 899–908.

Okresek, Wolf, Hoheitsakte auf fremdem Staatsgebiet. Eine Betrachtung anhand praktischer Fälle. ÖZöRV 35 (1985), 325–344.

Organisation for Economic Co-operation and Development, Computer-related Crime: Analysis of Legal Policy. Paris 1986.

Pappas, Claudia, Stellvertretende Strafrechtspflege. Zugleich ein Beitrag zur Ausdehnung deutscher Strafgewalt nach § 7 Abs. 2 Nr. 2 StGB. Freiburg 1996.

Park, Tido, Strafbarkeit von Internet-Providern wegen rechtswidriger Internet-Inhalte. GA 2001, 23–36.

Pätzel, Claus, Das Internet als Fahndungshilfsmittel der Strafverfolgungsbehörden. NJW 1997, 3131–3134.

Paul, Tobias, Primärrechtliche Regelungen zur Verantwortlichkeit von Internetprovidern aus strafrechtlicher Sicht. Baden-Baden 2005.

Pelz, Christian, Die strafrechtliche Verantwortlichkeit von Internet-Providern. ZUM 1998, 530–534.

Pelz, Christian, E-Commerce – Strafbarkeit, das vergessene Risiko, abrufbar unter http://web.archive.org/web/20050226134507/http://www.der-syndikus.de/briefings/it/it_017.htm [Stand: 6.11.2013].

Pfeiffer, Gerd, Strafprozessordnung und Gerichtsverfassungsgesetz. 5. Aufl. München 2007.

Plöckinger, Oliver, Zur Zuständigkeit österreichischer Gerichte bei Straftaten im Internet. ÖJZ 2001, 798–804.

Poenig, Andreas, Die strafrechtliche Haftung des Linkanbieters im Ausland nach deutschem Recht. Göttingen 2006.

Popp, Martin, Die strafrechtliche Verantwortung von Internet-Providern. Berlin 2002.

Pottmeyer, Klaus, Die Strafbarkeit von Auslandstaten nach dem Kriegswaffenkontroll- und dem Außenwirtschaftsrecht. NStZ 1992, 57–62.

Preuße, Thomas, Informationsdelikte im Internet. Hamburg 2001.

Raabe, Oliver, Die rechtliche Einordnung zweier Web-Anonymisierungsdienste. DuD 2003, 134–138.

Radbruch, Gustav, Der Überzeugungstäter. ZStW 44 (1924), 34–38.

Rasmussen, Heike, Datenschutz im Internet. Gesetzgeberische Maßnahmen zur Verhinderung der Erstellung ungewollter Nutzerprofile im Web – Zur Neufassung des TDDSG. CR 2002, 36–45.

Rath, Jürgen, Internationales Strafrecht (§§ 3–7 StGB) – Prüfungsschema, Auslandsbezug, Tatortbestimmung. JA 2006, 435–439.

Rehbinder, Eckard, Extraterritoriale Wirkungen des deutschen Kartellrechts. Baden-Baden 1965.

Reinel, Stefan, Die Auslandskopfüberwachung – Rechtsstaat auf Abwegen? wistra 2006, 205–210.

Rieß, Peter (Hrsg.), Löwe-Rosenberg, Die Strafprozeßordnung und das Gerichtsverfassungsgesetz. Großkommentar, §§ 151–212b StPO. 26. Aufl. Berlin u.a. 2008 (zit.: LR-StPO-*Bearbeiter*).

Rietzsch, Die Verordnung über den Geltungsbereich des Strafrechts vom 6. Mai 1940. RGBl. I, 754. Deutsche Justiz 1940, 563–566.

Ringel, Kurt, Rechtsextremistische Propaganda aus dem Ausland im Internet. CR 1997, 302–307.

Ritlewski, Kristoff M., Virtuelle Kinderpornographie in Second Life. Deutsche und US-amerikanische Regulierung von Online-Spielen im Spannungsverhältnis zwischen Verfassung und völkerrechtlichen Übereinkommen. K&R 2008, 94–99.

Rogall, Klaus, Hypothetische Ermittlungsverläufe im Strafprozeß – Ein Beitrag zur Lehre der Beweiserhebungs- und Beweisverwertungsverbote. NStZ 1988, 385–393.

Roger, Benjamin, Europäisierung des Strafverfahrens – oder nur der Strafverfolgung? Zum Rahmenbeschluss über die Europäische Beweisanordnung. GA 2010, 26–43.

Römer, Nicole, Verbreitungs- und Äußerungsdelikte im Internet. Eine Untersuchung zur strafrechtlichen Bewältigung von Normanwendungs- und Normauslegungsproblemen eines neuen Kriminalitätsfeldes. Frankfurt a.M. 2000.

Roxin, Claus, Strafrecht Allgemeiner Teil, Bd. II: Besondere Erscheinungsformen der Straftat. München 2003.

– Allgemeiner Teil, Bd. I: Grundlagen, der Aufbau der Verbrechenslehre. 4. Aufl. München 2006.

– Zum Beweisverwertungsverbot bei bewusster Missachtung des Richtervorbehalts nach § 105 I 1 StPO. NStZ 2007, 616–618.

Roxin, Claus/Schünemann, Bernd, Strafverfahrensrecht. 27. Aufl. München 2012.

Rudolf, Walter, 1. Referat, Territoriale Grenzen der staatlichen Rechtssetzung, S. 7–45. In: Berichte der Deutschen Gesellschaft für Völkerrecht, Heft 11, Territoriale Grenzen der staatlichen Rechtssetzung. Referate und Diskussion der 12. Tagung der Deutschen Gesellschaft für Völkerrecht in Bad Godesberg vom 14. bis 16. Juni 1971. Karlsruhe 1974 (zit.: *Rudolf*, in: BerDGesVölkR 11).

Ruess, Peter, Die E-Commerce-Richtlinie und das deutsche Wettbewerbsrecht. Eine Analyse der Auswirkungen unter besonderer Berücksichtigung des Herkunftslandprinzips. München 2003.

Sachs, Michael (Hrsg.), Grundgesetz Kommentar. 6. Aufl. München 2011 (zit.: *Bearbeiter*, in: Sachs, GG).

Sahlfeld, Miriam, Die Veränderung der Ausübung von Staatsgewalt. Aufgezeigt an den staatlichen Reaktionen auf Rechtsverletzungen im Internet. Berlin 2004.

Sankol, Barry, Verletzung fremdstaatlicher Souveränität durch ermittlungsbehördliche Zugriffe auf E-Mail-Postfächer. K&R 2008, 279–285.

Satzger, Helmut, Die Anwendung des deutschen Strafrechts auf grenzüberschreitende Gefährdungsdelikte. NStZ 1998, 112–117.

– Die Europäisierung des Strafrechts. Eine Untersuchung zum Einfluß des Europäischen Gemeinschaftsrechts auf das deutsche Strafrecht. Köln u.a. 2001.

– Strafrechtliche Verantwortlichkeit von Zugangsvermittlern. Eine Untersuchung der Verantwortlichkeit für rechtswidrige Inhalte im Internet vor dem Hintergrund der neuen E-Commerce-Richtline. CR 2001, 109–117.

– Strafrechtliche Providerhaftung. In: Peter W. Heermann/Ansgar Ohly (Hrsg.), Verantwortlichkeit im Internet. Wer haftet wofür? Stuttgart u.a. 2003, S. 161–180.

– Das deutsche Strafanwendungsrecht (§§ 3 ff. StGB) – Teil 1. Jura 2010, 108–116.

– Internationales und Europäisches Strafrecht. 6. Aufl. Baden-Baden 2013.

Schädel, Peter, Die Bewilligung internationaler Rechtshilfe in Strafsachen in der Europäischen Union. Das Spannungsfeld von Nationalstaatlichkeit und Europäischer Integration. Baden-Baden 2005.

Schantz, Peter, Verfassungsrechtliche Probleme von „Online-Durchsuchungen". KritV 2007, 310–330.

Scheller, Susanne, Ermächtigungsgrundlagen für die internationale Rechts- und Amtshilfe zur Verbrechensbekämpfung. Konkretisierung des Gesetzesvorbehalts. Freiburg 1997.

Schlochauer, Hans-Jürgen, Die extraterritoriale Wirkung von Hoheitsakten nach dem öffentlichen Recht der Bundesrepublik Deutschland und nach internationalem Recht. Frankfurt a.M. 1962.

Schmalz, Dieter, Methodenlehre für das juristische Studium. 4. Aufl. Baden-Baden 1998.

Schmidt, Eberhard, Die Verletzung der Belehrungspflicht gemäß § 55 II StGB als Revisionsgrund. JZ 1958, 596–601.

Schmidt, Stephan, Die Rechtmäßigkeit staatlicher Gefahrenabwehrmaßnahmen im Internet unter besonderer Berücksichtigung des Europäischen Gemeinschaftsrechts. Frankfurt a.M. 2006.

Schmidt, Uwe, Die Rechtsprechung zum Recht der Internationalen Rechtshilfe in Strafsachen seit dem Jahr 2000. NStZ-RR 2005, 161–167.

Schmitt, Bertram, Zur räumlichen Geltung des deutschen Strafrechts bei Straftaten im Internet. In: Horst Dreier/Hans Forkel/Klaus Laubenthal (Hrsg.), Raum und Recht. Festschrift 600 Jahre Würzburger Juristenfakultät. Berlin 2002, S. 357–375.

Schnigula, Jürgen, Probleme der internatonalen Rechtshilfe in Strafsachen bei ausgehenden deutschen Ersuchen im Bereich der „sonstigen" Rechtshilfe. DRiZ 1984, 177–183.

Scholten, Hans-Joseph, Das Erfordernis der Tatortstrafbarkeit in § 7 StGB. Ein Beitrag zur identischen Norm im transnationalen Strafrecht. Freiburg 1995.

Schomburg, Wolfgang/Lagodny, Otto/Gleß, Sabine/Hackner, Thomas, Internationale Rechtshilfe in Strafsachen. International Cooperation in Criminal Matters. Kommentar zum Gesetz über die internationale Rechtshilfe in Strafsachen. 4. Aufl. München 2006.

Schönke, Adolf/Schröder, Horst, Strafgesetzbuch. Kommentar. 28. Aufl. München 2010 (zit.: S/S-*Bearbeiter*).

Schreibauer, Marcus, Das Pornographieverbot des § 184 StGB. Grundlagen-Tatbestandsprobleme-Reformvorschläge. Regensburg 1999.

Schröder, Christian, Europäische Richtlinien und deutsches Strafrecht. Eine Untersuchung über den Einfluß europäischer Richtlinien gemäß Art. 249 Abs. 3 EGV auf das deutsche Strafrecht. Berlin u.a. 2002.

Schroeder, Friedrich-Christian, Schranken für den räumlichen Geltungsbereich des Strafrechts. NJW 1969, 81–85.

Schröder, Horst, Abstrakt-konkrete Gefährdungsdelikte? JZ 1967, 522–525.

Schulz, Wolfgang, Verfassungsrechtlicher „Datenschutzauftrag" in der Informationsgesellschaft. Schutzkonzepte zur Umsetzung informationeller Selbstbestimmung am Beispiel von Online-Kommunikation. Die Verwaltung 1999, 137–177.

Schünemann, Bernd, Die deutschsprachige Strafrechtswissenschaft im Spiegel des Leipziger Kommentars und des Wiener Kommentars, 2. Teil: Schuld und Kriminalpolitik. GA 1986, 293–352.

Schuster, Frank Peter, Verwertbarkeit im Ausland gewonnener Beweise im deutschen Strafprozess. Berlin 2006.

– Telekommunikationsüberwachung in grenzüberschreitenden Strafverfahren nach Inkrafttreten des EU-Rechtshilfeübereinkommens. NStZ 2006, 657–663.

Schwarzenegger, Christian, Der räumliche Geltungsbereich des Strafrechts im Internet. Die Verfolgung von grenzüberschreitender Internetkriminalität in der Schweiz im Vergleich mit Deutschland und Österreich. ZStrR 118 (2000), 109–110.

– Abstrakte Gefahr als Erfolg im Strafanwendungsrecht – ein leading case zu grenzüberschreitenden Internetdelikten. sic! 2001, 240–252.

– Hyperlinks und Suchmaschinen aus strafrechtlicher Sicht. In: Oliver Plöckinger/Dieter Duursma/Michael Mayrhofer (Hrsg.), Internet-Recht. Beiträge zum Zivil- und Wirtschaftsprivatrecht, Öffentlichen Recht, Strafrecht. Wien 2004, S. 395–434.

Schwörer, Andreas, Schranken grenzüberschreitender Beweisnutzung im Steuer- und Strafverfahren. wistra 2009, 452–458.

Seitz, Nicolai, Strafverfolgungsmaßnahmen im Internet. Köln u.a. 2004.

– Transborder Search: A New Perspective in Law Enforcement? IJCLP 9/2004, 1–18.

Sieber, Stefanie/Klimek, Alexander, Werbung in Push-Diensten: Zulässige unaufgeforderte kommerzielle Kommunikation? K&R 1999, 305–308.

Sieber, Ulrich, The international handbook on computer crime: computer-related economic crime and the infringements of privacy. Chichester u.a. 1986.

– Collecting and using evidence in the field of information technology. A comparative analysis. In: Albin Eser/Jonatan Thormundsson (Hrsg.), Old Ways and New Needs in Criminal Legislation. Documentation of a German-Icelandic Colloquium on the Development of Penal Law in General and Economic Crime in Particular. Freiburg 1989, S. 203–239.

– Europäische Einigung und Europäisches Strafrecht. ZStW 103 (1991), 957–979.

– The International Emergence of Criminal Information Law. Köln u.a. 1992.

– Strafrechtliche Verantwortlichkeit für den Datenverkehr in internationalen Computernetzen (1). JZ 1996, 429–442.

– Cyberlaw: Die Entwicklung im deutschen Recht. In: William R. Cheswick/Steven M. Bellovin (Hrsg.), Firewalls und Sicherheit im Internet. Schutz vernetzter Systeme vor cleveren Hackern. Deutsche Übersetzung von Thomas Maus. Bonn u.a. 1996, S. 283–325.

– Legal Aspects of Computer-Related Crime in the Information Society, – COMCRIME-Study –, prepared for the European Commission, 1998, abrufbar aus dem Web-Archiv unter http://web.archive.org/web/20051029105251/http://www.jura.uni-muenchen.de/einrichtungen/ls/sieber/article/comcrime/comcrime_www.pdf [Stand: 6.11.2013].

– Internationales Strafrecht im Internet. NJW 1999, 2065–2073.

– Die Bekämpfung von Hass im Internet. ZRP 2001, 97–103.

– Cybercrime and Jurisdiction in Germany. The Present Situation and the Need for New Solutions. In: Bert-Jaap Koops/Susan W. Brenner (Hrsg.), Cybercrime and Jurisdiction. A Global Survey. Den Haag 2006, S. 183–210.

– Straftaten und Strafverfolgung im Internet. München 2012.

Sieber, Ulrich/Brüner, Franz-Herrmann/Satzger, Helmut/von Heintschel-Heinegg, Bernd, Europäisches Strafrecht. Baden-Baden 2011 (zit.: *Bearbeiter*, in: Sieber/Brüner/Satzger/von Heintschel-Heinegg, Europäisches Strafrecht).

Sieber, Ulrich/Nolde, Malaika, Sperrverfügungen im Internet. Nationale Rechtsdurchsetzung im globalen Cyberspace? Berlin 2008.

Siegrist, Dave, Hoheitsakte auf fremdem Staatsgebiet. Zürich 1987.

Simma, Bruno, Grenzüberschreitender Informationsfluß und domain réservé der Staaten. In: Berichte der Deutschen Gesellschaft für Völkerrecht, Heft 19, Das Problem des grenzüberschreitenden Informationsflusses und des „domain réservé" (Free Flow of Information Across Boundaries and the „domain réservé"). 16. Tagung in Köln vom 5. bis 7. April 1979. Karlsruhe 1979, S. 39–88 (zit.: *Simma*, in: BerDGesVölkR 19).

Sofaer, Abraham D./Goodman, Seymour E. (Hrsg.), The Transnational Dimension of Cyber Crime and Terrorism. Stanford, California, 2001.

Soiné, Michael, Fahndung via Internet – 1. Teil. NStZ 1997, 166–169.

– Strafverfolgung, Polizei und Internet – Teil 1. Polizeispiegel 2001, 167–174; Teil 2, Polizeispiegel 2001, 199–200.

Spang-Hanssen, Henrik, Cyberspace & International Law on Jurisdiction. Kopenhagen 2004.

Spatscheck, Rainer, Steuern im Internet. Steuerprobleme des E-Commerce. Köln 2000.

– Steuerhinterziehung im Internet. StraFO 2000, 1–7.

– Der Beschuldigte im virtuellen Ermittlungsverfahren. Verteidigungsmöglichkeiten im globalen Netz. In: Jürgen Welp (Hrsg.), kriminalität@net. Beiträge zur 13. Alsberg-Tagung 2001 in Berlin und zur Verleihung des Max-Alsberg-Preises an die Redaktion der Zeitschrift Strafverteidiger. Baden-Baden 2003, S. 85–95.

Spatscheck, Rainer/Alvermann, Jörg, Internet-Ermittlungen im Steuerstrafprozeß. Verfahrensprobleme bei der Einführung in die Hauptverhandlung. wistra 1999, 333–336.

– Steuerfahndung ohne Grenzen? – Auslandsermittlungen im Steuer- und Steuerstrafverfahren. IStR 2001, 33–39.

Spindler, Gerald, E-Commerce in Europa. Die E-Commerce-Richtlinie in ihrer endgültigen Fassung. Beilage 7 zu MMR 2000, 4–21.

– Der Entwurf zur Umsetzung der E-Commerce-Richtlinie. ZRP 2001, 203–207.

– Das Gesetz zum elektronischen Geschäftsverkehr – Verantwortlichkeit der Dienste-anbieter und Herkunftslandprinzip. NJW 2002, 921–927.

– Das Herkunftslandprinzip im neuen Teledienstegesetz. RIW 2002, 183–188.

– Herkunftslandprinzip und Kollisionsrecht – Binnenmarktintegration ohne Harmonisierung? Die Folgen der Richtlinie im elektronischen Geschäftsverkehr für das Kollisionsrecht. RabelsZ 66 (2002), 633–709.

Spindler, Gerald/Schmitz, Peter/Geis, Ivo, TDG Teledienstegesetz, Teledienstedatenschutzgesetz, Signaturgesetz Kommentar. München 2004 (zit.: *Bearbeiter*, in: Spindler/Schmitz/Geis, TDG).

Stegbauer, Andreas, Rechtsextremistische Propaganda im Lichte des Strafrechts. München 2000.

Stein, Torsten/von Buttlar, Christina, Völkerrecht. 13. Aufl. München 2012.

Storbeck, Jürgen, Verwirrend – von Gesetzes wegen. Wenn im Ausland ermittelt werden muß, können in der Bundesrepublik viele Behörden zuständig sein. Kriminalistik 1987, 472–474.

Störing, Marc, Anmerkung zu LG Hamburg, Beschluss vom 08.01.2008 - 619 Qs 1/08. MMR 2008, 187–189.

Strupp, Karl, Das völkerrechtliche Delikt. In: G.A. Walz (Hrsg.), Handbuch des Völkerrechts, Dritter Bd.: Staatsorgane – Staatsverträge – Völkerrechtliches Delikt. Stuttgart 1920.

Strupp, Karl/Schlochauer, Hans-Jürgen (Hrsg.), Wörterbuch des Völkerrechts, Erster Bd.: Aachener Kongress bis Hussar-Fall. 2. Aufl. Berlin 1960 (zit.: *Bearbeiter*, in: Strupp/Schlochauer, Stichwort, Wörterbuch des Völkerrechts, Bd. 1).

Tettenborn, Alexander, Europäischer Rechtsrahmen für den elektronischen Geschäftsverkehr. K&R 1999, 252–258.

Tettenborn, Alexander/Bender, Gunnar/Lübben, Natalie/Karenfort, Matthias, Rechtsrahmen für den elektronischen Geschäftsverkehr. Kommentierung zur EG-Richtlinie über den elektronischen Geschäftsverkehr und zum Elektronischen Geschäftsverkehr-Gesetz – EGG: Inhalt – Auswirkungen – Umsetzung in Deutschland. Beilage Nr. 10 zu BB 2001, S. 1–40.

Tiedemann, Jens, Die Auslandskopf-Überwachung nach der TKÜV 2005. Zulässige Telekommunikationsüberwachung oder Eingriff in die Souveränität fremder Staaten? CR 2005, 858–864.

Tiedemann, Klaus, Privatdienstliche Ermittlungen im Ausland – strafprozessuales Verwertungsverbot? In: Arthur Kaufmann (Hrsg.), Festschrift für Paul Bockelmann zum 70. Geburtstag am 7. Dezember 1978. München 1979, S. 819–830.

– Europäisches Gemeinschaftsrecht und Strafrecht. NJW 1993, 23–31.

Tiedemann, Klaus/Kindhäuser, Urs, Umweltstrafrecht – Bewährung oder Reform? NStZ 1988, 337–346.

Tomuschat, Christian, Völkerrecht. 4. Aufl. Baden-Baden 2009.

Triantafyllou, Anastassios, Das Delikt der gefährlichen Körperverletzung (§ 223a StGB) als Gefährdungsdelikt. Zugleich ein Beitrag zur Dogmatik der Gefährdungsdelikte. Frankfurt a.M. u.a. 1996.

Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein, Verkettung digitaler Identitäten, Version 1.0, abrufbar unter https://www.datenschutzzentrum.de/projekte/verkettung/2007-uld-tud-verkettung-digitaler-identitaeten-bmbf.pdf [Stand: 6.11.2013].

United Nations, Yearbook of the International Law Commission 1979, vol. II, Part Two, Report of the Commission to the General Assembly on the work of its thirty-first session. New York 1980.

– Manual on the prevention and control of computer-related crime. International review of criminal policy. International Review of Criminal Policy, Nos. 43 and 44. 1994.

Vahrenwald, Arnold (Hrsg.), Recht in Online und Multimedia. Praxis-Handbuch, Loseblatt-Ausgabe 6. Aktualisierung, Dez. 2001. Neuwied u.a.

Valerius, Brian, Das globale Unrechtsbewusstsein. Oder: zum Gewissen im Internet. NStZ 2003, 341–346.

– Ermittlungen der Strafverfolgungsbehörden in den Kommunikationsdiensten des Internet. Hoheitliche Recherchen in einem grenzüberschreitenden Medium. Berlin 2004.

Vander Beken, Tom/Vermeulen, Gert/Lagodny, Otto, Kriterien für die jeweils „beste" Strafgewalt in Europa. Zur Lösung von Zuständigkeitskonflikten jenseits eines transnationalen Ne-bis-in-idem. NStZ 2002, 624–628.

Vander Beken, Tom/Vermeulen, Gert/Steverlynck, Soetekin/Thomaes, Stefan, Finding the Best Place for Prosecution. European study on jurisdiction criteria. European Commission (2001/GRP/025). Antwerpen/Apeldoorn 2002.

Vassilaki, Irini E., Strafrechtliche Verantwortlichkeit der Diensteanbieter nach dem TDG. Eine Untersuchung unter besonderer Berücksichtigung der Einordnung des § 5 TDG im Strafrechtssystem. MMR 1998, 630–638.

– Anmerkung zu BGH, Urteil vom 12.12.2000 – 1 StR 184/00. CR 2001, 262–265.

Vec, Miloš, Internet, Internationalisierung und nationalstaatlicher Rechtsgüterschutz. NJW 2002, 1535–1539.

Verdross, Alfred/Simma, Bruno, Universelles Völkerrecht. Theorie und Praxis. 3. Aufl. Berlin 1984.

Vogel, Joachim, Stand und Tendenzen der Harmonisierung des materiellen Strafrechts in der Europäischen Union. In: Frank Zieschang/Eric Hilgendorf/Klaus Laubenthal (Hrsg.), Strafrecht und Kriminalität in Europa. Baden-Baden 2003, S. 29–56.

Volk, Annette, Glücksspiel im Internet. Köln u.a. 2006.

von Bonin, Andreas/Köster, Oliver, Internet im Lichte neuer Gesetze. ZUM 1997, 821–829.

von Briel, Olaf G./Ehlscheid, Dirk, Steuerstrafrecht. 2. Aufl. Bonn 2001.

von Bubnoff, Eckhart, Krimineller Missbrauch der neuen Medien im Spiegel europäischer Gegensteuerung. In: Frank Zieschang/Eric Hilgendorf/Klaus Laubenthal (Hrsg.), Strafrecht und Kriminalität in Europa. Baden-Baden 2003, S. 83–106.

von der Groeben, Hans/Schwarze, Jürgen (Hrsg.), Kommentar zum Vertrag über die Europäische Union und zur Gründung der Europäischen Gemeinschaft, Bd. 1 Art. 1–53 EUV, Art. 1–80 EGV. 6. Aufl. Baden-Baden 2003 (zit.: *Bearbeiter*, in: von der Groeben/Schwarze, EGV).

von Heintschel-Heinegg, Bernd/Stöckel, Heinz (Hrsg.), KMR, Kommentar zur Strafprozessordnung, Bd. 2: §§ 94–150, Bd. 3: §§ 151–225a. Köln 2011 (Stand 69. Lieferung, Oktober 2013) (zit.: KMR-*Bearbeiter*).

von Hinden, Michael, Persönlichkeitsverletzungen im Internet. Das anwendbare Recht. Tübingen 1999.

von der Horst, Rutger, Rollt die Euro-Pornowelle? Zur Strafbarkeit von aus dem Ausland gesendeter Porno-Satellitenprogramme nach deutschem Strafrecht. ZUM 1993, 227–230.

von Münch, Ingo, Das völkerrechtliche Delikt in der modernen Entwicklung der Völkerrechtsgemeinschaft. Frankfurt a.M. 1963.

von Münch, Ingo/Kunig, Philip, Grundgesetz-Kommentar, Bd. 1 (Präambel bis Art. 19). 6. Aufl. München 2012 (zit.: *Bearbeiter*, in: v. Münch/Kunig, GG).

Wabnitz, Heinz-Bernd/Janovsky, Thomas (Hrsg.), Handbuch des Wirtschafts- und Steuerrechts. 3. Aufl. München 2007.

Walden, Ian, Computer Crimes and Digital Investigations. New York 2007.

Walter, Tonio, Einführung in das internationale Strafrecht. JuS 2006, 870–873.

Weigend, Thomas, Unbegrenzte Freiheit oder grenzenlose Strafbarkeit im Internet? In: Gerhard Hohloch (Hrsg.), Recht und Internet. Baden-Baden 2001, S. 85–92.

Weingärtner, Dieter, Globale Netze und lokale Werte. Möglichkeiten und Grenzen strafrechtlicher Regulierung. AfP 2002, 134–136.

Werle, Gerhard, Anmerkung zu BGH, Urteil vom 30.04.1999 – 3 StR 215/98 (OLG Düsseldorf). JZ 1999, 1181–1184.

Werle, Gerhard/Jeßberger, Florian, Grundfälle zum Strafanwendungsrecht. JuS 2001, 35–39; 141–144.

Wessels, Johannes/Beulke, Werner, Strafrecht Allgemeiner Teil. 42. Aufl. Heidelberg 2012.

Wiedemann, Peter, Tatwerkzeug Internet. Ein Überblick über das System und seine kriminelle Nutzung. Kriminalistik 2000, 229–239.

Wilske, Stephan, Die völkerrechtswidrige Entführung und ihre Rechtsfolgen. Berlin 2000.

Wolter, Jürgen, Beweisverbote und Umgehungsverbote zwischen Wahrheitserforschung und Ausforschung. In: Claus-Wilhelm Canaris (Hrsg.), 50 Jahre Bundesgerichtshof. Festgabe aus der Wissenschaft, Bd. IV: Strafrecht, Strafprozeßrecht. München 2000, S. 963–1009.

– (Hrsg.), Systematischer Kommentar zum Strafgesetzbuch, Bd. 1 §§ 1–45b, Bd. 2: §§ 80–122, Bd. 3: §§ 123–358. 8. Aufl. Köln 2013 (138. Lieferung, Mai 2013) (zit.: SK-StGB-*Bearbeiter*).

Ziegenhain, Hans-Jörg, Extraterritoriale Rechtsanwendung und die Bedeutung des Genuine-Link-Erfordernisses. Eine Darstellung der deutschen und amerikanischen Staatenpraxis. München 1992.

Zieher, Wolfgang, Das sog. Internationale Strafrecht nach der Reform. Der Rechtsgrund bei Straftaten im Ausland nach den §§ 5 und 6 StGB. Berlin 1977.

Ziercke, Jörg, Polizei in der digitalen Welt. Tatort Internet – eine globale Herausforderung für die Innere Sicherheit, BKA-Herbsttagung vom 20.–22. November 2007, Langfassung, abrufbar unter http://www.bka.de/nn_193608/SharedDocs/Downloads/DE/Publikationen/Herbsttagungen/2007/herbsttagung2007zierckeLangfassung,templateId=raw,property=publicationFile.pdf/herbsttagung2007zierckeLangfassung.pdf [Stand: 6.11.2013].

Zöchbauer, Peter, Herkunftslandprinzip und Strafrecht. In: Oliver Plöckinger/Dieter Duursma/Michael Mayrhofer (Hrsg.), Internet-Recht. Beiträge zum Zivil- und Wirtschaftsprivatrecht, Öffentlichen Recht, Strafrecht. Wien 2004, S. 435–444.

Zöller, Mark A., Der Rechtsrahmen der Nachrichtendienste bei der Terrorismus-„Bekämpfung". JZ 2007, 763–771.

Zusammenstellung der gutachterlichen Äußerungen über den Vorentwurf zu einem Deutschen Strafgesetzbuch, Gefertigt im Reichs=Justizamt, als Manuskript gedruckt. Berlin 1911 (zit.: *Stellungnehmender*, in: Zusammenstellung der gutachterlichen Äußerungen über den Vorentwurf zu einem Deutschen Strafgesetzbuch).

Schriftenreihe des Max-Planck-Instituts für ausländisches und internationales Strafrecht

Die zentralen Veröffentlichungen des Max-Planck-Instituts für ausländisches und internationales Strafrecht werden in Zusammenarbeit mit dem Verlag Duncker & Humblot in den folgenden vier Unterreihen der „Schriftenreihe des Max-Planck-Instituts für ausländisches und internationales Strafrecht“ vertrieben:

- „Strafrechtliche Forschungsberichte“,
- „Kriminologische Forschungsberichte“,
- „Interdisziplinäre Forschungen aus Strafrecht und Kriminologie“ sowie
- „Sammlung ausländischer Strafgesetzbücher in deutscher Übersetzung“.

Diese Publikationen können direkt über das Max-Planck-Institut unter <www.mpicc.de> oder über den Verlag Duncker & Humblot unter <www.duncker-humblot.de> erworben werden.

Darüber hinaus erscheinen im Hausverlag des Max-Planck-Instituts in der Unterreihe „research in brief“ zusammenfassende Kurzbeschreibungen von Forschungsergebnissen und in der Unterreihe „Arbeitsberichte“ Veröffentlichungen vorläufiger Forschungsergebnisse. Diese Veröffentlichungen können über das Max-Planck-Institut bezogen werden.

Detaillierte Informationen zu den einzelnen Publikationen des Max-Planck-Instituts für ausländisches und internationales Strafrecht sind unter <www.mpicc.de> abrufbar.

The main research activities of the Max Planck Institute for Foreign and International Criminal Law are published in the following four subseries of the “Schriftenreihe des Max-Planck-Instituts für ausländisches und internationales Strafrecht” (Research Series of the Max Planck Institute for Foreign and International Criminal Law), which are distributed in cooperation with the publisher Duncker & Humblot:

- “Strafrechtliche Forschungsberichte” (Reports on Research in Criminal Law),
- “Kriminologische Forschungsberichte” (Reports on Research in Criminology),
- “Interdisziplinäre Forschungen aus Strafrecht und Kriminologie” (Reports on Interdisciplinary Research in Criminal Law and Criminology), and
- “Sammlung ausländischer Strafgesetzbücher in deutscher Übersetzung” (Collection of Foreign Criminal Laws in German Translation).

These publications can be ordered from the Max Planck Institute at <www.mpicc.de> or from Duncker & Humblot at <www.duncker-humblot.de>.

Two additional subseries are published directly by the Max Planck Institute for Foreign and International Criminal Law: “research in brief” contains short reports on results of research activities, and “Arbeitsberichte” (working materials) present preliminary results of research projects. These publications are available at the Max Planck Institute.

Detailed information on all publications of the Max Planck Institute for Foreign and International Criminal Law can be found at <www.mpicc.de>.

Max-Planck-Institut für ausländisches
und internationales Strafrecht

Auswahl aus dem strafrechtlichen Veröffentlichungsprogramm:

S 141 *Gang Wang*
Die strafrechtliche Rechtfertigung von Rettungsfolter
Ein Rechtsvergleich zwischen Deutschland und den USA
2014 • 428 Seiten • ISBN 978-3-86113-815-0 € 41,00

S 140 *Ulrich Sieber / Marc Engelhart*
Compliance Programs for the Prevention of Economic Crimes
An Empirical Survey of German Companies
2014 • 312 Seiten • ISBN 978-3-86113-816-7 € 40,00

S 139 *Susanne Rheinbay*
Die Errichtung einer Europäischen Staatsanwaltschaft
2014 • 347 Seiten • ISBN 978-3-86113-819-8 € 35,00

S 138 *Sarah Herbert*
Grenzen des Strafrechts bei der Terrorismusgesetzgebung
Ein Rechtsvergleich zwischen Deutschland und England
2014 • 300 Seiten • ISBN 978-3-86113-820-4 € 35,00

S 137 *Nadine Zurkinden*
Joint Investigation Teams
Chancen und Grenzen von gemeinsamen Ermittlungsgruppen in der Schweiz, Europa und den USA
2013 • 396 Seiten • ISBN 978-3-86113-821-1 € 41,00

S 136 *Nico Herbert*
Strafrechtlicher Schutz von EU-Subventionen
Reichweite und Grenzen in Deutschland, Österreich und England am Beispiel nicht wirtschaftsfördernder Subventionen
2013 • 320 Seiten • ISBN 978-3-86113-823-5 € 38,00

S 135 *Nandor Knust*
Strafrecht und Gacaca
Entwicklung eines pluralistischen Rechtsmodells am Beispiel des ruandischen Völkermordes
2013 • 423 Seiten • ISBN 978-3-86113-824-2 € 41,00

S 130 *Hans-Georg Koch* (Hrsg.)
Wegsperren?
Freiheitsentziehende Maßnahmen gegen gefährliche, strafrechtlich verantwortliche (Rückfall-)Täter
Internationaler Vergleich – Kriminologische Perspektiven
2011 • 545 Seiten • ISBN 978-3-86113-831-0 € 52,00

Max-Planck-Institut für ausländisches
und internationales Strafrecht

Auswahl aktueller Publikationen aus dem kriminologischen Veröffentlichungsprogramm:

K 166 *Ramin Tehrani*
Die „Smart Sanctions" im Kampf gegen den Terrorismus und als Vorbild einer präventiven Vermögensabschöpfung
Berlin 2014 • 256 Seiten • ISBN 978-3-86113-247-9 € 35,00

K 165 *Daniela Cernko*
Die Umsetzung der CPT-Empfehlungen im deutschen Strafvollzug
Eine Untersuchung über den Einfluss des Europäischen Komitees zur Verhütung von Folter und unmenschlicher oder erniedrigender Behandlung oder Strafe auf die deutsche Strafvollzugsverwaltung
Berlin 2014 • 455 Seiten • ISBN 978-3-86113-246-2 € 39,00

K 164 *Franziska Kunz*
Kriminalität älterer Menschen
Beschreibung und Erklärung auf der Basis von Selbstberichtsdaten
Berlin 2014 • 387 Seiten • ISBN 978-3-86113-244-8 € 35,00

K 163 *David Jensen*
Maras
A study of their origin, international impact, and the measures taken to fight them
Berlin 2013 • 245 Seiten • ISBN 978-3-86113-243-1 € 35,00

K 161 *Gunda Wößner, Roland Hefendehl, Hans-Jörg Albrecht* (Hrsg.)
Sexuelle Gewalt und Sozialtherapie
Bisherige Daten und Analysen zur Längsschnittstudie „Sexualstraftäter in den sozialtherapeutischen Abteilungen des Freistaates Sachsen"
Berlin 2013 • 274 Seiten • ISBN 978-3-86113-241-7 € 35,00

K 159 *Andreas Armborst*
Jihadi Violence
A study of al-Qaeda's media
Berlin 2013 • 266 Seiten • ISBN 978-3-86113-119-9 € 35,00

K 158 *Martin Brandenstein*
Auswirkungen von Hafterfahrungen auf Selbstbild und Identität rechtsextremer jugendlicher Gewalttäter
Berlin 2012 • 335 Seiten • ISBN 978-3-86113-118-2 € 35,00

K 157 *Ghassem Ghassemi*
Criminal Policy in Iran Following the Revolution of 1979
A Comparative Analysis of Criminal Punishment and Sentencing in Iran and Germany
Berlin 2013 • 265 Seiten • ISBN 978-3-86113-116-8 € 35,00

K 156 *Gunther Olt*
Pressefreiheit im Kontext strafrechtlicher Ermittlungsmaßnahmen
Berlin 2013 • 265 Seiten • ISBN 978-3-86113-114-4 € 35,00