DuD-Fachbeiträge

RESEARCH

Antonie Moser-Knierim

Vorratsdatenspeicherung

Zwischen Überwachungsstaat und Terrorabwehr

DuD
Datenschutz und Datensicherheit

Springer Vieweg

DuD-Fachbeiträge

Herausgegeben von
H. Reimer, Erfurt, Deutschland
K. Rihaczek, Bad Homburg v.d. Höhe, Deutschland
A. Roßnagel, Kassel, Deutschland

Die Buchreihe ergänzt die Zeitschrift DuD – Datenschutz und Datensicherheit in einem aktuellen und zukunftsträchtigen Gebiet, das für Wirtschaft, öffentliche Verwaltung und Hochschulen gleichermaßen wichtig ist. Die Thematik verbindet Informatik, Rechts-, Kommunikations- und Wirtschaftswissenschaften.
Den Lesern werden nicht nur fachlich ausgewiesene Beiträge der eigenen Disziplin geboten, sondern sie erhalten auch immer wieder Gelegenheit, Blicke über den fachlichen Zaun zu werfen. So steht die Buchreihe im Dienst eines interdisziplinären Dialogs, der die Kompetenz hinsichtlich eines sicheren und verantwortungsvollen Umgangs mit der Informationstechnik fördern möge.

Herausgegeben von
Prof. Dr. Helmut Reimer
Erfurt

Dr. Karl Rihaczek
Bad Homburg v.d. Höhe

Prof. Dr. Alexander Roßnagel,
Universität Kassel

Antonie Moser-Knierim

Vorratsdaten-speicherung

Zwischen Überwachungsstaat und Terrorabwehr

Springer Vieweg

Antonie Moser-Knierim
Stuttgart, Deutschland

Dissertation Universität Kassel, 2013

ISBN 978-3-658-04155-7 ISBN 978-3-658-04156-4 (eBook)
DOI 10.1007/978-3-658-04156-4

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

Springer Vieweg

Gedruckt auf säurefreiem und chlorfrei gebleichtem Papier

Springer Vieweg ist eine Marke von Springer DE. Springer DE ist Teil der Fachverlagsgruppe Springer Science+Business Media.
www.springer-vieweg.de

Für meine Familie.

Danksagung

Die vorliegende Arbeit „Vorratsdatenspeicherung – zwischen Terrorabwehr und Überwachungsstaat“ wurde von der Universität Kassel als Dissertation angenommen (Fachbereich Wirtschaftswissenschaften (FB 07)). Die Arbeit wurde im November 2012 zur Begutachtung eingereicht. Die Disputation erfolgte am 12. Juni 2013. Änderungen der Sach- und Rechtslage wurden für die Druckfassung bis Juli 2013 berücksichtigt.

Danken möchte ich meinem Doktorvater Prof. Alexander Roßnagel für zahlreiche anregende Diskussionen, die Möglichkeit in der Projektgruppe verfassungsverträgliche Technikgestaltung (provet) mitzuwirken sowie seine umfassende Betreuung. Auch danke ich meiner Zweitgutachterin Prof. Martina Deckert und der Prüfungskommission für das angenehme Prüfungsgespräch.

Gedankt sei auch dem Bundesministerium für Bildung und Forschung für die Förderung des Forschungsprojekts INVODAS. Zudem möchte ich meinem Kollegen Herrn Sebastian Schweda (EMR, Saarbrücken) für die gute Zusammenarbeit im Forschungsprojekt danken.

Mein besonderer Dank gilt meinen ehemaligen KollegInnen und den wissenschaftlichen Hilfskräften bei provet für Rat, Kritik und Unterstützung bei der Dissertation und die gute, gemeinsame Zeit in Kassel. Danken möchte ich Prof. Gerrit Hornung, Dr. Silke Jandt, Dr. Mark Bedner, Carina Boos, Monika Desoi, Christian Geminn, Olga Grigorjew, Dennis Heinson, Maria Henning, Dr. Dennis Hoss, Paul Christopher Johannes, Aliye Kartal-Aydemir, Dr. Phillip Richter, Michaela Schuldt, Thomas Schulz, Hendrik Skistims, Bernd Volland, Dr. Daniel Wilke und Julia Zirfas.

Bedanken möchte ich mich auch bei Dr. Igor Herrmann für Korrekturen und konstruktive Anregungen bei der Fertigstellung des Manuskripts.

Schließlich danke ich ganz herzlich meiner Familie für ihr Vertrauen, ihre Unterstützung und Begleitung auf dem Weg zur Promotion.

Antonie Moser-Knierim

Vorwort des Herausgebers

Gegenstand der Arbeit ist ein für Wirtschaft und Gesellschaft sowie das Verhältnis von Recht und Technik sehr aktuelles und bedeutsames Thema, nämlich die verfassungsrechtliche Bewertung der Vorratsspeicherung von Telekommunikationsverkehrsdaten und die Möglichkeiten ihrer verfassungskonformen Gestaltung. Dieses Thema bietet eine doppelte, gleichermaßen dogmatisch wie methodisch hochrelevante Herausforderung für eine interdisziplinär orientierte Rechtswissenschaft: Zum einen sind die verfassungsrechtlichen Vorgaben für eine die gesamte Gesellschaft umfassende und politisch höchst umstrittene Überwachungsmaßnahme im Verhältnis zu europarechtlichen Vorgaben zu klären. Zum anderen müssen methodisch Wege gefunden werden, wie unter widersprüchlichen rechtlichen Vorgaben Gestaltungsvorschläge entwickelt werden können, die einen optimierten Interessenausgleich bewirken können.

Die Vorratsdatenspeicherung von Telekommunikationsverkehrsdaten wird von vielen als das entscheidende Instrument angesehen, um die Bedrohung durch Terrorismus und sonstige Verbrechen im digitalen Zeitalter abzuwehren. Ihre Einführung wurde 2006 durch eine Richtlinie allen Mitgliedstaaten der Europäischen Union vorgegeben. Da sie ausnahmslos und anlasslos zur Speicherung aller Telekommunikationsverkehrsdaten aller Personen in der Europäischen Union führt, um ihr Telekommunikationsverhalten für Überwachungszwecke nachvollziehen zu können, greift diese Maßnahme tief in Freiheitsrechte ein und hat erbitterten politischen Widerstand hervorgerufen: Durch sie werde Freiheit der Sicherheit geopfert und der entscheidende Schritt in einen „Überwachungsstaat“ getan.

Das Bundesverfassungsgericht hat die Umsetzung in Deutschland, die weit über die Vorgaben der Richtlinie hinausging, in seinem Urteil vom 2. März 2010 für verfassungswidrig erklärt. Allerdings stellte es fest, dass die Vorratsdatenspeicherung „nicht schlechthin verfassungswidrig“ ist, sondern nur die besondere Form der Umsetzung in Deutschland, die auf die Freiheitsrechte der Betroffenen zu wenig Rücksicht genommen hat. Hinsichtlich der Befürchtung, dass die Vorratsdatenspeicherung der entscheidende Schritt in den Überwachungsstaat darstelle, hat es die Feststellung getroffen, dass es verfassungsrechtlich nicht zu rechtfertigen sei, das Verhalten der Bürger total zu erfassen und zu registrieren, und daher eine „umfassende gesellschaftliche Überwachung“ unzulässig sei.

Auch nach dem Urteil des Bundesverfassungsgerichts ist weiterhin die Umsetzung der Vorratsdatenspeicherungs-Richtlinie gefordert. Die Richtlinie befindet sich aber selbst auch in Überarbeitung. Daher stellen sich sowohl für die Richtlinie als auch für ihre Umsetzung in Deutschland zwei Fragen, die in der vorliegenden Arbeit verfolgt werden: Wie kann erstens ein optimierter Interessenausgleich zwischen den Freiheits- und den Sicherheitsinteressen erreicht werden, der die Rahmensetzungen des Bundesverfassungsgerichts berücksichtigt? Kann zweitens durch die Grenzziehung des Bundesverfassungsgerichts gegenüber anlassloser Überwachung der Schritt in einen Überwachungsstaat verhindert werden?

Mit der vorgelegten Arbeit füllt Frau Moser-Knierim zwei wesentliche Lücken im Recht des elektronischen Rechtsverkehrs. Indem sie Möglichkeiten untersucht, wie auf der Grundlage der Entscheidung der Bundesverfassungsgerichts die Ziele der Sicherheitsgewährleistung und des Grundrechtsschutzes hinsichtlich der einzelnen Merkmale der Vorratsdatenspeicherung besser aufeinander abgestimmt werden können, trägt sie zu einem besseren Verständnis der Anforderungen der Sicherheitsgewährleistung und des Grundrechtsschutzes bei, entwickelt hilfreiche Vorschläge zur Gestaltung der Vorratsdatenspeicherung und bietet vor allem wertvolle Hinweise für die Rechtspolitik auf europäischer und deutscher Ebene. Indem sie untersucht, welche Grenzen das Verfassungsrecht einer weiteren Entwicklung zu einem „Überwachungsstaat" entgegensetzt und setzen kann, trägt sie zu einem besseren Verständnis schwieriger grundlegender verfassungsrechtlicher Fragen bei und bietet wichtige rationale Argumente in einer zentralen gesellschaftliche Auseinandersetzung um die Zukunft der Gesellschaft.

Die Arbeit entstand zu großen Teilen im Rahmen der Mitarbeit von Frau Moser-Knierim im Forschungsprojekt „Interessenausgleich im Rahmen der Vorratsdatenspeicherung" (INVODAS), das von 2010 bis 2011 von der Projektgruppe verfassungsverträgliche Technikgestaltung (provet) der Universität Kassel zusammen mit dem Institut für Europäisches Medienrecht (EMR) in Saarbrücken durchgeführt und vom Bundesministerium für Bildung und Forschung gefördert wurde. In diesem konnte Frau Moser-Knierim eigenverantwortlich die verfassungsrechtlichen Fragen der Vorratsdatenspeicherung und der Optimierung des Interessenausgleichs untersuchen.

Mit diesem Buch ergänzt Frau Moser-Knierim die bisher bereits umfangreiche rechtswissenschaftliche Literatur zur Vorratsdatenspeicherung um zwei wesentliche Aspekte. Zum einen ergänzt sie die rechtswissenschaftliche Bewertungsperspektive um eine rechtswissenschaftliche Gestaltungsperspektive und gewinnt aus dieser innovative Gestaltungsvorschläge für die Optimierung des Interessenaugleichs bei der Vorratsdatenspeicherung. Zum anderen erweitert sie die Perspektive von der Vorratsdatenspeicherung als einem Instrument der Überwachung und Ermittlung zur Vorratsdatenspeicherung als einem Schritt in einer fortschreitenden Entwicklung zu immer tiefgreifenderen und umfassenderen präventiven Sicherheitsmaßnahmen. Ihre Suche nach normativen Grenzen dieser Entwicklung führt sie zu wertvollen Erkenntnisse und wichtigen Ergebnissen, die für die politische Diskussion und die weitere rechtswissenschaftliche Forschung sehr hilfreich sind.

Für die weitere politische, forensische und rechtswissenschaftliche Diskussion zur Vorratsdatenspeicherung ist zu hoffen, dass die Entscheidungsträger in Politik, Justiz und Gesellschaft die Hinweise dieser Arbeit zur Kenntnis nehmen und bei ihren Entscheidungen zur Vorratsdatenspeicherung berücksichtigen.

Kassel, im Juli 2013 Alexander Roßnagel

Inhaltsübersicht

Inhaltsverzeichnis

Abkürzungsverzeichnis

a.A.	Andere Ansicht
Abs.	Absatz
AEUV	Vertrag über die Arbeitsweise der europäischen Union
AG	Amtsgericht
Akz.	Abkürzung
ÄndG	Änderungsgesetz
Anm.	Anmerkung
AO	Abgabenordnung
AöR	Archiv des öffentlichen Rechts
APuZ	Aus Politik und Zeitgeschichte
ArbR	Arbeitsrecht
Art.	Artikel
Az.	Aktenzeichen
BB	Betriebsberater
BBK	Bundesamt für Bevölkerungsschutz und Katastrophenhilfe
BDSG	Bundesdatenschutzgesetz
Beschw.	Beschwerde
BfDI	Bundesbeauftragter für den Datenschutz und die Informationsfreiheit
BfV	Bundesamt für Verfassungsschutz
BGBl.	Bundesgesetzblatt
BGHSt	Entscheidungen des Bundesgerichtshofs in Strafsachen
BImSchG	Gesetz zum Schutz vor schädlichen Umwelteinwirkungen durch Luftverunreinigungen, Geräusche, Erschütterungen und ähnliche Vorgänge
Bit	binary digit
BKAG	Gesetz über das Bundeskriminalamt und die Zusammenarbeit des Bundes und der Länder in kriminalpolizeilichen Angelegenheiten
BND	Bundesnachrichtendienst
Bnd.	Band
BPolG	Bundespolizeigesetz
BR-Drs.	Bundesrat Beratungsvorgänge und Drucksachen
BRD	Bundesrepublik Deutschland
BSI	Bundesamt für Sicherheit in der Informationstechnik
bspw.	Beispielsweise
BT-Drs.	Deutscher Bundestag Drucksachen
BtM	Betäubungsmittel
BVerfG	Bundesverfassungsgericht
BVerfGE	Entscheidungen des Bundesverfassungsgerichts
BVerfSch	Bundesverfassungsschutz
BVerwG	Bundesverwaltungsgericht
BVerwGE	Entscheidungen des Bundesverwaltungsgerichts

BvR	Bundesverfassungsrichter
bzw.	Beziehungsweise
CCC	Chaos Computer Club
Cilip	Bürgerrechte & Polizei
CR	Computer und Recht
c't	Magazin für Computertechnik
DANA	Die Datenschutznachrichten
Ders.	Derselbe
Dies.	Dieselbe
DÖV	Die öffentliche Verwaltung
DPolG	Deutsche Polizeigewerkschaft
DRiZ	Deutsche Richterzeitung
DS-GVO-E	Datenschutz-Grundverordnung-Entwurf
DSR	Datenschutzrecht
DuD	Datenschutz und Datensicherheit
DVBl.	Deutsches Verwaltungsblatt
Ebd.	Ebenda
EG	Europäische Gemeinschaft
EGMR	Europäischer Gerichtshof für Menschenrechte
eingef.	Eingeführt
EMRK	Europäische Menschenrechtskonvention
endg.	Endgültig
EnEG	Gesetz zur Einsparung von Energie in Gebäuden
ETSI	European Telecommunications Standards Institute
EU	Europäische Union
Eu Kom.	Europäische Kommission
EuGH	Europäische Gerichtshof
EU-GRCh.	Europäische Grundrechtecharta
EuGRZ	Europäische Grundrechte-Zeitschrift
EuR	Europarecht
EuRhÜbk	Übereinkommen gemäß Artikel 34 des Vertrags über die Europäische Union vom Rat erstellt - Rechtshilfe in Strafsachen zwischen den Mitgliedstaaten der Europäischen Union
Euroatom	Europäische Atomgemeinschaft
EuZW	Europäische Zeitschrift für Wirtschaftsrecht
EWR	Europäischer Wirtschaftsraum
f.	Folgende
ff.	Fortfolgende
FG	Festgabe
FGO	Finanzgerichtsordnung
Fn.	Fußnote
FS	Festschrift
G10	Gesetz zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses
GastG	Gaststättengesetz

GATT	General Agreements on Tariffs and Trades
GbR	Gesellschaft bürgerlichen Rechts
GG	Grundgesetz
Ggf.	Gegebenenfalls
GmbH	Gesellschaft mit beschränkter Haftung
GoBT	Geschäftsordnung des Deutschen Bundestages
GPS	Global Positioning System
GVG	Gerichtsverfassungsgesetz
Hb.	Handbuch
HdK	Handkommentar
hM	Herrschende Meinung
Hrsg.	Herausgeber
Hs.	Halbsatz
HSDPA	High Speed Downlink Packet Access
HSOG	Hessisches Gesetz über die öffentliche Sicherheit und Ordnung
HStR	Handbuch des Staatsrechts
HSUP(A)	High Speed Uplink Packet Access
i.d.F.	in der Form
i.e.S.	im engeren Sinne
i.S.d.	im Sinne des
i.S.v.	im Sinne von
i.V.m.	in Verbindung mit
IfD	Institut für Demoskopie
InPol	Polizeiliches Informationssystem
IP	Internetprotokoll
IPvpR	Internationaler Pakt über bürgerliche und politische Rechte
IStGH	Internationaler Strafgerichgtshof
IWF	Internationaler Währungsfonds
JA	Juristische Arbeitsblätter
JuS	Juristische Schulung
JVEG	Gesetz über die Vergütung von Sachverständigen, Dolmetscherinnen, Dolmetschern, Übersetzerinnen und Übersetzern sowie die Entschädigung von ehrenamtlichen Richterinnen, ehrenamtlichen Richtern, Zeuginnen, Zeugen und Dritten
JZ	Juristen Zeitung
K&R	Kommunikation und Recht
Kap.	Kapitel
Komm.	Kommentar
krit.	Kritisch
KritV	Kritische Vierteljahresschrift für Gesetzgebung und Rechtswissenschaft
LG	Landgericht
LTE	Long Term Evolution
m.	Mit
m.A.	meiner Ansicht

m.w.Nachw.	mit weiteren Nachweisen
m.W.v.	mit Wirkung vom
MAD	Militärischer Abschirmdienst
Mbit	Mega binary digit
MüKO	Münchner Kommentar
Nachw.	Nachweis(e)
NAT	Network Adress Translation
NATO	North Atlantic Treaty Oranization
NJ	Neue Justiz
NJW	Neue Juristische Wochenzeitschrift
NK	Neue Kriminalpolitik
Nr.	Nummer
NStZ	Neue Zeitschrift für Strafrecht
NSU	Nationalsozialistischer Untergrund
NVwZ	Neue Zeitschrift für Verwaltungsrecht
Orig.-Fsg.	Original Fassung
PharmR	Pharma Recht
PlPr.	Plenarprotokoll
PrOVG	Preußisches Oberverwaltungsgericht
Ratsdok.	Ratsdokument
RB	Rahmenbeschluss
RDV	Recht der Datenverarbeitung
RL	Richtlinie
Rn.	Randnummer
Rs.	Rechtssache
Rspr	Rechtsprechung
s.	Siehe
S.	Seite
SDÜ	Schengener Durchführungsübereinkommen
StGB	Strafgesetzbuch
Stopp	Strafprozessordnung
Strg.	Strittig
stRspr	ständige Rechtsprechung
StV	Strafverteidiger
Taz	Die Tageszeitung
teilw.	Teilweise
TK	Telekommunikation
TKG	Telekommunikationsgesetz
u.	Und
u. a.	unter anderem
UMTS	Universal Mobile Telecommunications System
UrhG	Gesetz über Urheberrecht und andere Schutzrechte
UrhR	Urheberrecht
Urt.	Urteil
v.	Vom

VBlBW	Verwaltungsblätter für Baden-Württemberg
VDS	Vorratsdatenspeicherung
VDS-RL	Vorratsdatenspeicherungsrichtlinie
Verw.	Verweis
VerwArch	Verwaltungsarchiv
VG	Verwaltungsgericht
vgl.	Vergleiche
VN-Ch.	Charta der Vereinten Nationen
Vorb.	Vorbemerkung
VVDStRL	Vereinigung der deutschen Strafrechtslehrer
WTO	World Trade Organisation
WWW	World Wide Web
z.B.	zum Beispiel
ZaöRV	Zeitschrift für ausländisches öffentliches Recht und Völkerrecht
ZD	Zeitschrift für Datenschutz
ZfS	Zeitschrift für Soziologie
Ziff.	Ziffer
ZIS	Zeitschrift für Informationsrechtspolitik
ZP	Zeitschrift für Politik
ZRP	Zeitschrift für Recht und Politik
ZStW	Zeitschrift für die gesamte Strafrechtswissenschaft
ZUM	Zeitschrift für Urheber und Medienrecht

Hinweis zum Gender Mainstreaming

Zur leichteren Lesbarkeit der Texte wurde vielfach nur die männliche Form personenbezogener Hauptwörter gewählt, womit jedoch keine Benachteiligung des weiblichen Geschlechts beabsichtigt ist.

Einführung

Im Jahr 2013 wurde mit dem NSA-Skandal die Diskussion um das Verhältnis zwischen Freiheit und Sicherheit im digitalen Zeitalter neu entfacht. Im Angesicht der umfassenden Datenerhebungen und -auswertungen, welche durch die National Security Agency scheinbar durchgeführt werden, scheint die Diskussion um die Speicherung der Telekommunikationsverkehrsdaten auf Vorrat, wie sie in Deutschland und Europa geführt wird, geradezu lächerlich. Denn dabei werden nicht sämtliche Inhalte digitaler Kommunikation erfasst (wie wohl im Zuge von PRISM), sondern es werden lediglich Telekommunikationsverkehrsdaten auf Vorrat erhoben. Es wird damit lediglich das Wer, Wie, Was, Wann und Wo einer jeden digitalen Kommunikation von der Vorratsdatenspeicherung erfasst.

Doch sowohl die Datenspeicherungspraxis der amerikanischen und britischen Geheimdienste als auch die Vorratsdatenspeicherung bewegen sich im Spannungsfeld zwischen Terrorabwehr und Überwachungsstaat. Sie wecken die Frage, wieviel Sicherheit verträgt die Freiheit?

Insofern hofft die Autorin, dass sie mit der hier vorgelegten Untersuchung, wie denn Freiheit und Sicherheit im digitalen Zeitalter in Einklang gebracht werden können, auch einen Beitrag zur Diskussion um PRISM, Keysource und sonstige Praktiken von Geheimdiensten leisten kann. Auch wenn sich die Arbeit selbst nicht mit konkreten Fragen zum NSA-Skandal befasst.

Im Fokus dieser Untersuchung steht die Frage, ob und wie Freiheits- und Sicherheitsinteressen bei einer Vorratsdatenspeicherung in Einklang gebracht werden können. Wesentlicher Bestandteil der Arbeit ist die Untersuchung der Frage, wie das Verhältnis von Freiheit und Sicherheit im Grundgesetz festgelegt ist und inwieweit die Identität der Verfassung auch eine freiheitliche Gesellschaftsordnung garantiert, die es auch bei der Einführung sicherheitspolitischer Instrumente zu wahren gilt.

Um die Vorratsdatenspeicherung(-srichtlinie) selbst wurde von Anfang an heftig gestritten. Aktuell verhandelt der *Europäische Gerichtshof* über zwei Klagen Österreichs und Irlands. Er befasst sich mit der auch in der Wissenschaft umstrittenen Frage, ob die Richtlinie mit der europäischen Grundrechtecharta vereinbar ist. Wie der Gerichtshof entscheiden wird, ist zum jetzigen Zeitpunkt (Juli 2013) nicht absehbar. Doch die Frage nach der Vereinbarkeit der Richtlinie mit europäischen Grundrechten ist auch nicht leitend für die hier vorgelegte Studie. Vielmehr wurde untersucht, wie das deutsche nationale Verfassungsrecht es vermag, Freiheit und Sicherheit zu schützen.

Denn die Vorratsdatenspeicherung fordert das Verfassungsrecht heraus: handelt es sich um verfassungskonforme und erforderliche Terrorabwehr oder um den Schritt in den Überwachungsstaat?

Diese Frage stellte sich besonders dringlich nach dem Urteil des Bundesverfassungsgerichts vom 2. März 2010, in dessen Folge diese Arbeit entstanden ist. Denn das Ge-

richt hatte festgestellt, dass eine Vorratsdatenspeicherung nicht schlechthin verfassungswidrig sei. Bis dahin war diese in der Wissenschaft überwiegend als verfassungswidrig beurteilt worden. Nach dem Urteil wurde insofern die Frage, ob und wie durch das Grundgesetz ein Ausgleich zwischen Freiheit und Sicherheit erzielt wird, der den Herausforderungen des 21. Jahrhunderts gerecht wird, neu aufgeworfen.

Freiheit und Sicherheit werden vielfach als Antipoden begriffen und so wird in der aktuellen Diskussion vielfach gefragt, ob es nicht mittlerweile „Sicherheit statt Freiheit" heißt.[1] Auf die terroristischen Anschläge von New York, Madrid und London reagierte die Politik mit der Ausweitung polizeilicher und nachrichtendienstlicher Befugnisse und der Einführung neuer Sicherheitsinstrumente.[2] Ins Zentrum der Debatte rückte die Abwehr von Gefahren durch den internationalen Terrorismus, und zwar durch eine Ausweitung der gesamtgesellschaftlichen Überwachung. Die Erfassung und Auswertung großer Mengen personenbezogener Daten soll es ermöglichen, zukünftig Anschläge zu verhindern. Sicherheit durch Prävention wird so zum innenpolitischen Dogma, welches in Deutschland seit Bekanntwerden der amerikanischen Überwachungspraxis nun erstmals wieder generell in Frage gestellt wird.

Die Befürchtung des ehemaligen Verfassungsrichters *Grimm*: „Im Kampf gegen den Terrorismus läuft der Staat Gefahr, die Freiheit der Sicherheit zu opfern"[3] scheint berechtigt. Nicht erst im Hinblick auf die nun bekannt gewordenen Spähprogramme, hat sich in der Gesellschaft die Besorgnis breit gemacht, dass sich der Verfassungsstaat als Reaktion auf die terroristische Bedrohung in einen Überwachungs- oder Präventionsstaat verwandelt.[4] Diese Diskussion wird in der Rechts- und Politikwissenschaft seit geraumer Zeit geführt. Auch wenn die Informationen über das Ausmaß der Überwachungsprogramme neu sind, ist seit langem bekannt, dass mit der voranschreitenden Digitalisierung nunmehr die Technologien verfügbar sind, um das Szenario eines totalen Überwachungsstaats zu realisieren.[5]

Fakt ist, dass sich das Spannungsverhältnis von Freiheit und Sicherheit durch digitale Datenverarbeitung, Technisierung[6], Globalisierung und neue Gefährdungslagen ver-

---

1 So Titel und Thema der Dissertation von *Hornig* 2009; so titeln auch *Adick,* WDR, Quarks & Co v. 2.3.2010, abrufbar unter: http://www.wdr.de/tv/quarks/sendungsbeitraege/2010/0309/004_sicherheit.jsp; *Biermann,* ZEIT online v. 27.5.2007, abrufbar unter: http://www.zeit.de/online/2007/21/Amnesty; *Hausar* telepolis v. 14.6.2009, abrufbar unter: http://www.zeit.de/online/2007/21/Amnesty.

2 Großer Lauschangriff, Onlinedurchsuchungen, Vorratsdatenspeicherung nur als Stichworte; zu den zahlreichen Sicherheitsgesetzen seit 9/11 ausführlich etwa *Albrecht* 2010a, Teil. 3; *Rzepka* 2009, 13 ff.

3 *Grimm,* „Aus der Balance", Die ZEIT v. 29.11.2007, abrufbar unter: *http://www.zeit.de/2007/49/Schaeuble-Antwort.*

4 *Hirsch*, DUD 2008, 87, 89; *Albrecht* 2010b; *Huster/Rudolph* 2008; *Prantl* 2008; *Zeh/Trojanow* 2009; dazu kritisch *Bull* 2011, 18.

5 *Roßnagel*, DUD 2010, 544, 546; *ders*. Informatik-Spektrum 2005, 467.

6 Bereits Ende der 1980er Jahre wurde festgestellt, dass „die Möglichkeiten der automatischen Datenverarbeitung den Grundkonflikt zwischen Effektivität polizeilichen Handelns und dem Schutz von Freiheitsgrundrechten" verschärfen und auf eine neue informationelle Ebene heben würden; *Pordesch,* in: *Roßnagel* 1989, 89.

schärft hat. Angesicht dieser Entwicklungen stellt sich die Frage, ob das Verfassungsrecht noch in der Lage ist, einen Ausgleich zwischen den widerstreitenden Interessen zu erzeugen. Dies gilt besondere, da das nationale Recht vielfach durch internationales (insbesondere europäisches) Recht überlagert wird.

Mit diesen Entwicklungen steht die verfassungsrechtliche Gewährleistung von Freiheit und Sicherheit vor neuen Herausforderungen. Paradigmatisch dafür steht die Vorratsdatenspeicherung, die im Jahr 2006 europaweit eingeführt wurde[7]. Bei ihr handelt sich um eine anlasslose Überwachungsmaßnahme, die in die in der Informationsgesellschaft zentrale Telekommunikationsinfrastruktur eingreift und von der jeder Bürger betroffen ist. Es verwundert daher nicht, dass der Widerstreit zwischen Freiheit und Sicherheit in der Diskussion um die Vorratsdatenspeicherung einen ersten Höhepunkt gefunden hat – und nun mit Blick auf PRISM, Keysource, etc. einen weiteren Höhepunkt findet. Und gerade für die Diskussion um diese Überwachungsprogramme können die rechtwissenschaftlichen Erwägungen, welche die Vorratsdatenspeicherung betreffen, fruchtbar gemacht werden.

Das *Bundesverfassungsgericht* hat in seinem Urteil aus dem Jahr 2010 festgestellt, dass eine Vorratsdatenspeicherung, wie sie die Richtlinie verlangt, „nicht schlechthin" verfassungswidrig ist.[8] Jedoch nur, wenn die hohen Anforderungen, die sich aus dem Verhältnismäßigkeitsgrundsatz ergeben, berücksichtigt werden. Die Voraussetzungen, die das Gericht für eine verfassungskonforme Ausgestaltung der Vorratsdatenspeicherung formuliert, sind zum Teil sehr konkret. Manch einer war gar der Ansicht, dass man das Urteil direkt abschreiben und in Gesetzesform gießen könne. Dass dem nicht so ist, wird gerade im Hinblick auf die aktuellen Entwicklungen deutlich: so hat das Gericht zwar festgestellt, dass die „Die Freiheitswahrnehmung der Bürger (…) nicht total erfasst und registriert werden" dürfe. Dies gehöre „zur verfassungsrechtlichen Identität der Bundesrepublik Deutschland für deren Wahrung sich die Bundesrepublik in europäischen und internationalen Zusammenhängen einsetzen muss."[9] Was dies für die Umsetzung der Richtlinie konkret bedeutet hat das Gericht jedoch nicht aufgezeigt. Die Frage, was aus dem Verbot einer totalen Erfassung und Registrierung er Freiheitswahrnehmung der Bürger resultiert, ist aber sehr bedeutsam. Dies zeigt sich gerade mit auf den NSA-Skandal.

Denn auf der anderen Seite, hat das *Bundesverfassungsgericht* nicht nur diese scheinbar absolute Grenze formuliert, es hat auch festgestellt, dass eine verfassungskonforme Umsetzung der Richtlinie möglich sei. Dies war bis dahin in der Wissenschaft überwiegend bezweifelt worden.

Das *Bundesverfassungsgericht* vertritt die Ansicht, dass die Vorratsdatenspeicherung legitimen Zwecken diene und als Reaktion auf das spezifische Gefahrenpotenzial der Telekommunikation grundsätzlich rechtfertigungsfähig sei. Denn die Telekommunikation erleichtert, so das *Bundesverfassungsgericht,* die „verdeckte Kommunikation und

---

7 Die Richtlinie 2006/24/EG v. 13.4.2006 wurde vom *Europäischen Parlament* und vom *Rat* am 15. März 2006 verabschiedet und trat zum 3. Mai 2006 in Kraft; ABl. EU Nr. L 105 S. 54–60

8 BVerfGE 125, 260.

9 BVerfGE 125, 260 (324).

Aktion von Straftätern“. Dadurch wird „eine Bündelung von Wissen, Handlungsbereitschaft und krimineller Energie möglich, die die Gefahrenabwehr und Strafverfolgung vor neuartige Aufgaben stellt“. Die Möglichkeit zur Rekonstruktion der Telekommunikationsverbindungen ist dementsprechend „für eine effektive Strafverfolgung und Gefahrenabwehr von besonderer Bedeutung“.[10]

Es zeigt sich, dass das Gericht sich bemüht die Bedeutung der Vorratsdatenspeicherung sowohl für die Freiheit als auch für die Sicherheit zu berücksichtigen. Es betont, dass ein verfassungskonformer Ausgleich möglich ist. Allerdings nur unter Beachtung strenger Anforderungen. Denn, dies wird darin deutlich, die Vorratsdatenspeicherung bewegt sich an der Grenze zur Verfassungswidrigkeit.

Im Hinblick auf die aktuell bestehende Umsetzungspflicht ist eine Auseinandersetzung mit der Frage geboten, wie ein optimierter Ausgleich der bei der Vorratsdatenspeicherung kollidierenden Freiheits- und Sicherheitsinteressen erreicht werden kann. Denn Deutschland ist europarechtlich zur Umsetzung der Vorratsdatenspeicherungsrichtlinie verpflichtet, und die Europäische Kommission hat Klage gegen Deutschland wegen fehlender Umsetzung der Vorratsdatenspeicherungsrichtlinie erhoben.[11]

Zwar wird die Frage, ob die Europäische Vorratsdatenspeicherungsrichtlinie mit den Europäischen Grundrechten vereinbar ist, derzeit vor dem *Europäischen Gerichtshof* ausgefochten, sodass sich wohl begründet argumentieren lässt, dass bis diese Frage geklärt ist, auch keine Umsetzung in nationales Recht erfolgen sollte. Auf der anderen Seite hat der *Europäische Gerichtshof* trotz der anhängigen Verfahren bislang nicht davor zurück geschreckt, Staaten zu verurteilen, die der Umsetzungspflicht bislang nicht nachgekommen waren. Zuletzt wurde im Mai 2013 Schweden wegen verspäteter Umsetzung zu einer Millionenstrafe verurteilt. Das *Bundesverfassungsgericht* selbst hat die Frage, ob die Richtlinie mit europäischen Grundrechten vereinbar sei, nicht für entscheidungserheblich gehalten und sie insofern auch nicht vorgelegt. Denn, so betont es das Gericht, eine verfassungskonforme Umsetzung der Richtlinie sei möglich. Selbst wenn der *Europäische Gerichtshof* die Richtlinie in ihrer aktuellen Form als europarechtswidrig erachten sollte, wird sich die Diskussion um die Speicherung sämtlicher Telekommunikationsverkehrsdaten auf Vorrat nicht zwingend erledigen. Insoweit stellt sich die Frage auch über die konkrete Fassung der Richtlinie hinaus, ob und wie eine verfassungsverträgliche Speicherung der Telekommunikationsverkehrsdaten auf Vorrat gelingen kann.

Das *Bundesverfassungsgericht* hat in seiner Entscheidung zwar aufgezeigt, was beachtet werden muss, um eine verhältnismäßige Umsetzung der Vorratsdatenspeicherung zu erreichen. Offen ist hingegen, wie die Vorratsdatenspeicherung gestaltet werden kann, dass sie nicht nur „nicht schlechthin verfassungswidrig ist“, sondern wie die kollidierenden Freiheits- und Sicherheitsinteressen in einen bestmöglichen Ausgleich gebracht werden.

---

[10] BVerfGE 125, 260 (322 f.).

[11] *Briegleb,* heise online v. 22.3.2012, „Brüssel stellt Berlin Ultimatum bei der Vorratsdatenspeicherung“, abrufbar unter: http://heise.de/-1478520.

Dafür ist es wichtig, Antworten auf die Frage zu finden, wie gewährleistet werden kann, dass die Vorratsdatenspeicherung nicht als Schritt in den Überwachungsstaat zu werten ist, wie es Kritiker befürchten. Was verbirgt sich hinter dem Verbot, die Freiheitswahrnehmung der Bürger total zu erfassen und zu registrieren, welches das *Bundesverfassungsgericht* im Urteil formuliert hatte.

Die vorliegende Arbeit gliedert sich in drei Teile.

Im ersten Teil werden die Herausforderungen detailliert beleuchtet, die sich an die Gewährleistung von „Freiheit und Sicherheit im digitalen Zeitalter" stellen. Es wird gefragt: Wie wirken sich Digitalisierung und Globalisierung auf die Verwirklichungsbedingungen von Freiheit und Sicherheit aus? Welche Rolle spielt die Bedrohung durch den internationalen Terrorismus? Inwiefern wurden sicherheitspolitische Instrumente ausweitet?

Anknüpfend an die Analyse der technischen, gesellschaftlichen und politischen Entwicklungen folgt die Untersuchung der verfassungsrechtlichen Garantie von Freiheit und Sicherheit. Inwiefern schützt das Grundgesetz Freiheit und Sicherheit?

Schließlich wird untersucht, wie im Verfassungsrecht und in der Rechtsprechung des *Bundesverfassungsgerichts* ein Ausgleich zwischen Freiheits- und Sicherheitsinteressen gefunden werden kann. Wann liegt ein im Sinne des Grundgesetzes optimaler Ausgleich zwischen Freiheits- und Sicherheitsinteressen vor? Dabei werden die Vorratsdatenspeicherung und das Urteil des *Bundesverfassungsgerichts* vom 2.März 2010 zunächst nicht miteinbezogen. Es werden also die gesellschaftlichen und rechtlichen Rahmenbedingungen beschrieben, zur Zeit als die Vorratsdatenspeicherung eingeführt wurde, während der Fokus auf dieser erst im zweiten Teil der Arbeit liegt.

Entsprechend wird im zweiten Teil der Arbeit „die Vorratsdatenspeicherung und das Verbot umfassender gesamtgesellschaftlicher Überwachung" in das Zentrum der Untersuchung gestellt. Nach einer Darstellung der Vorratsdatenspeicherung, der sie prägenden Begriffe, ihrer Einführungsgeschichte, einer Analyse des Urteils und der aktuellen politischen Diskussion, wird erörtert, inwieweit das *Bundesverfassungsgericht* mit der Formulierung des Verbots, die Freiheit der Bürger total zu erfassen und zu registrieren, die schleichende Ausweitung staatlicher Sicherheitsmaßnahmen begrenzt hat. Was verbirgt sich hinter dieser absolut klingenden Schranken-Schranke? In der Literatur wird daraus gefolgert, dass zukünftig eine Überwachungs-Gesamtrechnung durchzuführen sei.[12] Dieser Ansatz wird im Hinblick auf seine verfassungsrechtlichen Grundlagen und im Hinblick auf seine Operationalisierbarkeit untersucht.

Abschließend wird dann im dritten Teil der Arbeit konkret der Frage nachgegangen, wie ein bestmöglicher „Interessenausglich im Rahmen der Vorratsdatenspeicherung" erreicht werden kann.[13] Dafür werden die in den beiden ersten Untersuchungsabschnit-

[12] *Roßnagel*, NJW 2010, 1238, 1240; *Ders.,* DUD 2010, 544; dazu auch *Hornung*/*Schnabel*, DVBl. 2010, 824; *Knierim*, ZD 2011, 17.

[13] Die hier dargestellte Untersuchung wurde im Zuge der Mitarbeit im Forschungsprojekt INVODAS (Interessenausgleich im Rahmen der Vorratsdatenspeicherung) entwickelt. Dieses wurde von 2010 bis 2011 an der Universität Kassel unter der Leitung von Prof. Roßnagel und in enger Zusammen-

ten gewonnen Erkenntnisse analysiert. Insbesondere werden die Untersuchungsergebnisse aus Teil 1, wie ein optimierter Ausgleich bei der Kollision von Freiheits- und Sicherheitsinteressen erreicht werden kann, mit den Erkenntnissen über die Überwachungs-Gesamtrechnung (Teil 2) verbunden und konkret auf die Entwicklung von Gestaltungsvorschlägen für eine verfassungsverträgliche Vorratsdatenspeicherung angewendet.[14]

Im Fokus steht die Frage, wie die Vorratsdatenspeicherung so ausgestaltet werden kann, dass sämtliche betroffenen Interessen in einen möglichst schonenden Ausgleich zueinander gebracht werden, ob die Vorratsdatenspeicherung verfassungsverträgliches Sicherheitsinstrument sein kann.

Dabei beschränkt sich die Untersuchung nicht allein auf die Umsetzung der Vorgaben der Vorratsdatenspeicherungsrichtlinie, denn auch die Richtlinie wird aktuell überarbeitet. Es wird vielmehr auch grundsätzlich erwogen, ob es überhaupt möglich ist, einen im Sinne des Grundgesetzes optimalen Interessenausgleich im Rahmen einer Speicherung der Telekommunikationsverkehrsdaten aller Bürger auf Vorrat zu erzeugen.

Über die Vorratsdatenspeicherung hinaus versucht diese Arbeit einen Beitrag leisten für die Entwicklung verfassungsverträglicher Gestaltungen anderer Sicherheitsinstrumente. Wie kann die Kollision von Freiheits- und Sicherheitsinteressen so aufgelöst werden, dass sich diese verfassungsrechtlich geschützten Interessen nicht gegenseitig ausschließen? Wie können Freiheit und Sicherheit in einen verfassungsverträglichen Ausgleich gebracht werden?

---

arbeit mit dem Institutt für Europäisches Medienrecht (EMR, Saarbrücken) durchgeführt. Ermöglicht wurde das Projekt durch eine Förderung des Bundesministeriums für Bildung und Forschung. Die Forschungsergebnisse werden insgesamt präsentiert in *Roßnagel/Moser-Knierim/Schweda,* 2013.

[14] Das Merkmal der Verfassungsverträglichkeit geht auf *Roßnagel* zurück, der ein Konzept verfassungsverträglicher Technikgestaltung verfolgt. Um sowohl Techniknutzung als Verfassungskonformität im Hinblick auf zukünftige Entwicklungen zu ermöglichen, sollen Verfassungsanforderungen möglichst in die Technikgestaltung implementiert werden. Dabei sollen möglichst schonende Gestaltungen entwickelt werden, dazu grundlegend *Roßnagel* 1989, 177, 181 f.

Teil 1: Freiheit und Sicherheit im digitalen Zeitalter

Neue Bedrohungslagen, eine globalisierte Welt und eine stetig fortschreitende Digitalisierung stellen große Herausforderungen an die Gewährleistung von Freiheit und Sicherheit. Die Herstellung eines möglichst optimalen Ausgleichs zwischen dem Bedürfnis nach kollektiver Sicherheit und der Wahrung individueller Freiheit stellt sich mit neuer Brisanz.[15] Der Diskurs um das Verhältnis von Freiheit und Sicherheit ist im 21. Jahrhundert mit großer Wucht entflammt. In ihm spiegeln sich sowohl gesellschaftspolitische Entwicklungen als auch ein Wandel des Gemeinwesens.[16] Das Verhältnis von Freiheit und Sicherheit ist nicht rein durch die verfassungsrechtlichen Vorgaben, sondern wesentlich durch die gesellschaftlichen Rahmenbedingungen, geprägt.

Die veränderten Verwirklichungsbedingungen sind geeignet die verfassungsrechtlichen Vorgaben in Frage zu stellen: wie können unter den Bedingungen digitaler Datenverarbeitung und unter dem Druck terroristischer Bedrohungslagen Freiheit und Sicherheit gewährleistet werden?

Wesentlich ist daher für eine rechtswissenschaftliche Untersuchung zunächst die gesellschaftlichen Verwirklichungsbedingungen zu erfassen (Kap. 1) um sie dann in Kontext zu den verfassungsrechtlichen Vorgaben, die in rechtlicher Hinsicht das Verhältnis von Freiheit und Sicherheit beschreiben, zu stellen (Kap. **2**). Denn auch wenn sich gesellschaftliche Rahmenbedingungen ändern, kann es in einer „freiheitlich demokratischen Grundordnung“ nicht heißen, Freiheit oder Sicherheit. Ziel sollte sein, diese beiden legitimen Interessen miteinander in Einklang zu bringen. Wie dies nach den Vorgaben der Verfassung zu erfolgen hat, ist eine Frage, die es im Anschluss zu untersuchen gilt (Kap. **3**).

[15] *Zöller* 2003, 291, 318.
[16] *Ronellenfitsch/Wehrmann* 2008, 7.

1 Verwirklichungsbedingungen von Freiheit und Sicherheit im digitalen Zeitalter

Die Gesellschaft zu Beginn des 21. Jahrhunderts wird als Informations- oder Wissensgesellschaft bezeichnet. Geprägt ist sie wesentlich durch Globalisierung und Digitalisierung.

Digitalisierung bezeichnet das Umsetzen analoger Formate und Verfahren in digitale Formate und Verfahren. Dabei werden die vorhandenen Informationen in Binärcode zur elektronischen Datenverarbeitung überführt.[17] Globalisierung beschreibt die im 20 Jahrhundert konstant wachsende weltweite Verflechtung von Wirtschaft, Politik, gesellschaftlichem Leben, Kultur und Kommunikation. Diese wurde letztlich erst durch die „digitale Revolution" ermöglicht.[18] Denn die weltweite Vernetzung, für die der Begriff Globalisierung steht, wäre ohne den technischen Fortschritt, insbesondere im Bereich der Kommunikations- und Transporttechniken nicht möglich gewesen.

Heute wird über alle Grenzen hinweg kommuniziert, gehandelt, gereist und gelebt. Die Globalisierung ist in unserem Alltag angekommen. Große Unternehmen verfügen über Abteilungen, die über die Welt verstreut sind – und wenige sehr große Unternehmen prägen nicht nur die digitale Wirtschaft, sondern auch das gesamtgesellschaftliche Zusammenleben.[19]

Dabei ist die Telekommunikation zur Grundlage unseres Wirtschafts- und Gesellschaftslebens geworden.

Unmittelbare Kommunikation ist zeit- und kostenintensiver und häufig überhaupt nicht machbar, da die Entfernungen viel zu groß sind. So finden heute Konferenzen auch ohne die physische Anwesenheit der Teilnehmer statt – der digitale, satellitengestützte Bildaustausch ermöglicht es. Die Weiterentwicklung und Verbreitung der Telekommunikationstechnologie ist Folge der Digitalisierung der Gesellschaft und ist Grundlage der Globalisierung. Sowohl bei der Digitalisierung der Gesellschaft als auch bei der Globalisierung handelt es sich um gesellschaftliche Rahmenbedingungen, die für die Bestimmung der Begriffe Freiheit und Sicherheit von großer Bedeutung sind. Denn Freiheit und Sicherheit realisieren sich zu Beginn des 21. Jahrhunderts genau unter diesen gesellschaftlichen Rahmenbedingungen. Es geht insofern um die Ge-

---

17 *Ernst,* in: *Hoeren/Sieber* MMR 2012, Teil 7.1 Rn. 50.

18 Und wurde durch die politischen Entscheidungen zur Liberalisierung des Weltmarktes, die zu einer Senkung der Zölle führten, befördert, wie die Gründung der WTO, die Verabschiedung der GATT-Abkommen, die Bildung des IWF etc. (weitere Nachweise dazu in Fn. **231**) . Ausführlich zu deren Rolle in der Globalisierung, *Morasch/Bartholomae* 2011,286 ff.; eine zentrale Rolle spielen darüber hinaus sinkende Energiepreise und Transportkosten, dazu sind ausführliche Informationen abrufbar unter http://www.bpb.de/wissen/3R6PN0,0,0,Voraussetzungen.html ; vgl. dazu auch ausführlichen unten Kap. 1.3.

19 Zu nennen sind hier insbesondere Facebook, Google, Apple und Microsoft. Zur wirtschaftlichen und damit auch gesellschaftlichen Übermacht dieser Unternehmen ausführlich *Kurz/Rieger* 2011, 13 ff., 87 ff.

A. Moser-Knierim, *Vorratsdatenspeicherung,* DuD-Fachbeiträge,
DOI 10.1007/978-3-658-04156-4_1, © Springer Fachmedien Wiesbaden 2014

währleistung von Freiheit und Sicherheit in einer digitalisierten und globalisierten Welt.

Ein dritter wesentlicher Aspekt, der die Verwirklichungsbedingungen von Freiheit und Sicherheit im digitalen Zeitalter prägt, ist die Veränderung der Bedrohungslagen. Durch die weltweite Vernetzung, die technische Abhängigkeit von Wirtschaft und Gesellschaft und die immense Steigerung an verfügbaren Informationen haben sich die Angriffsmöglichkeiten immens gesteigert. Zeitgleich ist eine zunehmende „Versicherheitlichung" zu beobachten. Zu dieser gehören neue Sicherheitsstrategien und dabei auch neue Instrumente zur proaktiven Bekämpfung von Straftaten.

All dies sind Faktoren, welche die Verwirklichungsbedingungen von Freiheit und Sicherheit heute beeinflussen. Berechtigt ist daher die Frage, inwiefern sie jeweils konkret neue Herausforderungen für die verfassungsrechtliche Gewährleistung von Freiheit und Sicherheit verursacht haben. Dem soll im Folgenden nachgegangen werden, indem die Entwicklungen der Informationsgesellschaft (Kap. **1.2**), der Globalisierung (Kap. **1.3**) dargestellt und schließlich die politischen Entscheidungen, die zu einer Ausweitung der Sicherheitsvorsorge geführt haben, nachgezeichnet werden (Kap. **1.4**). Abschließend wird dargestellt, inwiefern diese Veränderungen die Verwirklichungsbedingungen von Freiheit und Sicherheit im 21. Jahrhundert prägen (Kap. **1.5**). Doch bevor die veränderten gesellschaftlichen Rahmenbedingungen betrachtet werden, sind die Begriffe Freiheit und Sicherheit näher zu konkretisieren – und zwar sowohl in Hinsicht auf ihre intensionale als auch ihre staatstheoretische Bedeutung (Kap. 1.1). Sie werden hier auch rechtsdogmatisch und rechtsphilosophisch begründet.

1.1 Freiheit und Sicherheit – zwei schillernde Begriffe

Für die Untersuchung der Fragen, ob mit der Vorratsdatenspeicherung der Weg in eine Überwachungsgesellschaft geebnet wurde oder ob sie unentbehrliches Sicherheitsinstrument ist, ist es zunächst erforderlich überhaupt die Begriffe Freiheit und Sicherheit näher zu bestimmen. Denn sie sind für die Untersuchung von besonderer Bedeutung, da es darum geht zu klären, ob mit der Vorratsdatenspeicherung eine Gesellschaft, die Sicherheit über alles stellt, errichtet wird oder ob eine freiheitliche Gesellschaftsordnung erhalten bleibt. Es sind insofern die abstrakten Begriffe Freiheit und Sicherheit, die die vorliegende Untersuchung wesentlich prägen. Daher kann die Untersuchung nicht ohne eine nähere Bestimmung dieser beiden, so vagen Begriffe auskommen.

Es werden im Folgenden zunächst die Begriffe Freiheit und Sicherheit dargestellt, bevor ihre rechtliche Bedeutung mit Blick auf Rechtsgeschichte und Rechtsphilosophie erörtert wird, um sich der inhaltlichen, verfassungsrechtlichen Bestimmung der Begriffe anzunähern. Dies soll hier unter Rückgriff auf eine umfassende Untersuchung durch das Institut für Demoskopie Allensbach mit dem Titel „Der Wert der Freiheit" erfolgen.[20] Nach dieser kann abstrakt unterschieden werden zwischen Freiheit von Belastungen und Beschränkungen und der Freiheit zu etwas. Wobei letztlich jede Art von Freiheit zugleich eine Freiheit von etwas und eine Freiheit zu etwas begründet. Ein

[20] „Der Wert der Freiheit", *IfD Allensbach* 2003.

besseres Begriffsverständnis ermöglicht eine Analyse der verschiedenen Dimensionen der Freiheit.[21]

Historisch am weitesten zurück reicht die Bedeutung von Freiheit als Gegensatz zu Knechtschaft und Fremdbestimmung. Freiheit also im Sinne von Freiheit vor Willkür und Sklaverei.[22] Auch das lateinische Libertas hat diese Hauptbedeutung.[23] Ebenso war dies der Sinn des gotischen „Freihals", aus dessen Wortstamm sich das Wort Freiheit entwickelt hat.[24] Es wird daher angenommen, dass sich andere Bedeutungen des Begriffs Freiheit erst aus diesem juristischen Gehalt des Wortes heraus entwickelt haben.[25] Freiheit in diesem Sinne meint die Freiheit *von* staatlicher (und anderweitiger) Bevormundung und *zu* selbstbestimmtem Handeln und Entscheiden.

Daneben kommt Freiheit die Bedeutung zu, zu tun und zu lassen, was man will. Also im Sinne einer moralischen Freizügigkeit, als Zügellosigkeit auch entgegen gesellschaftlicher und rechtlicher Normen. Diese Freiheit wird auch als Libertinage bezeichnet. Freiheit in diesem Sinne meint die Freiheit *von* Normen und Zwängen und *zu* einem ungezwungenen Leben.[26]

Schließlich wird Freiheit zum Teil auch verstanden als Freiheit von Not, Armut, Arbeitslosigkeit und sonstigen Risiken des Lebens. In diesem Sinne wird Freiheit als etwas erkannt das durch einen starken Staat gewährt wird.[27] Es ist die Freiheit *von* Sorgen und Not oder anders formuliert, die Freiheit *zu* einem sorgenfreien privaten Leben.

Politisch ist Freiheit als Möglichkeit der Bürger anerkannt, sich ungehindert am öffentlichen Leben zu beteiligen, insbesondere seine Meinung frei zu äußern. Politische Freiheit ist also die Freiheit *von* staatlichen Zwängen und *zu* einer politischen Beteiligung.[28]

Sozialwissenschaftlich wird Freiheit betrachtet als die Möglichkeit des Einzelnen, sein Leben selbst zu bestimmen: es in diesem Sinne selbst zu gestalten und sich selbst zu verwirklichen.[29] Wesentlich dafür sind, die Freiheit zur Selbstdarstellung und damit auch die kommunikative Freiheit.[30] Gefordert wird vom Einzelnen zur Verwirklichung von Freiheit in diesem Sinne ein aktives Handeln.

---

21 *IfD Allensbach* 2003, 17 ff.
22 Bereits 3000 v. Chr. ist diese Deutung bei den Sumerern zu finden, vgl. Fn. 21.
23 http://de.pons.eu/latein-deutsch/libertas: Libertas als die „bürgerliche Freiheit".
24 Nach dem Wörterbuch der Gebrüder Grimm, bezeichnet „Freihals" den Hals, der kein Joch tragen muss (zitiert nach *IfD Allensbach* 2003, 17).
25 *IfD Allensbach* 2003, 17.
26 *IfD Allensbach* 2003, 19.
27 Dieses Begriffsverständnis wurde primär in sozialistischen Systemen propagiert. Freiheit durch Arbeit und soziale Sicherheit wird hier gegen politische Unfreiheit ausgetauscht, so *IfD Allensbach* 2003, 18.
28 *IfD Allensbach* 2003, 18.
29 *IfD Allensbach* 2003, 18.
30 *Luhmann* 1999, 61.

Diese Bedeutungen des Begriffs Freiheit sind noch lange nicht abschließend. Es handelt sich jedoch um die unserem Sprach- und Begriffsverständnis zu Grunde liegenden wesentlichen Dimensionen von Freiheit.[31]

Sicherheit ist nicht etwa ein Antonym zum Begriff der Freiheit oder zu einem seiner Bedeutungsinhalte, auch wenn Freiheit und Sicherheit häufig in der öffentlichen Diskussion als Gegensatzpaar gebraucht werden, wie es etwa in der Formel „Freiheit stirbt mit Sicherheit“[32] oder der Frage „Sicherheit statt Freiheit?“[33] deutlich wird. Gegensatz von Freiheit ist Unfreiheit. Sicherheitsmaßnahmen können zu Unfreiheit führen, sie dienen aber in der Regel dazu Sicherheit zu erzeugen, um Freiheit zu ermöglichen. Sie sind insofern durchaus eng miteinander verknüpft: für die Freiheit von Not bedarf es einer wirtschaftlichen Sicherheit, für die politische Freiheit ist die Sicherheit vor willkürlicher Festnahme erforderlich, etc.

Darüber hinaus ist den Begriffen Freiheit und Sicherheit gemein, dass sie sehr vage sind und der Konkretisierung bedürfen. Letztlich ist jeweils der Bezug zu einem Referenzobjekt erforderlich, um die aktuelle Bedeutung des Begriffs erfassen zu können.

Sicherheit meint politisch die innere und äußere Sicherheit. Darüber hinaus gibt es die private und öffentliche, die finanzielle und die ökologische Sicherheit.[34]

Lange wurde Sicherheit als Unversehrtheit von Rechtsgütern seitens Privater definiert − während Freiheit als Unversehrtheit von Rechtsgütern gegenüber der Staatsgewalt galt.[35] Heute wird Sicherheit hingegen zunehmend als Abwesenheit von Risiken verstanden.[36]

Damit lösen sich allerdings die Kriterien, die bis dato den Sicherheitsbegriff konkretisiert haben, auf.[37] Er ist also nicht mehr beschränkt auf den Schutz von Privaten im Staat, also auf die Innen- und Verteidigungspolitik, sondern bezieht sich generell auf die Abwesenheit von Risiken. Es wird von einem „erweiterten Sicherheitsbegriff gesprochen“.[38] Die Schwierigkeit besteht hier darin, dass mit zunehmender Erweiterung des Sicherheitsbegriffs, dieser immer unschärfer wird. Denn Risiken können potentiell überall entstehen.

---

31 *IfD Allensbach* 2003, 18 ff.

32 Gebräuchlich als linke Protestformel. So auch der Titel eines Buchs *JungdemokratInnen et al.* 2001.

33 So Titel und Thema der Dissertation von *Hornig* 2009; so titeln auch *Adick,* WDR, Quarks & Co v. 2.3.2010, abrufbar unter: http://www.wdr.de/tv/quarks/sendungsbeitraege/2010/0309/004_sicherheit.jsp; *Biermann,* ZEIT online v. 27.5.2007, abrufbar unter: http://www.zeit.de/online/2007/21/Amnesty; *Hausar* telepolis v. 14.6.2009, abrufbar unter: http://www.zeit.de/online/2007/21/Amnesty.

34 *Fuchs* 2010.

35 *Gusy*, VerwArch 2010, 309.

36 *Hefendehl*, JZ 2009, 165, 171.

37 *Gusy*, VerwArch 2010, 309, 311.

38 Kritisch zum erweiterten Sicherheitsbegriff *Pieroth/Schlink/Kniesel* 2012, § 2 Rn. 2a, der zur Rechtfertigung einer engeren Zusammenarbeit von Polizei und Nachrichtendiensten herangezogen wird.

Aus diesem Grund betonte schon *Luhmann* die Bedeutung der Unterscheidung von Sicherheit und Risiko. Denn Sicherheit gebe es in Bezug auf das Nichteintreten künftiger Nachteile gar nicht.[39] „Soziologisch gesehen heißt dies, dass der Sicherheitsbegriff eine soziale Fiktion bezeichnet und dass man, statt nach den Sachbedingungen der Sicherheit zu forschen, fragen muss, was in der sozialen Kommunikation als sicher behandelt wird. (…) Der Sicherheitsbegriff ist mithin ein Leerbegriff (…). Er universalisiert das Risikobewusstsein.“[40]

Entsprechend konstatiert sich in der Erweiterung des Sicherheitsbegriffs auf Sicherheit vor Risiken verschiedenster Art eine generelle Ausweitung des Sicherheitsbegriffs.[41]

Es wird im Bereich der Innen- und Verteidigungspolitik von einem „erweiterten Sicherheitsbegriff“ gesprochen.[42] Deutlich wird dies in Bezug auf die Innere Sicherheit etwa an der Aussage, Deutschlands Sicherheit werde am Hindukusch verteidigt.[43]

Um den Prozess der Ausweitung des Sicherheitsbegriffs und seinen Bedeutungszuwachs zu erklären, wurde in der Politikwissenschaft die *Securitization*-Theorie entwickelt. Der Begriff wurde von der konstruktivistischen *Kopenhagener Schule* geprägt.[44] Securitization wird hier als sozialer Prozess verstanden. Themen würden zu Sicherheitsproblemen durch die Nennung als Sicherheitsprobleme („securitzing speech act“).[45] Durch die Konstruktion einer existenzgefährdenden Bedrohung werden unter Verweis auf die kommunizierten Sicherheitsprobleme außergewöhnliche Formen des Regierens legitimiert.[46] Nach dieser Betrachtungsweise wird Sicherheit nicht objektiv/statisch definiert, sondern stets durch bestimmte „Sprechakte“[47] konstruiert. Dies zeigt auch warum, bzw. dass die Sicherheitsagenda unbeschränkt erweitert werden kann. Denn

---

39 *Luhmann* 1991, 28 f.

40 *Luhmann* 1991, 28.

41 *Fischer-Lescano*, KJ 2008, 166, Rn. 168.

42 Ausführlich zu diesem: *Daase* 2010; Auch im Vertrag von Lissabon wird der „erweiterte Sicherheitsbegriff“ für die Definition des Vorgehens der Union herangezogen, dazu *Kaufmann-Bühler,* in: *Grabitz/Hilf/Nettesheim,* EUR 2012, Art. 43 EUV Rn. 6.

43 So rechtfertigte der ehemalige Verteidigungsminister Struck 2002 den Einsatz deutscher Soldaten in Afghanistan. Dazu etwa *Strutynski* 2007. Hieran zeigt sich, dass nicht mehr zwischen innerer und äußerer Sicherheit differenziert wird, so: *Gusy*, VerwArch 2010, 309, 310; Diese Entwicklung spiegelt sich auch in der Diskussion um eine Neudefinition des Sicherheitsbegriffs bei den Vereinten Nationen: Eine Bedrohung der Weltsicherheit, sei „jedes Ereignis oder jeder Prozess, der zu einer großen Zahl von Todesfällen führt oder die Lebenschancen verringert und so die Staaten als Basiseinheiten des internationalen Systems unterminiert“. Dabei werden sechs Cluster von Bedrohungen genannt: 1. Wirtschaftliche und soziale (inklusive Armut, Infektionen und Umweltzerstörung); 2. Zwischenstaatliche Konflikte; 3. Innerstaatliche Konflikte, Bürgerkriege; 4. Nukleare, radiologische, chemische und biologische Waffen; Terrorismus; 6. Transnationales organisiertes Verbrechen.“ zitiert nach *Strutynski* 2007.

44 *Buzan/Waever/de Wilde* 1998.

45 *Williams*, International Studies Quarterly 2003, 511, 513; *Waever* 1995, 54 f.

46 *Buzan/Waever/de Wilde* 1998; Als wesentliche Elemente der Securitization benennt *Williams* „existential threats, emergency action, effects on interunit relations by breaking free of rules” *Williams*, International Studies Quarterly 2003, 511, 513 f.

47 Die Sprechakttheorie selbst ist umstritten. Dieser Diskurs ist aber für den hier gegebenen Verweis auf das Erklärungsmodell von Versicherheitlichung als Kommunikationsprozess in der Politikwissenschaft nicht weiter relevant. Zu dem Theorienstreit etwa *Schneider* ZfS 1996, 263.

durch die Bezeichnung von Sicherheitsproblemen als solche können sie aus dem „normalen“ Diskurs herausgehoben werden.

Gelungene Versicherheitlichungen in diesem Sinne sind Prozesse, in denen eine Sicherheitsgefährdung kommuniziert wird und jene Instrumente, die als neue und besonders rechtfertigungsbedürftige Maßnahmen zur Bewältigung der Sicherheitsgefährdung gefordert werden, von dem Adressaten des Sprechakts (Parlament oder Bevölkerung) sodann als alternativlos akzeptiert werden.[48] Als Beispiel für einen geglückten Securitization-Akt kann etwa die öffentliche akute Terrorwarnung im Winter 2010 durch den damaligen Innenminister *De Maiziére* genannt werden, in dessen Folge die Präsenz bewaffneter Polizei an Bahnhöfen drastisch erhöht und verstärkt Sicherheitskontrollen eingeführt wurden. Bei der Bevölkerung wurde dies als zwingend erforderliches und insofern alternativloses Instrument zur Gewährleistung der Sicherheit wahrgenommen.[49]

Auch die Verabschiedung der Vorratsdatenspeicherungsrichtlinie durch Rat und Europäisches Parlament ist beispielhaft für einen gelungenen Securitization-Prozess. So war die Einführung der Speicherung sämtlicher Telekommunikationsdaten aller Bürger auf Vorrat heftig umstritten.[50] Selbst der Berichterstatter im Parlament votierte gegen eine Annahme des Richtlinienentwurfs. Dennoch wurde der Entwurf, der unter dem Eindruck der Bombenanschläge in London vorgelegt worden war, in dem bis dahin schnellsten Rechtssetzungsverfahren der EU angenommen. Überzeugend wirkte dabei, dass vermittelt wurde die Anschläge in London durch eine Auswertung der Handy-Daten eines der Attentäter aufgeklärt worden seien.[51]

Der Sicherheitsbegriff hat heute eine starke Ausdehnung erfahren, indem er auf die verschiedensten Lebensbereiche ausgeweitet wurde. In seinem Kern bleibt aber die Bedeutung des lateinischen Securitas erhalten: Sicherheit als Sorgenfreiheit.[52]

Es wurde bereits dargelegt, dass Freiheit und Sicherheit keine Gegensätze sind. Dennoch stehen sie in einem natürlichen Spannungsfeld zueinander. Damit der Einzelne ohne Sorge seine Freiheit entfalten kann, muss die Freiheit des Einzelnen eingeschränkt werden. Dieser Zusammenhang zeigt deutlich ein Blick auf die Entwicklung des modernen Staats, der sowohl der Freiheit als auch der Sicherheit zu dienen verpflichtet ist.

---

48 *Fuchs* 2010.

49 *Fischer* 2011.

50 Eine ausführliche Darstellung der Einführung der Vorratsdatenspeicherung mit zahlreichen Nachweisen erfolgt unten S. 147 ff. (Kap.4.2).

51 *Rusteberg*, VBlBW 2007, 171, 173; *Alvaro*, DANA 2006, 52; *Prantl* 2008; Die Richtlinie wurde nach nur drei Monaten nach ihrer Vorstellung in einem Blitzverfahren verabschiedet. Die britische Ratspräsidentschaft hatte massiven Druck ausgeübt um das Verfahren noch während ihrer Präsidentschaft abschließen zu können; Ausführlich zur Einführung der Vorratsdatenspeicherungsrichtlinie, siehe unten S. 147 (Kap. 4.2).

52 Securitas, atis, f. lat. Für Sorgenfreiheit, Gemütsruhe auch Unerschrockenheit, Sicherheit, Sicherung; sicheres Geleit. So *Stowasser* 1994.

Schon im Mittelalter war Ziel guter Regierung „Securitas“.[53] Als sich die Agrargesellschaft hin zu einer Handelsgesellschaft entwickelte, wuchs ökonomisch begründet das Bedürfnis nach Sicherheit. Geboren wurde hier die Idee einer souveränen Staatsgewalt. *Bodin* (1530-1596) sprach der Staatsführung die „souveräne Gewalt“, das absolute und immerwährende Monopol jeglicher Gewaltanwendung, zu. Dieses wird heute als Gewaltmonopol des Staats bezeichnet.[54] Historisch hat sich das Gewaltmonopol aus dem Verbot der Fehden und dem Ewigen Landfrieden (1495) entwickelt.[55] Es war insofern wesentliches Merkmal des „modernen Staates“ im Gegensatz zum mittelalterlichen Herrschaftsverband, dass dieser das Gewaltmonopol innehat.[56]

Bei *Bodin*, der zwar die Souveränität als Wesensmerkmal des Staats ausmacht, bleibt in staatstheoretischer Hinsicht allerdings offen, worauf er diese Berechtigung gründet.[57] Eine Begründung findet sich später bei *Hobbes* (1588-1679), der dem Bürger einen absolutistischen Staat gegenüberstellt. Da alle Menschen Egoisten sind, bedürfe es eines starken Staats. Nur der *Leviathan* könne dem Bürger Sicherheit geben.[58] Allein durch den Staat könne das egoistische Individuum gebändigt werden.

Der übermächtige Staat, der bei *Hobbes* noch derjenige ist, der dem Bürger Sicherheit gibt, wird dann bei *Locke* (1632-1704) bereits als Bedrohung empfunden. Die Perspektive wird so auf eine Sicherheit vor dem Staat gelenkt. Der Gesetzgeber wird an das Recht gebunden und ihm unterworfen. *Locke* verlangt, um Sicherheit vor dem Staat zu gewährleisten, eine Teilung der Gewalten. Anders als *Hobbes,* der den Staat als absolut, eben als *Leviathan* zeichnet, sieht *Locke* den Legitimationsgrund des Staats auch in der Freiheitsgewährleistung.[59] Die Vereinigung von Sicherheits- und Freiheitsziel als Legitimationsgrund und Wesensmerkmal des modernen, westlichen Verfassungsstaats geht insoweit auf *Locke* zurück.[60]

Diese enge Verbindung von Freiheit und Sicherheit prägt zwar noch die heutige Verfassungsstaatlichkeit, sie hat sich aber durchaus seitdem weiter entwickelt. Zu erkennen ist dabei insbesondere im ausgehenden 18. und 19. Jahrhundert eine Verschiebung der Gewichte hin zur Konzentration auf die Gewährleistung individueller Freiheit

---

53 Dies illustriert etwa das Fresko in der Sala della Pace in Siena von *Ambrogio Lorenzetti* aus dem 14. Jahrhundert, so *Götz,* in: *Isensee*/*Kirchof*, HStR IV 2006, § 85 Rn. 18; eine ausführliche Analyse des Freskos findet sich bei *Schmidt* 2003.

54 "Der Staat ist definiert durch die dem Recht gemäß geführte, mit souveräner Gewalt ausgestattete Regierung einer Vielzahl von Familien und dessen, was ihnen gemeinsam ist" Von grundlegender Bedeutung ist für *Bodin* die Souveränität (oberste Befehlsgewalt) des Staates; „Les Six livres de la République“, (französische Erstausgabe 1583); Zitate nach *Schliesky* 2004, 77.

55 *Kloepfer,* Verfassungsrecht I 2011, § 1 Rn. 45

56 *Götz,* in: *Isensee*/*Kirchof*, HStR IV 2006, § 85 Rn. 19.

57 *Calliess*, ZRP 2002, 1, 2.

58 Leviathan or the Matter, Forme and Power of a Commonwealth Ecclesiastical and Civil, *Hobbes* (1651); *Hobbes,* (Hrsg. *Mayer* 2000).

59 *Calliess*, ZRP 2002, 1, 4.

60 *Götz,* in: *Isensee*/*Kirchof*, HStR IV 2006, § 85 Rn. 19.

durch die Begrenzung staatlicher Macht.[61] Dies verdeutlicht ein Zitat *Wilhelm von Humboldts*, der Sicherheit als „Gewißheit der gesetzmäßigen Freiheit" verstand.[62]

Entsprechend beinhalten die liberal geprägten Verfassungstexte eine Betonung der Freiheitsgefährdung durch die Staatsmacht. So verschwanden etwa Schutzpflichten oder ein Recht auf Sicherheit vollkommen aus den Verfassungstexten des 19. und 20. Jahrhunderts.[63] Die Funktion des Staates Sicherheit zu gewährleisten, insbesondere durch den Schutz des Lebens und die Gewährleistung einer funktionsfähigen Gefahrenabwehr und Strafverfolgung, sollte damit aber nicht aufgegeben werden, eine Positivierung dessen wurde vielmehr als entbehrlich betrachtet. Die Pflicht des Staates, seine Bürger zu schützen, wurde als Legitimationsgrund der Staatlichkeit dem Staat vorgelagert begriffen.[64]

Besonders deutlich wird der Fokus auf die Freiheitssicherung bei der Genese des Grundgesetzes. Unter dem unmittelbaren Eindruck des nationalsozialistischen Regimes lag der Fokus darauf die Allmacht des Gesetzgebers zu beseitigen, indem ihm inhaltliche Schranken gesetzt und Aufträge mit konkreten inhaltlichen Vorgaben erteilt wurden.[65] Dafür wurde die Legislative in ihrer Souveränität beschränkt, indem auch sie, und nicht mehr nur Judikative und Exekutive, sowohl an die Verfassung als auch an einfaches Recht gebunden wurde.[66]

Das Grundgesetz ist geprägt als liberaler (und sozialer) Rechtsstaats.

Schließlich lässt sich feststellen, dass zwar der Staatszweck Sicherheit „an der Wiege moderner Staatlichkeit" steht, wenn der Staat dieses Versprechen jedoch nicht einlöst, „gefährdet er seine Legitimität". Dennoch ist das, historisch betrachtet jüngere Versprechen, die Gewährleistung von individueller und gesellschaftlicher Freiheit, „nicht minder legitimationskräftig".[67]

---

61 *Götz,* in: *Isensee*/*Kirchof*, HStR IV 2006, § 85 Rn. 19.

62 *Von Humboldt* 1960, 147 (in der Schrift „Ideen zu einem Versuch, die Gränzen der Wirksamkeit des Staats zu bestimmen" von 1792). Dort führt er auch aus: „Dann ist eben diese Sicherheit, als der eigentliche Gegenstand der Wirksamkeit des Staats dargestellt, und endlich das Princip festgesetzt worden, dass, um dieselbe zu befördern und zu erhalten, nicht auf die Sitten und den Charakter der Nation selbst zu wirken, diesem eine bestimmte Richtung zu geben, oder zu nehmen, versucht werden dürfe. Gewissermaßen könnte daher die Frage: in welchen Schranken der Staat seine Wirksamkeit halten müsse, schon vollständig beantwortet scheinen, indem diese Wirksamkeit auf die Erhaltung der Sicherheit und in Absicht der Mittel hierzu noch genauer auf diejenigen eingeschränkt ist, welche sich nicht damit befassen, die Nation zu den Endzwecken des Staats gleichsam bilden oder vielmehr ziehen zu wollen. (…) Sicher nenne ich die Bürger in einem Staat, wenn sie in der Ausübung der ihnen zustehenden Rechte, dieselben mögen nun die Person, oder ihr Eigenthum betreffen, nicht durch fremde Eingriffe gestört werden" S. 145 ff.; ausführlich zum Verhältnis Freiheit und Sicherheit in der Philosophie *Humboldts*/*Petersen* 2010, 118 ff.

63 *Hopfauf*, in: *Schmidt-Bleibtreu/ Klein*, GG 2011, Einl., Rn. 141.

64 Sie braucht „vom Verfassungstext nicht förmlich sanktioniert werden, weil sie eine Voraussetzung seiner effektiven Geltung bildet", *Hopfauf*, in: *Schmidt-Bleibtreu/ Klein*, GG 2011, Einl., Rn. 141.

65 *Bettermann* 1986, 10.

66 *Bettermann* 1986, 11.

67 *Hoffmann-Riem* 2009, 56.

In der Entwicklung des modernen Staatsbegriffs spiegelt sich, was schon die sprachwissenschaftliche Betrachtung der beiden Begriffe zu Tage geführt hat – Freiheit und Sicherheit stehen in einem Spannungsverhältnis zueinander. Sicherheit heißt frei von Sorge sein und Freiheit ist nur möglich, wenn Sicherheit herrscht: Freiheit und Sicherheit setzen sich gegenseitig voraus.

1.2 Die Informationsgesellschaft

Die Informationsgesellschaft kann als eine auf Informations- und Kommunikationstechnik basierende „Transformationsgesellschaft", die auf einer „Informationsökonomie" beruht, beschrieben werden, die durch eine Durchdringung sämtlicher Lebensbereich mit dieser Technik (Informatisierung) gekennzeichnet ist.[68]

Das Internet ist heute von zentraler Bedeutung für private wie berufliche Aktivitäten: ob der Einzelne in seiner Freizeit mit Freunden kommuniziert, sich informiert oder einkaufen geht. Im Internet gibt es nahezu alles, was es auch in der Offline-Welt gibt. Kinder lernen schon in der Schule den Umgang mit PC und Internet. Universitäten bieten Online-Vorlesungen an. Millionen von Menschen kommunizieren über das Internet,[69] ob in Chatrooms, über Twitter oder Blogs, in sozialen Netzwerken, mittels Internet-Telefonie oder via E-Mail. Und es ist nicht nur private Kommunikation, die über das Internet erfolgt. Digitale Kommunikation prägt vielmehr sämtliche Lebensbereiche.[70] Der Einzelne ist dabei nicht nur Nutzer, der auf Informationen zurückgreift, sondern ist spätestens seit dem Einzug des Web 2.0 selbst zum Bestandteil der Netzstrukturen geworden.[71]

Gerade auch durch die aktive Einbindung des Einzelnen hat sich das Verständnis von und das Bedürfnis nach Privatheit gravierend verändert. Hatte man früher sein Tagebuch mit Schloss und Riegel unterm Kissen versteckt, so schreiben heute Millionen Menschen in Blogs, die frei zugänglich sind, über ihr intimes Leben.[72] Mehrere Milliarden Menschen stellen sich und ihr Leben über Einträge in sozialen Netzwerken dar. Das Mitwirken an diesen Netzwerken erfolgt heute nicht mehr vom Schreibtisch zu

---

68 *Thiel*, 2011, 6 im Folgenden ausführlich dazu, dass diese Definition nur ansatzweise die dahinter stehenden künftig zu bewältigenden Konflikte und Probleme erfasse.

69 Nach einer Studie des *bitkom* nutzten im Jahr 2011 72 Prozent der Deutschen das Internet, bitkom Studie „Datenschutz im Internet" v. 28.6.2011, S. 7; abrufbar unter: http://www.bitkom.org/de/publikationen/38338_68303.aspx. Anzumerken ist, dass der Prozentsatz bei über 65 Jährigen, die das Internet nicht nutzten bei 73 Prozent lag, während der Anteil der Nutzer im Alter zwischen 14 und 29 bei 95 Prozent lag.

70 *Sievers* 2002, 25.

71 Wesensmerkmal des Web 2.0 ist, dass die Benutzer Inhalte selbst in quantitativ und qualitativ entscheidendem Maße selbst erstellen, bearbeiten und verteilen und dabei von interaktiven Anwendungen unterstützt werden. Dazu *Alpar/Blaschke* 2008.

72 Eine speziell dafür eingerichtete Seite ist etwa http://www.tagebuchonline.com/portal.php; darüber hinaus gibt es zahlreiche private Blogs in denen Einzelne über ihr Leben und Befinden berichten.

Hause aus, sondern vielfach über das Smart-Phone, welches man ständig mit sich trägt.[73]

Ein Mobilfunkgerät ist so längst nicht mehr nur mobiler Telefonanschluss, sondern Kalender, Fotoapparat, Musik-Player und portabler Klein-Computer, der den Zugang zum Internet und dort die Verwaltung von sozialen Netzwerken, Informationen oder den Abruf und das Versenden von E-Mails ermöglicht – eben ein *Smart*phone.

Der Schritt in die Informationsgesellschaft wurde durch die „Digitale Revolution" ermöglicht. Ein Verständnis dieser Entwicklungen ist erforderlich um die Diskussion um den Ausgleich zwischen Freiheits- und Sicherheitsinteressen im digitalen Zeitalter adäquat führen zu können. Denn es ist notwendig zu verstehen, wie die Digitalisierung funktioniert, welche Auswirkungen sie hat und wie sie die gesellschaftlichen Verwirklichungsbedingungen prägt um die Frage der Auswirkung von technischen Sicherheits- und Überwachungsinstrumenten erfassen zu können. Daher wird diese Entwicklung im Folgenden genauer nachgezeichnet, bevor die technischen Grundlagen der Informations- und Telekommunikationsgesellschaft erläutert werden. Anschließend werden die Auswirkungen auf das Verständnis von und Bedürfnis nach Anonymität und Privatheit erörtert, bevor abschließend darauf eingegangen werden kann, ob und inwiefern die Digitalisierung und Informatisierung Freiheit und Sicherheit verändert haben.

1.1.1 Digitale Revolution

Als digitale Revolution wird in Anlehnung an den Begriff der industriellen Revolution[74], der seit Ende des 20. Jahrhunderts erfolgende, durch Computer und Digitalisierung ausgelöste, Umbruch bezeichnet, welcher zu einer Veränderung der Technologie und nahezu aller Lebensbereiche geführt hat.

1.2.1.1 Digitalisierung des Alltags

Grundlage dieser sind die Erfindung des Mikrochips, die Digitalisierung, die Verbreitung von Computern, der Aufbau weltweiter Kommunikationsnetze, insbesondere des Internets, und die stetige Steigerung der Speicher- und Rechenleistung sowie die zunehmende Miniaturisierung der Bauelemente.[75] Schließlich wurde die Verbreitung der

---

[73] *Briegleb,* heise online v. 20.8.2012, abrufbar unter: http://www.heise.de/-1670370.html; Dazu auch *Krempl,* „Vom Funk-Knochen bis zum I-Phone", Spiegel online v. 11.9.2007, abrufbar unter: http://www.spiegel.de/netzwelt/mobil/0,1518,504765,00.html.

[74] Wesensmerkmal der Industriellen Revolution ist, dass hier Muskelkraft durch Maschinen ersetzt wurde. Im Rahmen der digitalen Revolution wird nun die Denkleistung des Menschen durch Maschinen ersetzt.

[75] Zur Entwicklung von Preisen und Rechenleistung kann der drastische Vergleich gezogen werden: „Hatte man 1972 noch die Wahl, ob man sich für umgerechnet rund 80.000 Euro ein Einfamilienhaus oder 1 Mbit Speicher zulegen sollte, entspricht der Gegenwert für dieses Speichervolumen heutzutage bei einem Preis von wenigen Cent gerade noch einem einzelnen Kaugummi", so *Donath,* „Rechenleistung für erste Mondlandung heute in einem Laptop", v. 10.4.2002, abrufbar unter: http://www.golem.de/0204/19234.html.

Informations- und Kommunikationstechnologie in der gesamten Gesellschaft auch durch einen deutlichen Preisverfall begleitet und ermöglicht.[76]

Im privaten Bereich werden Computer erst seit den 1980er Jahren eingesetzt. Heute handelt es sich um einen Alltagsgegenstand, der jedenfalls in westlichen Ländern zur allgemeinen Grundausstattung gehört.[77] Dieser Prozess wird auch als Computerisierung bezeichnet.[78]

Neuartig sind die digitalen Güter Software und Informationen. Im Unterschied zu klassischen Gütern der Offline-Welt können sie beliebig oft benutzt und kopiert werden − ohne dass sie dabei verbraucht würden. Meist ist sogar nicht einmal ihr Gebrauch nachweisbar. Die Möglichkeit, digitale Güter zu verbreiten, hat auf Grund dessen sowohl die Marktwirtschaft stark verändert[79] als auch neue Formen der Kriminalität hervorgebracht, wie etwa Datenbeschädigung oder Angriffe auf Computersysteme. Auch wird das gesamte geltende Urheberrecht auf Grund der digitalen Revolution in Frage gestellt.[80]

Gleichfalls stehen die Strafverfolgungsbehörden, die bedingt durch veränderte und neuartige Formen der Kriminalität und die Verlagerung der Kriminalität aus der Offline-Welt in die Online-Welt, vor neuen Herausforderungen. Denn anders als in der Offline-Welt hat das Internet kein soziales Gedächtnis: es gibt keine Zeugen, wie es sie in der Offline-Welt gibt.[81] Zwar ist grundsätzlich alles, was einmal im Netz ist, rekonstruierbar. Dies ermöglicht – soweit diese Daten denn verfügbar sind – allerdings noch nicht unbedingt den Schluss darauf, welche Person wie in der Online-Welt gehandelt hat.

Genauso hat die Digitalisierung aber auch neue Möglichkeiten der Strafverfolgung und Kriminalitätsbekämpfung geschaffen. Noch nie konnten so viele Informationen gesammelt und analysiert werden, wie es die moderne Datenverarbeitung ermöglicht.

Staat, Wirtschaft und Bürger – sie sind allesamt sowohl Nutznießer als auch Getriebene einer sich rasant fortentwickelnden Informations- und Kommunikationstechnik, die das gesamte Alltagsleben wesentlich verändert hat.[82] Symptomatisch dafür ist, dass die Menge an personenbezogenen Daten, die in den modernen Technikanwendungen genutzt und verarbeitet werden, stetig wächst. Damit einher geht die Möglichkeit umfas-

---

[76] Der Verbraucherpreisindex für PCs sank von 2000 bis 2008 um 87,1Prozent; *DESTATIS* Informationsgesellschaft 2009, S. 36.

[77] Im Jahr 2008 verfügten 75 Prozent der deutschen Haushalte über einen PC, *DESTATIS* Informationsgesellschaft 2009, S. 23.

[78] http://de.wikipedia.org/wiki/Digitale_Revolution, Technischer Wandel v. 30.10.2012.

[79] So können die Entwicklungen auf dem Telekommunikationsmarkt als Voraussetzung der Globalisierung bezeichnet werden, dazu ausführlich Kap. **1.3**.

[80] Dazu etwa *Wandtke*, in *Wandtke*/*Bullinger*, Einl. Rn. 1; Zu den veränderten Rahmenbedingungen des Urheberrechts, siehe auch *Flechsig*, ZGE 2011, 19; Ansätze zur Reform des Urheberrechts etwa einer Kulturflatrate *Roßnagel* et al. 13.3.2009.

[81] Das *BVerfG* erkennt an, dass es kein „gesellschaftliches Gedächtnis“ gebe, BVerfGE 125, 260 (323).

[82] *Roßnagel* 2011b, 36.

sende Informationen aus diesen Daten über den Einzelnen ermitteln zu können.[83] Der Einzelne droht dabei zum „gläsernen Bürger" zu werden.

1.1.1.1 Auf dem Weg in eine Welt des Ubiquitous Computing

Die Entwicklungen von Internet und Mobilfunktechnologie sind noch längst nicht abgeschlossen. Wir entwickeln uns hin zu einer allumfassenden Datenverarbeitung – einer Welt des *Ubiquitous Computing*.[84]

Dieser Zukunftsvision, deren Realisierung immer näher rückt, liegt die Vorstellung zugrunde, dass der Computer als spezifisches Gerät weitgehend aus unserer Welt verschwinden wird und an dessen Stelle vielfältige Alltagsgegenstände über eine umfassende Rechenleistung verfügen. Diese bieten dem Menschen unmerklich und allgegenwärtig eine „smarte" Umgebung.[85] Die Entwicklung dahin hat längst begonnen. So werden heute intelligente Stromzähler und -netze eingeführt,[86] die E-Mobilität nimmt zu, erste intelligente Haushaltsgeräte kommen auf den Markt.[87] Die Anbindung von Alltagsgeräten an das Internet nimmt stetig zu. So sind heute schon der Einsatz von RFID-Technologie zur Information über Produkte im Supermarkt, die Vernetzung der Digital-Kamera mit dem Internet und der automatische Abruf von Informationen zu jedem Ort, an dem wir uns befinden gängige Technik. Die Weiterentwicklung von RFID-, GPS-, Bilderkennungssoftware, Robotik, Rechen- und Speicherkapazitäten schreitet unaufhörlich voran. Dass bald nicht mehr das Smart-Phone, sondern die intelligente Brille uns über das informiert was uns umgibt, erscheint so schon heute als greifbare Vision.[88] Eine Welt des *Ubiquitous Computing* ist zwar weitgehend noch immer Zukunftsmusik. Der Weg dorthin ist aber nicht mehr weit.

1.1.2 Technische Grundlagen digitaler Kommunikation

Wenn man sich mit der Frage auseinandersetzen möchte, wie sich die Verwirklichungsbedingungen von Freiheit und Sicherheit im digitalen Zeitalter verändert haben, ist dafür ein Verständnis der technischen Rahmenbedingungen notwendig. Im Fol-

---

83 *Roßnagel* 2011b, 36.

84 Grundlegend hat den Begriff Ubiquitous Computing Weiser bereits in einer zukunftsweisenden Vision 1991 geprägt, *Weiser,* Scientific American 1991, 94; dazu auch *Mattern* 2003; *Roßnagel* 2008 (hier insbesondere der Teil der von *Mattern*, S. 4 ff.); *Roßnagel/Müller,* CR 2004, 625; *Guinard//Trifa/Mattern/Wilde* 2011, 97. Der Forschungsverbund Venus, der im Rahmen der LOEWE-Initiative gefördert wird, entwickelt an der *Universität Kassel* sozialverträgliche Ubiquitous Computing Anwendungen, http://www.uni-kassel.de/einrichtungen/iteg/venus/.

85 *Roßnagel/Müller*, CR 2004, 625, 625. Die Autoren setzen sich auf den S. 628 ff. ausführlich mit den neu erwachsenden Anforderungen für den Datenschutz auseinander.

86 Zu den IT- und Datenschutzrechtlichen Anforderungen bei sog. Smart Metern und Smart Grids, etwa *Raabe/Lorenz/Pallas/Weis/Malina* DuD 2011, 519 ff.; *Wiesemann*, MMR 2011, 355; vgl. auch *Jandt/Roßnagel/Volland*, ZD 2011, 99.

87 Die Vision eines „smart homes" war etwa Thema der Cebit 2011, *Jäger,* PC-Welt v. 3.3.2011, „Das Haus der Zukunft", abrufbar unter: http://www.pcwelt.de/ratgeber/Automation-und-intelligente-Elektronik-So-schlau-wird-das-Smart-Home-1482302.html.

88 Wie etwa Googles „Project Glass", dazu *Schwan,* Technology Review v. 3.7.2012, abrufbar unter: http://heise.de/-1630150.

genden sollen daher die Grundlagen der modernen Informationstechnologie mit einem Schwerpunkt auf der Telekommunikation[89] dargestellt werden.

1.1.2.1 Die Funktionsweise des Internet

Im Allgemeinen wird der Begriff Internet verwendet als Bezeichnung für das World-Wide-Web (WWW). Dabei handelt es sich um das architektonische Rahmenwerk für den Zugriff auf verknüpfte Dokumente, die auf Millionen von Rechnern überall im Internet verteilt liegen.[90] Dieses wird auch als riesiges „Online-Informationslager" beschrieben, das Benutzer mit Hilfe eines interaktiven Anwendungsprogramms namens Browser, durchsuchen können.[91] Das WWW ist jedoch nur einer der Dienste, den das Internet ermöglicht.

Dies führt zu der Frage, was ist das Internet? Der Begriff Internet kommt vom englischen *Interconnected Network* was auf Deutsch *verbundenes Netzwerk* heißt. Dies macht deutlich, was das Wesen des Internets ausmacht: Es handelt sich um ein weltumfassendes Computernetzwerk, das unzählige Computer, die über die ganze Welt verteilt stehen, miteinander verbindet. Es ist insofern nicht ein Netz, sondern es handelt sich um eine riesige Ansammlung verschiedener Netze, die bestimmte gängige Protokolle nutzen und bestimmte allgemeine Dienste zur Verfügung stellen. *Tanenbaum* beschreibt es als „ein ungewöhnliches System, das von niemandem geplant war und auch von niemandem kontrolliert wird."[92] *Intranets* sind im Gegensatz dazu Computernetzwerke, die über ein lokales, etwa ein Firmen-Netzwerk oder ein Universitätsnetzwerk, miteinander verbunden sind.

Dass es sich beim Internet um ein Computernetzwerk handelt, ist insofern irreführend, als es nicht traditionelle Desktop-PCs sind, die Informationen senden und speichern, sondern es in einer zunehmend ubiquitären Welt zahlreiche Gegenstände des Alltags sind, die an das Internet angeschlossen sind, wie Mobiltelefone, Webcams, Automobile, Umweltsensoren, digitale Bilderrahmen, Haushaltsgeräte oder Sicherheitssysteme.[93]

Die Endgeräte, die selbst wenige oder gar keine Dienste bereitstellen, werden als Clients bezeichnet. Diejenigen Rechner hingegen, die in erster Linie Internetdienste bereitstellen, werden als Server bezeichnet.

Zu nennen sind darüber hinaus noch sogenannte Peer-to-Peer-Anwendungen. Diese bezeichnen Systeme, bei denen der Client anderen Clients eines Verbundes Anwendungen zur Verfügung stellt.

---

89 Eine ausführliche Erläuterung der modernen Telekommunikationstechnik findet sich etwa bei *Schnabel* 2008.

90 *Tanenbaum* 2003, 664.

91 *Comer* 2002, 489.

92 *Tanenbaum* 2003, 67.

93 *Kurose/Ross* 2008, 23. Hier wird aufgeführt, dass im Juli 2007 bereits 490 Millionen Endsysteme das Internet benutzten, heute dürften es weit mehr sein.

Endsysteme greifen nicht unmittelbar auf das Internet zu, sondern werden über Internetdienstanbieter (Internet Service Provider; kurz: ISP) mit dem Internet verbunden.[94] Die Verbindung von Endnutzern und Content-Providern im Zugangsnetz ist nur ein einzelnes kleines Teil im Puzzle, das darin besteht, „die Hunderte Millionen Endbenutzer und hunderttausende Netzwerke miteinander zu verbinden, die das Internet bilden."[95] Bei diesen handelt es sich um die unterste Stufe der Hierarchie von ISPs. Im Gegensatz zu den Internetdienstanbietern, die dem Endnutzer den Zugang zum Internet ermöglichen, stehen an der obersten Spitze sogenannte Tier-1-ISPs (auch: Stufe-1-ISPs) oder Internet-Backbones.[96]

Endsysteme sind durch ein Netz von Kommunikationsleitungen (Communication Links) und Paketvermittlungen (Packet Switches) verbunden.[97]

Die Kommunikationsleitungen sind aus unterschiedlichen physikalischen Medien aufgebaut, wie etwa Koaxialkabel, Kupferdrähte, Glasfasern oder Funkwellen.[98] Im Kernbereich, also auf Ebene der Backbone-Netzen, besteht das Internet im Wesentlichen aus Glasfaserkabeln, die durch Router zu einem Netz verbunden sind.

Informationen werden über das Internet verschickt, indem diese zunächst vom sendenden System aufgeteilt, dann mit Header-Bytes versehen und so dann in einzelnen Teil-Paketen an das Zielendsystem versandt werden. Die Übertragungsgeschwindigkeit einer Leitung wird in Bit[99] pro Sekunde gemessen. Dabei ist die Struktur des Internets insgesamt stark dezentral; was der Entwicklungsgeschichte geschuldet ist und eine hohe Ausfallsicherheit gewährleistet.[100]

Die Paketvermittlungsstellen, in der Regel Router oder Switches, haben die Funktion ankommende Pakete auf eine Ausgangsleitung in Richtung der Zieladresse weiterzuleiten und so den weltumspannenden Datentransfer zu ermöglichen. Der größte deut-

---

94 *Kurose/Ross* 2008, 25. Zu beachten ist, dass auch jeder Internetdiensteanbieter ein Netzwerk ist, das aus Paket-Switches und Kommunikationsleitungen besteht. Zu Privatanbietern gehören AOL und lokale Telefongesellschaften, sowie Kabelanbieter, ebenso wie Firmen-Netzwerke, Universitäts-Netzwerke und Anbieter von Drahtlosnetzwerken, wie etwa T-Mobile.

95 *Kurose/Ross* 2008, 54.

96 *Kurose/Ross* 2008, 55. Wesensmerkmal dieser ist, dass sie direkt mit jedem anderen Tier-1-ISP verbunden sind, sie mit vielen Tier-2-Netzwerken und anderen Kundennetzen verbunden sind und dass sie international arbeiten. Dazu zählen Sprint, Verizon, AT&T, NTT, Level3, Qwest und Cable&Wireless. Tier-2-ISPs arbeiten im Gegensatz dazu nicht international sondern meist in einem ganzen Land.

97 Datenübertragung wird ausführlich im Teil 1 S. 63 ff, Paketübertragung ausführlich im Teil 2 S. 99 ff. bei *Comer* 2002 behandelt.

98 *Kurose/Ross* 2008, 23, die verschiedenen Trägermedien werden auf den S. 42 ff. beschrieben.

99 Die Datenmenge entspricht in diesem Fall der verwendeten Anzahl von binären Variablen zur Abbildung der Information, kann also nur als ganzzahliges Vielfaches von 1 Bit angegeben werden, so http://de.wikipedia.org/wiki/Bit (30.10.2012).

100 Zu Selbstheilungskräften durch Routing, *Dierichs/Pohlmann, „*So funktioniert Internet-Routing, Wie Routing dem Netz seine Selbstheilungskräfte verleiht", heise netze v. 15.9.2008, abrufbar unter: http://www.heise.de/netze/artikel/So-funktioniert-Internet-Routing-221495.html.

sche Internetknotenpunkt (DE-CIX in Frankfurt am Main)[101] schaltet über hundert Netzwerke zusammen.

Da ein autonomes System, wenn es globalen Datenverkehr ermöglichen möchte, wie z. B. ein Internetprovider, nicht alle anderen Knotenpunkte erreichen kann, benötigt auch dieser in der Regel mindestens einen Provider, der den verbleibenden Datenverkehr zustellt. Nur die wenigen großen Tier-1-Provider können ihren gesamten Datenverkehr allein auf Basis der Gegenseitigkeit (Peering) abwickeln, ohne über einen Upstream-Provider zu kommunizieren.[102] Nur ein Bruchteil, der Internetdienstanbieter, die am deutschen Markt aktiv sind, verfügen selbst über ein Netz,[103] alle anderen Betreiber nutzen vollständig die Netze anderer Internetdienstanbieter. Aber auch jene Anbieter, die in Teilen über ein eigenes Netz verfügen, müssen bei fast allen Kommunikationsvorgängen um eine Nachricht dem Adressaten zu übermitteln auch die Netze anderer Anbieter nutzen.

1.1.2.1.1 Datenübertragung: Schichten und Protokolle

Die Datenübertragung im Internet wird mit Autobahnen, Straßen und Kreuzungen, die als Transportnetze verbunden sind, verglichen: Ein Unternehmen vor, welches ein hohes Frachtaufkommen von einem Lager zu einem anderen weit entfernten Lager verbringen muss, kann dies nicht auf einmal, sondern muss die Fracht aufteilen und auf eine Flotte von Lastkraftwagen oder Güterzügen verteilen. Jeder Transporter fährt dann unabhängig von den anderen auf dem Straßennetz zum vorgegebenen Zielort. Dort wird es dann wieder erneut zusammengesetzt.[104]

Wie für den Frachtverkehr auf der Straße sind auch für einen reibungslosen Ablauf der Datenübertragung im Internet bestimmte Regeln und Verfahren erforderlich. Um den verschiedenen Teilproblemen bei der Datenübertragung zwischen verschiedenen Netzen Herr zu werden, wurde der Gesamtvorgang der Kommunikation im Internet auf verschiedene Ebenen aufgeteilt.[105]

Das Standardmodel für internationalen Datenaustausch über Netzwerke ist das OSI-Modell.[106] Das Modell wurde auf einen Vorschlag von der „*International Organizati-*

---

[101] http://www.de-cix.de/

[102] http://de.wikipedia.org/wiki/Internet (30.10.2012).

[103] Über das größte Netz in Deutschland verfügt die Deutsche Telekom *AG*. Darüber hinaus gibt es ca. 30 weitere Internetdiensteanbieter, die über ein eigenes Netz verfügen: BITel Gesellschaft für Telekommunikation mbH; DATEL (Daten- und Telekommunikations-) GmbH; DNS:NET Internet Service Gmbh; DOKOM GmbH; ComIngolstadt; Envia Tel; EWE Netz GmbH; Heli Net- Telekommunikations GmbH & Co. KG; Herzo Media GmbH & Co. KG; Kabel Deutschland Holding *AG*; Kabel BW GmbH; KielNet GmbH; KurpfalzTel GmbH; LambdaNet Communications Deutschland *AG*; M-Net Telekommunikations GmbH; Multi Connect; NetCologne Gesellschaft für Telekommunikation mbH; PrimaCom GmbH; QSC *AG*; RelAIX Networks GmbH; R-Kom GmbH; std.net *AG*; Tele Columbus GmbH & Co. KG; Telefónica Germany; Unitymedia *AG*; Versatel *AG*; Vodafone Deutschland *AG*; VSE NET GmbH; Sitz in Saarbrücken; wilhelm.tel GmbH; Witcom GmbH (keine Anspruch auf eine abschließende Nennung der Betreiber/ Stand 2012).

[104] *Kurose/Ross* 2008, 25.

[105] *Kurose/Ross* 2008, 25.

[106] Die Abkürzung steht für Open Systems Interconnection Reference Model.

on for Standardization" (ISO) entwickelt und war der erste Schritt auf dem Weg zur internationalen Standardisierung der verschiedenen Protokolle.[107] Es handelt sich dabei um ein aus sieben Schichten bestehendes Referenzmodell.

Das OSI-Modell wurde mittlerweile durch das Internet-Referenzmodell (TCP/IP-Referenzmodell) abgelöst, beide Modelle haben jedoch viel gemeinsam. So ist etwa auch ein Großteil der OSI-Terminologie bis heute gebräuchlich, auch wenn das heute gängige TCP/IP-Referenzmodell an sich über weniger Schichten verfügt. Dieses eignet sich jedoch gut, um leicht verständlich die komplexen Beziehungen zwischen den Hardware- und Protokollkomponenten eines Netzwerks zu erklären.[108]

Im Internet wird heute das TCP/IP-Referenzmodell eingesetzt, das ursprünglich für das ARPANET[109] vom US-Amerikanischen Department of Defence entwickelt wurde.[110] Ziel war es eine möglichst flexible Architektur zu gestalten, die in der Lage ist sowohl Dateien als auch Sprache in Echtzeit zu übertragen und dabei sicherzustellen, dass selbst bei einem Hardwareausfall von einzelnen Verbindungsnetzen das Netz an sich funktionsfähig bleibt.[111]

Die sogenannte Internetschicht[112] hält wie eine „Sicherheitsnadel", die gesamte Architektur zusammen.[113] Sie hat die Aufgabe, es den Hosts zu ermöglichen, Pakete in jedes beliebige Netz einzuspeisen und an das jeweils gewählte Ziel, ob im gleichen Netzwerk oder in ein anderes, zu befördern. Die Pakete können in anderer Reihenfolge als sie versendet wurden ankommen. Es ist dann die Aufgabe der übergeordneten Schichten, sie wieder in die richtige Reihenfolge zu bringen.[114]

Beim Datenversand im Internet wird den einzelnen Paketen, in welche eine Information zerteilt wurde, je ein Kopf vorangestellt, der unter anderem die IP-Adresse des Zielrechners sowie die IP-Adresse des Absenders enthält. Für die eigentliche Übertragung wird dann auf die Dienstleistungen der physischen Schicht zurückgegriffen.[115] Vorbereitet wird die Übertragung durch die Internetschicht von der Transportschicht, indem diese den Ursprungsdatenstrom in einzelne Datenpakete aufteilt.[116] Die IP-Adresse ist insofern zentral damit jede Information den richtigen Adressaten erreichen kann.

---

[107] *Tanenbaum* 2003, 54 eine ausführliche Darstellung der einzelnen Schichten findet sich bei *Tanenbaum* auf S. 55 ff.
[108] *Comer* 2002, 269.
[109] Das Arpanet ist der „Urahn aller Rechnernetze", dessen Entwicklung vom US-Verteidigungsministerium gefördert wurde, *Tanenbaum* 2003, 58.
[110] *Sievers* 2002, 38.
[111] *Tanenbaum* 2003, 58 f.
[112] Hier gilt es zu beachten, dass der Begriff Internet hier in einem allgemeinen Sinn verwendet wird und nicht nur das Internet gemeint ist. Die Internetschicht des TCP/IP-Referenzmodells ist mit der OSI Vermittlungsschicht von Ihrer Funktionalität her vergleichbar.
[113] *Tanenbaum* 2003, 59.
[114] *Tanenbaum* 2003, 58 ff.
[115] *Freiling* 2009, 5.
[116] *Sievers* 2002, 41.

1.1.2.1.2 IP-Protokoll und IP-Adresse

Das Internet Protocol wird in der Netzwerkschicht verwendet. Dem Grunde nach kann jede IP-Adresse eindeutig einem Rechner zu einem Zeitpunkt zugeordnet werden. Denn nur so ist der korrekte Datenverkehr im Internet möglich.

Die IP-Adresse der Zielseite, die lautet „431.431.401.01“ und insofern kaum zu merken ist, wird in einen leicht fassbaren Namen, etwa „uni-kassel.de“ umformuliert. Die Übersetzung der IP-Adresse beim Aufruf einer Webseite erfolgt durch ein Domain Name System (kurz: DNS). Dieses hat die Funktion den Domain-Namen (*uni-kassel.de)* in die zugehörige IP-Adresse umzuwandeln. Der Browser ermittelt über die Anfrage bei einem DNS-Server die IP-Adresse der gesuchten Domain, sodass einfach Webseiten aufgerufen werden können. Denn ohne DNS müsste man anstatt Namen einzugeben, jeweils die IP-Adresse einer Webseite eingeben.

IP-Adressen der vierten Generation (IPv4)[117] bestehen aus zwei Teilen. Davon dient der erste Teil dazu, das lokale Netzwerk, in dem sich der Rechner befindet, zu identifizieren. Der zweite Teil bezeichnet dann den einzelnen Rechner innerhalb des lokalen Netzwerkes. IPv4 Adressen bestehen aus vier Stellen, die jeweils ein Byte groß sind.[118] Daraus ergibt sich eine 32 Bit lange Binärzahl. Insgesamt stellt IPv4 damit 2^{32} ($2^{32} = 256^4 = 4.294.967.296$) Adressen zur Verfügung.[119]

Da dieser Adressraum schon lange nicht mehr genügt, um alle an das Internet angeschlossenen Geräte mit einer Adresse zu versehen, wurden in der Vergangenheit (und werden auch noch aktuell) vielfach Adressen dynamisch, also nur für eine Sitzung, vergeben. Es wird insofern zwischen dynamischen und statischen IP-Adressen differenziert. Statische sind solche, die einem bestimmten Gerät oder Nutzer fest zugewiesen sind. Dynamische solche, die nur für eine Sitzung vergeben werden. Ein weiterer Grund für die Vergabe dynamischer IP-Adressen besteht darin, dass diese aus datenschutzrechtlicher Perspektive sowie zur Gewährleistung der Datensicherheit vorzugswürdig sind. Denn bei der Nutzung dynamischer IP-Adressen kann das Handeln im Netz nicht unmittelbar einem Anschluss zugeordnet werden kann und so auch weniger leicht nachvollzogen werden.

Fest werden auch vielfach innerhalb von privaten oder firmeneigenen Netzwerken IP-Adressen an die Nutzer bzw. Mitarbeiter verteilt. Während intern die Kommunikation über diese festen IP-Adressen erfolgt, wird für die externe Kommunikation via *Network Address Translation* (NAT) jeweils kurzfristig eine dynamische öffentliche und global eindeutige IP-Adresse zugewiesen.[120] Auch im Bereich des mobilen Internets

---

[117] IP Adresse der vierten Version des Internet Protocol. Es wurde in RFC 791 im September 1981 definiert.

[118] Die Blöcke sind über Punkte voneinander getrennt und erfassen je eine Dezimalzahlenzahl zwischen 0 und 255.

[119] *Sievers* 2002, 43.

[120] Dabei werden temporär private IP-Adressen intern vergeben, die jedoch im öffentlichen Netz nicht sichtbar sind. Auf Port-Basis wird dem Nutzer eine öffentliche IP-Adresse zugeordnet. Eine nachträgliche Rückverfolgung erfordert daher mehrere Daten, nämlich die private IP-Adresse, den Port der Verbindung, die öffentliche IP-Adresse sowie den exakten Zeitpunkt der Nutzung. Port und

wird dieses Verfahren eingesetzt, da Adressen nur sehr kurz vergeben und jede andere Methode für die Internetdienstanbieter zu aufwendig und teuer wäre. Dies gilt jedoch nur soweit die Geräte nicht I6Pv-fähig sind. Ansonsten wird auch bei der Nutzung mobilen Internets Endgeräten jeweils eine feste IPv6 Adresse zugewiesen.

Bei IPv6[121] handelt es sich um die Nachfolgeversion von IPv4, welche dieses Schritt für Schritt ablösen wird.[122] Die neue Adressversion stellt 2^{128} Adressen (≈ 340 Sextillionen = $3{,}4 \cdot 10^{38}$) zur Verfügung.[123] Das sind 2^{96} mehr Kombinationen als mit IPv4.[124] Damit soll die Adressknappheit nun dauerhaft behoben sein.[125] Dies führt dazu, dass NAT nicht mehr benötigt werden wird.[126] Daher dürfte grundsätzlich auch eine Mehrfachverwendung nicht mehr erforderlich sein, so dass die Zuordnung einer IP-Adresse zu einem Rechner (theoretisch) vereinfacht wird.[127]

Durch die Einführung von IPv6 wird nicht nur die Adressknappheit behoben. IPv6 beinhaltet darüber hinaus einen für die Netzwerkschnittstelle eindeutigen Interface Identifier, der nicht vom Provider zugeteilt wird, sondern vom Endgerät selbst erzeugt wird. Der Provider vergibt nur noch den ersten Teil, das sogenannte Präfix, welches insoweit der bisherigen IPv4-Adresse entspricht.[128] Der Interface Identifier ermöglicht es jedem mit Netzwerkschnittstellen ausgestatteten Gerät – ob PC, Laptop, TabletPC, Computer oder Fernseher –, eine eigene statische IP-Adresse zuzuweisen. Damit ermöglicht IPv6 grundsätzlich eine Nachverfolgung sämtlicher Nutzer.[129]

Da der mit IPv6 zur Verfügung stehende Adressraum eine permanente fixe Adressierung ermöglicht, welche dazu führt, dass letztlich eine anonyme Kommunikation ausscheidet, hat die *Internet Engineering Task Force (IETF)* Privacy Extensions[130] entwi-

---

IP-Adressen werden jedoch nur temporär und häufig nur für einen sehr kurzen Zeitraum vergeben. Dies führt dazu, dass bereits kurze Zeit später ein anderer Kunde über den Port verfügt und die öffentliche IP-Adresse das Internet nutzt. Daher kann häufig nur eine große Anzahl von Kunden zu einer öffentlichen IP-Adresse genannt werden und nicht auf eine konkrete Person verwiesen werde.

121 RFC 2460 (Dezember 1998).

122 Das Ende des IPv4 Adressraums wurde im April 2011 erreicht, http://www.apnic.net/publications/news/2011/final-8.

123 http://de.wikipedia.org/wiki/IPv6.

124 IPv6 sind 16 Byte lang und werden als 8 getrennte Blöcke aus jeweils 4 hexadezimal Ziffern angegeben, z.B. 2001:0db8:85a3:08d3:1319:8a2e:0370:7344. In URLs kollidiert das Kolon mit der Portangabe. Es werden daher die IPv6-Nummern in einer URL in eckige Klammern gesetzt, z.B. http://[2001:0db8:85a3:08d3:1319:8a2e:0370:7344]:80/, dazu http://www.heise.de/netze/artikel/Adress notation-224160.html.

125 *Sievers* 2002, 46.

126 So RFC 4864.

127 *Sievers* 2002, 46.

128 Dieser Teil kann bei IPv6 unterschiedlich lang sein, er umfasst maximal 64 Bit. Das Präfix ist innerhalb eines Netzwerks immer gleich, *Endres*, c't 2011, 182.

129 Ursprünglich war sogar gedacht den Interface Identifier jeweils aus der MAC-Adresse (also der eindeutigen Seriennummer des Endgerätes) abzuleiten. So wäre es möglich den Datenverkehr, unabhängig vom Präfix, einem bestimmten Endgerät zuzuordnen, *Freund/Schnabel*, MMR 2011, 495, 496.

130 RFC 4941 (Privacy Extensions for Stateless Address Auto configuration).

ckelt. Diese ermöglichen es, dass eben keine permanente Verbindung zu einer IP-Adresse erzeugt wird, sondern zumindest in Teilen eine dynamische Adressierung beibehalten wird. Bei vielen Betriebssystemen sind diese jedoch standardmäßig deaktiviert.[131] Notwendig ist insoweit Aufklärung und Schulung der Nutzer, dass und wie sie in Zukunft weiterhin anonym surfen können. Soweit die Privacy Extensions aktiviert sind, erzeugt der Rechner regelmäßig (für eine begrenzte, konfigurierbare Zeit) zufällige Interface Identifier.[132] Damit wird sichergestellt, dass ein Rechner auch nicht mehr über längere Zeit über den Interface Identifier identifiziert werden kann.

Möglich ist theoretisch auch die Präfixe zukünftig weiter dynamisch zu vergeben. Dies bedeutet jedoch im Vergleich zu einer statischen Vergabe einen höheren technisch-organisatorischen Aufwand. Daher wird zum Teil davon ausgegangen, dass die Provider unter IPv6 ein statisches Zuweisungsverfahren einsetzen werden.[133] Andererseits haben mehrere große Telekommunikationsdiensteanbieter bereits angekündigt, dass sie auch nach der Umstellung auf IPv6 weiter das Präfix dynamisch vergeben werden.[134]

Möglicherweise werden jedoch die Provider die Vorteile des hierarchischen Adressaufbaus auch innerhalb der Netze nutzen, um darin die Netzstruktur abzubilden. Die Präfixe hätten dann automatisch eine geografische Bedeutung.[135]

Neben dem Interesse eine anonymen Nutzung des Internet zu ermöglichen, besteht auch aus Perspektive der Provider ein wirtschaftliches Interesse daran, gegen einen Aufpreis statische IPv6-Präfixe zu vergeben, wie derzeit statische IPv4-Adressen vergeben werden. Denn professionelle Server brauchen die statischen IP-Adressen und sind daher auch bereit dafür zu bezahlen. Soweit nur noch leitungsgebundene Präfixe vergeben werden, würden die Provider sich letztlich selbst das profitable Zusatzgeschäft nehmen.[136]

Inwiefern IPv6 eine eindeutige Identifizierbarkeit eines bestimmten Geräts erlaubt, hängt letztlich von zwei Kriterien ab, von denen zumindest eines vom Nutzer gestaltet werden kann: 1. Wie werden die Provider die Präfixe vergeben (wobei das Präfix letztlich einen ähnlichen Informationsgehalt hat, wie die derzeitige IPv4-Adresse)? 2. Sind die Privacy Extensions aktiviert sind und wie sind sie konfiguriert?[137]

---

131 *Freund/Schnabel*, MMR 2011, 495, 496; Auf Mac OS X und Linux muss der User diese selbst einschalten, wie das geht erklärt *Endres*, c't 2011, 146, 147. Bei IPv6-tauglichen Geräten wie dem iPad, dem iPhone mit iOS ab Version 4 oder bei aktuellen Android-Handys, können hingegen die Privacy Extensions überhaupt nicht aktiviert werden.

132 *Endres*, c't 2011, 146.

133 *Freund/Schnabel*, MMR 2011, 495, 496; *Endres*, c't 2011, 146, 148.

134 So erklärten laut eines Berichts des Spiegel, Vodafone und Telekom, dass sie an einer dynamischen Adressvergabe für Privatkunden festhalten würden, *Reißmann* „Provider versprechen Datenschutz bei IPv6“, Spiegel online v. 4.5.2011, abrufbar unter: http://www.spiegel.de/netzwelt/web/0,1518,760274,00.html.

135 *Endres*, c't 2011, 146, 148.

136 *Endres*, c't 2011, 146, 148; auch IPv4-Adressen haben eine beschränkt geografische Aussagekraft, dazu *Heinson/Freiling*, DUD 2009, 547 ff.

137 Ähnlich auch *Endres*, c't 2011, 146, 148.

1.1.2.1.3 E-Mail – einer der meistgenutzten Dienste im Internet

Um E-Mails versenden zu können, benötigt der Benutzer zunächst ein elektronisches Postfach. Dabei handelt es sich meist um einen passiven Speicherbereich (ein Computer-Konto/ Account). Jede elektronische Mailbox hat eine eindeutige E-Mail-Adresse, die sich aus zwei Bestandteilen besteht, die durch ein @ verbunden werden. Im ersten Teil wird die Mailbox genannt und im zweiten der Computer, der für den Empfang der Daten zuständig ist, zusammensetzt – mailbox@computer.de.[138]

Über einen sogenannten Benutzeragenten können Nachrichten gelesen und gesendet werden. Benutzeragenten sind Mailprogramme, die die verschiedenen Befehle (Verfassen, Entgegennehmen und Beantworten von Nachrichten) annehmen. Die Übermittlung der Nachricht erfolgt dann, durch Nachrichtenübertragungsagenten.[139] Der Versand einer E-Mail läuft dann wie folgt ab: Zunächst wird die gesamte Nachricht in einen Umschlag gepackt. Der Umschlag beinhaltet alle Informationen, die zur Beförderung benötigt werden. Die Nachricht selbst umfasst zwei Teile: Einmal den Header, der die Steuerinformationen für die Benutzeragenten enthält, und zum anderen den Nachrichtenteil (auch als Body oder Rumpf bezeichnet), der allein für den Empfänger bestimmt ist.

Im Internet werden E-Mails zugestellt, indem eine TCP-Verbindung von der Quelle zu Port 25 oder einer SSL-Verschlüsselung zu Port 465 des Ziels aufgebaut wird.[140] Dafür ist jedoch wichtig, dass der Adressat auch erreichbar ist. Er muss online sein. Da der Client dies meist nicht ist, werden dafür heute in der Regel Nachrichtenübertragungsagenten eines Internetdienstanbieters genutzt. Diese nehmen für alle Kunden den Mail-Verkehr an, so dass man nicht persönlich online sein muss, um eine Nachricht erhalten zu können. E-Mails werden dort gespeichert und dann von einem Übertragungsagenten des Endkunden vom Nachrichtenübertragungsagenten des Internetdienstanbieters abgerufen.[141]

Die Kommunikation via E-Mail hat heute vielfach den Brief-Verkehr und in weiten Teilen auch die klassische Telefonie ersetzt. Beispielsweise ist gerade im geschäftlichen Bereich von großem Vorteil, dass bei einer E-Mail immer auch etwas Schriftliches vorliegt. Allerdings ist die Beweiskraft von E-Mails stark eingeschränkt.[142] Denn es handelt sich grundsätzlich um kein besonders sicheres Kommunikationsmittel. E-Mails können verloren gehen oder verändert werden. Mailboxen können gehackt und Nachrichten unter fremden Namen versendet werden. Aus diesem Grund wurde in Deutschland für eine sichere Kommunikation mittels E-Mail, De-Mail entwickelt.[143]

---

138 *Comer* 2002, 455 f.

139 *Tanenbaum* 2003, 642, 644 ff.

140 Dieser Port wird von einem E-Mail-Dämon, der SMTP (Simple Mail Transfer Protocol) spricht, abgehört, dies erklärt ausführlich *Tanenbaum* 2003, 655.

141 Als Protokolle werden hier POP3 und IMAP verwendet, dazu *Tanenbaum* 2003, 658 f.

142 *Roßnagel/ Pfitzmann* NJW 2003, 1209 ff.

143 Ziel von De-Mail ist es ein verbindliches, zuverlässiges und sicheres Versenden von elektronischer Post zu ermöglichen; BSI TR 01201 De-Mail. Zu den Funktionen vor allem Teil 3.1 (Postfach und Versanddienst; Funktionalitätsspezifikation); vgl. auch *Roßnagel/Hornung/Knopp,* DUD 2009,

1.1.2.1.4 Internet-Telefonie (VoIP)

Als Internet Telefonie oder auch IP-Telefonie oder Voice over IP (VoIP) wird das Telefonieren auf der IP-Infrastruktur, also über nach Internet-Standards aufgebaute Computernetzwerke, bezeichnet.[144] Sprache und Steuerungsinformationen werden dabei digitalisiert, also in Datenpakete umgewandelt, und über das Internet übertragen. IP-Telefonie könnte zukünftig die klassische Telefonie-Infrastruktur samt ISDN vollständig ersetzen.[145] Bereits Ende des Jahres 2010 telefonierten beinahe fünf Millionen Deutsche ausschließlich über Internet-Telefonie.[146] Insgesamt existieren derzeit noch beide Technologien parallel.[147]

Der Unterschied zur klassischen Festnetz-Telefonie besteht darin, dass es an sich keine geographisch fest zugeordneten Anschlüsse gibt. Vielmehr wird ähnlich wie bei der Mobilfunktelefonie erst durch eine Authentifizierung des Angerufenen seine momentane Adresse bzw. der aktuell genutzte Anschluss festgestellt. Es erfolgt insofern auch keine feste Zuordnung zu einer Rufnummer, sondern der Teilnehmer hinterlässt jeweils die aktuelle IP-Adresse bei einem Dienstrechner, die dann, wenn eine Verbindung aufgebaut werden soll, abgefragt wird, um so den Verbindungsaufbau zu ermöglichen. Die Sprache wird zunächst analog aufgezeichnet und dann in elektrische Signale umgewandelt.[148] Diese elektrischen Signale werden digitalisiert. In dieser Form werden sie dann direkt an die IP-Adresse des Gesprächspartners übermittelt.

1.1.2.1.5 Möglichkeiten anonymer Kommunikation im Internet

Grundsätzlich hinterlässt jede Handlung im Internet, ob der Aufruf einer Web-Seite, der Versand einer E-Mail oder die Nutzung von IP-Telefonie, digitale Spuren, die es zumindest in der Theorie ermöglichen jede Kommunikation im Netz einer bestimmten Person in der Offline-Welt zuzuordnen. Zudem können diese Spuren im Netz, wenn sie zusammengeführt werden, dem Nutzer ein Gesicht verleihen, wenn sie für eine Profilbildung genutzt werden. Entscheidend dafür ist, dass möglichst viele Daten vorhanden sind, um einen Nutzer zu identifizieren oder ein Profil zu bilden.

Umgekehrt bedarf es, um anonyme Kommunikation im Internet zu ermöglichen, technischer Maßnahmen, um die Spuren im Netz zu verwischen. Dazu dienen Anonymi-

---

728 ff.; *Roßnagel* NJW 2011, 1473; weitere Infos zu De-Mail sind auch abrufbar unter https://www.bsi.bund.de/DE/Themen/EGovernment/DeMail/DeMail_node.html; De-Mail-Gesetz vom 28.4.2011, BGBl. 2011 I, 666.

144 *Weise/Freiheit,* IT Labor Bnd. 2, 2010, 5; *Schnabel* 2008, 285; ausführlich zu den Grundlagen, Funktionsweise und den technischen Anforderungen bei VoIP *Badach* 2010.

145 *Mozek/Zendt,* in: *Hoeren/Sieber* 2012, Teil 23, Rn. 8 sehen die Internet-Telefonie auf dem „Siegeszug".

146 *Bundesnetzagentur* Jahresbericht 2010, erschienen am 6.4.2011, S. 72, abrufbar unter: http://www.bundesnetzagentur.de/SharedDocs/Downloads/DE/BNetzA/Presse/Berichte/2011/Jahresbericht2010pdf.pdf; hinzukommen 2,9 Mio. Anschlüsse über Kabel-TV-Zugänge. 2008 waren es noch lediglich 2,4 Mio. Anschlüsse über VoIP, so dass sich hier der Anteil der Nutzer quasi verdoppelt hat.

147 Zur Geschichte der Internet-Telefonie: *Mozek/Zendt,* in: *Hoeren/Sieber* 2012, Teil 23, Rn. 8 f.

148 Sie wird dabei auch komprimiert. Je stärker sie komprimiert wird, desto stärker leidet die Sprachqualität, *Schnabel* 2008, 287.

sierungsdienste und Remailer. Der Betrieb dieser Dienste ist nach geltendem Recht legal.[149] Anonymisierungsdienste sind auch für Staaten von großem Interesse. Sie werden beispielsweise von Botschaften genutzt.[150]

In Deutschland wurde mit staatlicher Förderung der Anonymisierungsdienst „Jon Donym" entwickelt.[151] Dieser ermöglicht anonymes Surfen indem die IP-Adresse verschleiert wird. Mittels fester Mix-Kaskaden aus zwei oder drei Knoten werden die Anfragen der einzelnen Nutzer gemixt, um eine Erkennung zu vermeiden. Erkennbar für eine Webseite ist daher nur die IP-Adresse der Mix-Kaskade und der eigentliche Nutzer ist nicht identifizierbar. Der Datenverkehr wird sodann mehrfach verschlüsselt. Der Anbieter wird von der *TU Dresden* zertifiziert. Um Missbrauch für die Verschleierung von Straftaten vorzubeugen, wurde die Möglichkeit implementiert, die Identität eines Nutzers zur Verfolgung schwerer Straftaten aufzudecken.[152] Ein Schwachpunkt eines Anonymisierungsdienstes mittels Mixkaskaden wie bei „Jon Donym" besteht darin, dass in der Praxis um funktionsfähig zu sein, nur bestimmte Mixfunktionen tatsächlich implementiert werden können.

Anonymes Surfen im Internet wird auch durch die Nutzung des bekannten Anonymisierungsdienstes „The Onion Routing" (TOR) ermöglicht.[153] Es handelt sich dabei um ein Netzwerk mit über 2000 Servern (Nodes), das auf einem anderen Konzept als „Jon Donym" beruht. Bei TOR werden von den über 2000 Nodes jeweils drei für eine Route ausgewählt. Diese wechseln etwa alle zehn Minuten. Dadurch, dass eine Route stets über drei Server vermittelt wird, bleibt selbst dann anonymes Surfen gewährleistet, wenn ein Teil der Nodes kompromittiert ist. Nur dann wenn alle Nodes überwacht werden sollten, kann keine Anonymität mehr erzeugt werden. Die Nutzung von TOR ist einfach. Es muss lediglich ein Client, der „Onion Proxy", auf installiert werden. Dieser stellt dann, wenn man eine Internetverbindung herstellen möchte, verschlüsselt eine Verbindung mit dem Tor-Netzwerk auf.

Anonymisierungsdienste können, zwar nur in gewissen Grenzen, aber dennoch zuverlässig eine anonyme Nutzung des Internets ermöglichen.

Für den anonymen Versand von E-Mails werden nicht Anonymisierungsdienste, sondern Remailer eingesetzt. Dabei handelt es sich um Internetdienste, die E-Mail-Nachrichten annehmen und diese pseudonym oder anonym weiterleiten, indem die Nachrichten entpersonalisiert werden. Ermöglicht wird dies, indem eine Nachricht über Remailer-Kaskaden verschickt wird. Vergleichbar ist dies mit dem Versand eines Briefes, der in mehrere Umschläge gesteckt wird, um auf diese Weise den Absender zu verschleiern. Jeder Empfänger innerhalb der Kaskade öffnet den Umschlag und

---

149 *Redeker* ITR 2012, Kap. D, Rn. 1187.

150 „Anonymisierungsdienste im Internet" v. 28.1.2010, S. 1, abrufbar unter: https://www.awxcnx.de/download/einfuehrung_anon_dienste.pdf.

151 „Anonymisierungsdienste im Internet" v. 28.1.2010, S. 1, abrufbar unter: https://www.awxcnx.de/download/einfuehrung_anon_dienste.pdf; *JonDonym GmbH,* http://anonym-surfen.de/.

152 Die Anforderungen der richterlichen Anordnung wurde jedoch von 2006-2010 nur ein Mal erfolgreich gestellt, vgl. Fn. 150 (S. 2).

153 https://www.torproject.org/.

sendet den darin enthaltenen Brief ohne Hinweise auf den vorherigen Absender weiter. Der letzte Remailer der Kaskade liefert dann den Brief an den Empfänger aus. Technisch basieren Remailer auf einer asymmetrischen Verschlüsselung.[154]

Soweit keine Anonymisierungsdienste eingesetzt werden ist es grundsätzlich möglich, an jedem Zwischen- und Endpunkt eines über das Internet abgewickelten Kommunikationsvorganges den Inhalt und die genauen Umstände der Kommunikation zu speichern (soweit sie nicht verschlüsselt wurden), da sämtliche Informationen für die erfolgreiche Übermittlung der Informationen erforderlich sind.[155] Dem Einsatz von Anonymisierungsdiensten kommt insofern zum Schutz der Vertraulichkeit der Kommunikation im Internet eine sehr hohe Bedeutung zu.

1.1.2.2 Mobilfunktechnologie

Mobile Telekommunikation beruht auf der Übertragung von Signalen über Mobilfunknetze. Jedes Mobilfunkgerät kommuniziert über eine Sendestation (Basisstationen, meist auf Sendemasten angebrachte Antennen) mit dem Mobilfunknetz – dem Vermittlungsteilsystem. Lediglich die Kommunikation zwischen dem mobilen Endgerät und der Basisstation erfolgt über Funk und insofern drahtlos. Die Kommunikation wird dann drahtgebunden über das GSM- UMTS- und zukünftig über das LTE-Netz geleitet.[156]

Der Bereich, den jede Basisstation mit seinen Antennen erfasst, wird als Funkzelle bezeichnet.[157] Dabei unterscheidet sich deren Größe stark. So gibt es etwa in Stadtgebieten Funkzellen mit einem Durchmesser von nur wenigen 100 Metern, während es im ländlichen Bereich zum Teil sehr große Funkzellen gibt, die teilweise eine Ausdehnung von wenigen Kilometern erreichen.[158] Sie sind auch nicht kreisförmig oder quadratisch aneinandergereiht, sondern variieren nach Größe und Form.

Soweit ein Mobiltelefon sich in einer Funkzelle bewegt, wird es von dem Sendemast, der Basisstation dieser Zelle, kontrolliert. Das heißt, sie kommuniziert mit und über diese Basisstation. Da sich die Funkzellen zum Teil überschneiden, wird stets die Basisstation und damit die Zelle ausgewählt, die über die stärkste Sendeleistung im Augenblick verfügt.[159]

Sobald ein Mobiltelefon eine Zelle verlässt, stellt die Basisstation fest, dass sich das Signal des Telefons entfernt. Sie fordert dann von den benachbarten Basisstationen die Information an, wie hoch die Signalstärke bei Ihnen ist. Die Basisstation übergibt die Zuständigkeit dann an die Zelle, die das stärkste Signal empfängt, das ist diejenige, die am nächsten zum Aufenthaltsort des Mobilfunkgeräts steht.[160]

---

154 *Mix1* v. 28.1.2010, „Remailer“, abrufbar unter: https://www.privacyfoundation.de/wiki/Remailer.
155 *Sievers* 2002, 76.
156 *Freiling* 2009, 9.
157 *Freiling* 2009, 9; *Tanenbaum* 2003, 179 f.
158 *Freiling* 2009, 9.
159 *Freiling* 2009, 10.
160 *Tanenbaum* 2003, 179 f.

Eine oder mehrere Funkzellen werden in geographische Bereiche zusammengefasst, die von einer Mobilvermittlungsstelle verwaltet werden. An diese sind regional verteilt sogenannte Heimatdateien angegliedert. Dabei handelt es sich um eine Datenbank, in der Teile der Kundendaten wie Name und Telefonnummer, Betriebszustand, aktueller Aufenthaltsort, Roaming-Nummer der Mobilfunkstation, etc. des Teilnehmers gespeichert werden. Jeder Teilnehmer wird nur in einer Heimatdatei geführt.[161]

1.1.2.2.1 Mobilfunkkennungen: IMSI, TIMSI und IMEI

Mobilfunkgeräte verfügen über eine Kennung, die jedem Gerät international eindeutig zugewiesen ist: die *International Mobile Equipment Identity*, kurz IMEI. Sie besteht aus mehreren Feldern, in denen der Hersteller und das Modell beschrieben sind sowie einer Seriennummer.[162] Diese hat eine mit der MAC-Adresse eines Rechners in einem lokalen Netzwerk vergleichbare Funktion.[163] Ihre Manipulation ist jedoch schwieriger als die einer MAC-Adresse.[164] Die 15stellige IMEI ermöglicht dem Kunden bei Diebstahl seines Mobilfunkgerätes, eben dieses sperren zu lassen. Darüber hinaus wird sie vielfach benötigt, um ein Sim-Lock zu entfernen. Für die unmittelbare Kommunikation hat die IMEI keine Bewandtnis.[165]

Vielmehr wird für die Kommunikation in GSM- und UMTS-Mobilfunknetzen für die eindeutige Identifizierung von Netzteilnehmern eine IMSI (*International Mobile Subscriber Identity*) vergeben, die jeweils auf der SIM-Karte gespeichert wird. Die IMSI-Nummer wird weltweit einmalig pro Kunde vergeben.[166] Beim Aufbau einer Mobilfunkverbindung wird der Teilnehmer bei einer Funkverbindung durch eine temporäre Funkkennung, die die IMSI des Teilnehmers verschleiert und durch die TMSI (*Temporary Mobile Subscriber Identity*) identifiziert. Diese wird von der Mobilvermittlungsstelle vergeben und wechselt periodisch oder sobald der durch die Mobilvermittlungsstelle kontrollierte Sendebereich verlassen wird.[167]

1.1.2.2.2 SMS & MMS-Versand im GSM-Netz

Die Funktionsweise des Versands von Kurznachrichten (*Short Messaging Service,* SMS) mit (Mobil-)Telefonen im GSM-Netz ist mit dem E-Mail-Versand vergleichbar. Kurznachrichten, deren Adressaten einer Mobilstation zuzuordnen sind, werden von einem SMS-Betriebszentrum (*Short Messaging Service Center*, SMSC) zwischengespeichert. Durch Kontaktaufnahme mit dem Mobilgerät werden die Nachrichten dann an den genauen Adressaten übermittelt. Die Übermittlung einer Kurznachricht an ein Mobilgerät erfolgt dann ähnlich wie die Annahme eines Anrufs.[168] Eine Signalisierungsnachricht mit der TMSI des SMS-Empfängers wird an alle Mobilstationen im ak-

---

[161] *Freiling* 2009, 9 ff.
[162] *Freiling* 2009, 11.
[163] Fn. 162.
[164] Fn. 162.
[165] Fn. 162.
[166] Diese enthält zum einen eine Länderkennzeichnung sowie eine Kennung zur Identifizierung der Heimatdatei und des Netzbetreibers sowie des jeweiligen Kunden, *Freiling* 2009, 10.
[167] Fn. 162.
[168] Fn. 162.

tuellen Aufenthaltsbereich gesendet. Sobald der Empfänger der Basisstation geantwortet hat, wird die Mitteilung über eine verschlüsselte Verbindung übertragen.[169]

SMS werden nicht nur für den Versand privater Kurznachrichten verwendet. Beispielsweise nutzt auch das Mautsystem Toll Collect SMS-Technologie. Toll Collect ermöglicht die automatische Mauterhebung.[170] Dafür sind in den Lastkraftwagen „Fahrzeuggeräte" angebracht (*Onboard Unit*, OBU). Diese enthalten neben einem GPS-Empfangsgerät ein GSM-Mobiltelefon. Mit Hilfe der GPS-Satellitensignale erkennt das Fahrzeuggerät die Positionen und gleicht diese mit im Gerät gespeicherten Karten aller mautpflichtigen Straßen ab. Wenn sich der Lastkraftwagen auf einer mautpflichtigen Bundesfernstraße befindet, wird zunächst eine Übereinstimmung festgestellt. Anhand dieser werden dann auf Grundlage der zurückgelegten mautpflichtigen Streckenabschnitten, der Achs-Zahl und der Schadstoffklasse des jeweiligen Lkw die Gebühren berechnet. Die Daten werden dann in regelmäßigen Abständen per SMS an das Rechenzentrum versandt.[171]

1.1.2.2.3 Mobiles Internet

Die Mobilfunktechnik hat sich rasant fortentwickelt. Auf dem Markt sind heute – gut 60 Jahre nach ihrer Einführung – Mobiltelefone der dritten Generation: Geräte, die sowohl digitale Sprachtelefonie ermöglichen als auch den Versand von Daten.[172]

Die Entwicklung des mobilen Internets ist eng mit der Entwicklung der Mobilfunktechnik verknüpft. Unter mobilem Internet versteht man die Möglichkeit, mittels mobiler Endgeräte, vielfach sogenannte Smart-Phones, das Internet (vornehmlich das WWW) zu nutzen.[173] Erstmals möglich wurde der Zugang zum Internet mittels Mobiltelefon bereits in den 1990er Jahren. Damals allerdings noch mit sehr geringer Geschwindigkeit. Erst die Einführung von UMTS im Jahr 2002 und dessen Weiterentwicklung HSPA (*High Speed Downlink Packet Access*)[174] wurde es etwa ab dem Jahr 2006 ermöglicht mit annehmbaren Geschwindigkeiten im Internet zu surfen. Seit der Umstellung der Mobilfunknetze auf UMTS[175] bzw. HSPDA und HSUPA (*High Speed Uplink Packet Access)* und der zeitgleichen Weiterentwicklung der mobilen Endgeräte,

---

169 Fn. 162.

170 http://www.toll-collect.de/home.html.

171 Die Kontrollbrücken an Autobahnen dienen lediglich dazu passierende LKWs stichprobenartig zu fotografieren, um die mautrelevanten Angaben zu überprüfen. Ausführlich zum Entstehen von Verkehrsdaten im Rahmen von Toll-Collect, *Freiling* 2009, 12 f.

172 In jeder Generation kommen andere Technologien zum Einsatz (1. analoge Sprache; 2. Digitale Sprache; 3. Digitale Sprache und Daten (Internet, E-Mail)), *Tanenbaum* 2003, 177.

173 Ausführlich zum Mobilen Internet und dessen Entwicklungsgeschichte auch http://de.wikipedia.org/wiki/Mobiles_Internet (30.10.2012).

174 Zu diesem gehören zwei Protokollzusätze: HSDPA für den Downlink und HSUPA für den Uplink. Etwa seit 2007 bauen in Deutschland die Netzbetreiber ihr Netz HSUPA fähig aus. Die Telekom hat dies bereits abgeschlossen. Zur Funktionsweise und der gesteigerten Leistung ausführliche Informationen unter *Schnabel* Elektronik-Kompendium, „HSPA", abrufbar unter: http://www.elektronik-kompendium.de/sites/kom/1301141.htm.

175 Akz. für Universal Mobile Telecommunication System.

erfreut sich das mobile Internet wachsender Beliebtheit. So gingen im Jahr 2010 bereits 26 Prozent der Handynutzer mit diesem auch online.[176]

Diese Entwicklung ist noch lange nicht beendet. Aktuell wird die dritte UMTS-Generation durch den neuen Mobilfunkstandard LTE (*Long Term Evolution)* abgelöst, indem dieser nunmehr flächendeckend ausgebaut wird.[177] Mit diesem werden die Handynetze um ein zehnfaches schneller – zugleich kommen erste Endgeräte auf den Markt.[178]

Auch beim mobilen Surfen im Internet, wird dem Endgerät eine IP-Adresse zugewiesen.[179] Da diese vorwiegend nur für einen kurzen Zeitraum vergeben werden und der IPv4-Adressraum stark beengt ist, werden mobilen Endgeräten nur IP-Adressen aus dem privaten Bereich zugewiesen, die dann per NAT[180] auf gemeinsamen öffentlichen IP-Adressen abgebildet werden. Das heißt, alle gleichzeitig ins Internet eingebuchten Mobilgeräte werden in IP-Pools aufgeteilt und jeder Pool erzeugt über eine einzige öffentliche IP-Adresse mit dem öffentlichen Internet eine Verbindung.[181]

Dies gilt allerdings nur für allein IPv4-taugliche Geräte. IPv6-taugliche Endgeräte wie iPad, iPhone oder aktuelle Android-Handys nutzen automatisch IPv6 im WLAN. Ein Internetzugang via NAT ist hier nicht mehr erforderlich, sondern es erfolgt eine eindeutige Adressierung mit einer bestimmten IP-Adresse.[182] Auch eine Anonymisierung oder Pseudonymisierung mittels Privacy Extensions scheidet hier aus, da diese bei den Geräten vielfach überhaupt nicht aktiviert werden können.[183]

1.1.2.3 Spuren im Netz

Wer durch eine Straße läuft und sich Schaufenster ansieht, wird, sollte er unbeobachtet sein, keine Spuren hinterlassen. Ganz anders im Internet, wer etwa eine Internet-Seite besucht, hinterlässt Spuren im digitalen Netz. Es kommt insofern nur darauf an, ob diese Daten auch gespeichert sind. Und wenn sie gespeichert sind, ob auf sie zugegriffen werden kann und darf. Letztlich ist eine anonyme Nutzung des Internet nur dann möglich, wenn durch die Nutzer aktive Maßnahmen getroffen werden, um Spuren zu verhindern oder dafür zu sorgen, dass die technisch notwendig hinterlassenen Spuren nicht miteinander kombiniert werden können.[184] Dies gilt insbesondere soweit eine Pflicht zur Speicherung von Telekommunikationsverkehrsdaten auf Vorrat besteht –

---

176 *Geißlitz* „TNS Convergence Monitor“, Pressemitteilung v. 7.9.2011, abrufbar unter: http://www.tns-infratest.com/presse/presseinformation.asp?prID=816; 19 Prozent der Befragten gaben an, privat ein Smartphone zu nutzen.

177 *Briegleb,* heise online v. 16.8.2012, abrufbar unter: http://www.heise.de/-1668714.html.

178 *Spier,* heise online v. 13.1.2012, abrufbar unter: http://www.heise.de/-1412596.html.

179 Vgl. dazu oben S. 25 f.

180 Vgl. dazu oben Fn. 120.

181 *Zivadinovic,* heise mobil, „Es kann nur einen geben“ v. 29.3.2010, abrufbar unter: http://heise.de/-954840, S. 4, „NAT-Probleme"

182 *Meyer/Behrens,* c't 5/2012, 180 ff.

183 *Freund/Schnabel*, MMR 2011, 495.

184 *Brunst* 2009, 35.

hier gehen die letzten Möglichkeiten der anonymen und pseudonymen Nutzung des Internets verloren.[185]

Insgesamt sind riesige Datensammlungen durch die zunehmende Digitalisierung und den Einsatz von Internet-basierter Kommunikation in den verschiedensten Lebensbereichen entstanden.[186] Welche enormen Mengen an personenbezogenen Kommunikationsdaten verarbeitet werden, wird deutlich an dem Rechenzentrum, welches der amerikanische Geheimdienst NSA in den USA aufbaut.[187]

Die digitalisierten Informationen enthalten zum Teil höchst persönliche Informationen. Zudem lassen sich aus der Analyse digitaler Daten zahlreiche Informationen ableiten. Es konnte aufgezeigt werden, dass Verkehrsdaten von Mobiltelefonen über einen Zeitraum von drei Monaten genügen, um den Aufenthaltsort eines Handynutzers zu einem beliebigen Zeitpunkt mit einer Wahrscheinlichkeit von 93 Prozent vorauszusagen.[188] Auch lassen sich aus einer umfassenden Mobilfunkdatenanalyse 95 Prozent aller tatsächlich bestehenden Freundschaften ermitteln.[189] Darüber hinaus ermöglicht die Analyse von Mobilfunkdaten nicht nur Rückschlüsse auf einzelne Personen, sondern auch auf Ereignisse. So wurde aufgezeigt, dass Anrufmuster eine Art „Soziometer" bilden und Rückschlüsse auf bestimmte Ereignisse ermöglichen.[190] So wie das Telefonverhalten ermöglicht auch eine Analyse des Surfverhaltens zahlreiche Rückschlüsse auf den jeweiligen Nutzer. Durch die Digitalisierung des Alltagslebens entsteht ein digitales Abbild des Bürgers. Es gibt zwar technische Möglichkeiten, Spuren zu verwischen, gänzlich verhindern lassen sie sich aber nicht.

1.1.3 Digitalisierung von Freiheit und Sicherheit

Die technischen Innovationen eröffnen neue Freiheitsräume, aber auch neue Kontroll- und Überwachungsmöglichkeiten. Dies hat dazu geführt, dass sich die Verwirklichungsbedingungen von Freiheit und Sicherheit grundlegend verändert haben. Es wird im Folgenden erörtert, inwiefern die digitale Revolution Freiheiten eröffnet oder beschränkt und inwieweit Sicherheit dadurch gesteigert oder gefährdet wird.

---

185 *Orantek*, NJ 2010, 193, 194.

186 Laut Medienberichten aus dem Jahr 2008 produziert der Mensch zu dieser Zeit 1 Terabyte Daten pro Jahr, http://www.netzeitung.de/internet/1148020.html.

187 *Klinger,* ZDnet v. 19.3.2012, abrufbar unter: http://www.zdnet.de/41560992/nsa-baut-2-milliarden-dollar-teures-rechenzentrum/.

188 *Song/Zehui/Blumm/Barabási*, Limitis of Preditability in Human Mobility, Science 2010, Vol. 327, 1018 ff.

189 Bei dieser Studie des MIT-Forschers *Alex Pentland* wurden die Testteilnehmer nicht nur via Handy überwacht, sondern auch befragt mit wem sie befreundet sind. Um die Nähe von Personen zueinander automatisiert zu analysieren, nutzen die Forscher die Bluetooth-Funktion der Mobiltelefone; *Eagle/Pentland/Lazer* 2009, 15274; dazu auch *Langfeldt,* „Aussagekraft von Verkehrsdaten: Rekonstruktion sozialer Netzwerke möglich", Virtuelles Datenschutzbüro v. 28.4.2008, abrufbar unter: http://www.datenschutz.de/news/detail/?nid=2674.

190 *Darnbeck, H.,* Wie Handy-Daten-Schnüffelei und helfen kann, Spionage in guter Mission. Der Spiegel v. 15.7.2011, abrufbar unter http://www.spiegel.de/wissenschaft/mensch/0,1518,771085,00.html.

1.1.3.1 Anonymität und Privatheit im digitalen Zeitalter

Die Nutzung moderner Technologien, die unweigerlich mit der Verarbeitung personenbezogener Daten verknüpft ist, hat insgesamt zu einer Desensibilisierung in Bezug auf die Verarbeitung personenbezogener Daten und den Anspruch und die Wertung von Privatem generell geführt.

Während in den Neunzigern noch vielfach eine grundlegende Abwehrhaltung gegen einzelne Technologien zu erkennen war, haben sich diese trotz datenschutzrechtlicher und gesundheitlicher Bedenken, wie das Beispiel der Mobiltelefonie veranschaulicht, gesamtgesellschaftlich durchgesetzt.[191] Die hier zu Tage tretende Diskrepanz zwischen der abstrakter Bewertung und ihrer praktischen Nützlichkeit, die zur Verwendung führt, zeigt sich auch in anderen Bereichen: So wurde etwa im April 2011 bekannt, dass das iPhone die Bewegungen seiner Nutzer speichert und diese auch automatisch ausgelesen werden.[192] Dies hatte für kurzzeitige Empörung gesorgt, zu einem Boykott des iPhones oder ähnlichem hat dieser Datenschutz-Fauxpas aber bei Weitem nicht geführt.[193] Auch in der Diskussion um google-Streetview zeigt sich die beschriebene Diskrepanz zwischen Empörung und Verhalten. Die Einführung löste in Deutschland heftige Proteste aus, obwohl doch viele der sich empörenden Google-Mail nutzen und hier viel sensitivere Informationen erhoben und verarbeitet werden. Dieses Verhalten lässt den Schluss zu, dass in der Praxis die Nützlichkeit von bestimmten Instrumenten geeignet ist, datenschutzrechtliche Bedenken auszustechen.[194]

Darüber hinaus besteht die grundlegende Schwierigkeit für jeden Einzelnen, überhaupt zu erfassen, welche Anwendung, welche Daten erhebt und wie sie weiterverwendet werden. Vielfach sind sich die Nutzer nicht darüber im Klaren, welche Informationen sich aus der Analyse ihrer Handy-Daten, ihres Surfverhaltens oder der von ihnen im Netz freigegebenen Informationen ergeben.[195]

---

[191] *Darnbeck, H.,* Wie Handy-Daten-Schnüffelei und helfen kann, Spionage in guter Mission. Der Spiegel v. 15.7.2011, abrufbar unter http://www.spiegel.de/wissenschaft/mensch/0,1518,771085,00.html

[192] *Pete Warden* und *Alasdair Allan* entdeckten die bis dato versteckte und nicht bekannte Software auf dem iPhone (http://petewarden.github.com/iPhoneTracker/); vgl. dazu: *Becker,* heise online v. 20.4.2011, abrufbar unter: http://www.heise.de/-1231120.html.

[193] Vielmehr hatte der Hersteller Apple im selben Quartal den Absatz des Smartphones sogar um über 140 Prozent auf 20,3 Millionen Stück steigern können (Vorjahresquartal: 8,4 Millionen), *Briegleb* v. 20.7.2011, abrufbar unter: http://www.heise.de/-1282263.html.

[194] *Bernau,* „Gläsern und faul" Kommentar SZ v. 3.11.2012, „Längst ist da eine Generation herangewachsen, die – anders als ihre Eltern und Großeltern – nicht mehr erlebt hat, was passieren kann, wenn leichtfertig preisgegebene Informationen in die falschen Hände geraten. Sie kann es sich nicht einmal mehr vorstellen. Sie sind gern bereit, für die neuen Bequemlichkeiten mit persönlichen Daten zu zahlen. Hauptsache umsonst. Denn im selben Maße, wie die Vorstellung eines gläsernen Bürgers an Schrecken verliert, gewinnen all die kostenlosen Apps an Reiz".

[195] Insofern ist durchaus der Ruf nach verbesserter Aufklärung richtig und wichtig. Jugendliche sind sich vielfach nicht darüber im Klaren, dass die Daten, die sie etwa von sich im Vollsuff im Internet einstellen, einen potentiellen späteren Arbeitgeber davon abhalten könnten, sie einzustellen. Das Bewusstsein, dass „das Netz nichts vergisst", muss insofern geschult werden und wie datenschutzgerecht Online-Dienste genutzt werden können.

Hinzukommt, dass die Spuren, die man quasi beiläufig im Internet hinterlässt, vielfach zu vernachlässigen sind, im Vergleich zu den persönlichen Informationen, die bewusst und freiwillig ins Internet gestellt werden. Das Internet ist Spielwiese für die Selbstdarstellung, die ganz generell stetig an Bedeutung zunimmt.[196] Sie wird heute in vielen Bereichen als notwendig erachtet. Sie ist prägender Bestandteil des sozialen Lebens geworden. Geburtstagseinladungen, neue Adressen, der aktuelle Aufenthaltsort und was man gerade isst, all das und noch viel mehr wird heute in sozialen Netzwerken veröffentlicht.[197]

Der Frage, ob in Zeiten der Selbstdarstellung und -entblößung im Internet nicht datenschutzrechtliche Bedenken obsolet geworden sind, liegt der Gedanke zu Grunde, der unter dem Schlagwort „Post-Privacy" zeitweise Aufmerksamkeit erregte.[198] Datenschutz, wie wir ihn heute kennen, sei überholt. Aufgrund der globalen Vernetzung, den Grenzen der staatlichen Handlungsfähigkeit im Internet und dem Voranschreiten der Technik sei Datenschutz nicht mehr realisierbar. Datenschutz würde eine vermeintliche Sicherheit vermitteln, die faktisch nicht vorhanden sei. Erforderlich sei vielmehr, dass sich der Einzelne selbst schützt. Er sei verantwortlich für den Schutz seiner Privatsphäre im Internet, die er selbst durch den Einsatz technischer Mittel erzeugen könne. Staatliche Regulierung im Internet sei zum Scheitern verurteilt. Die Post-Privacy-Bewegung wendet sich insofern nicht, wie vielfach missverstanden wurde, generell gegen den Gedanken von Privatheit, sondern gegen den Datenschutz. Datenschutz sei „ein vermeintlich richtiges Feigenblatt in einer falschen Welt. (…) Die Utopie zu formulieren, eine Welt zu wollen, die diesen Schutz nicht benötigt – das muss das Ziel sein."[199]

Den Ursprung dieser These, dass Privatheit unter den Bedingungen moderner Datenverarbeitung überholt sei, machen *Kurz/ Rieger* bei den drei großen Unternehmen der Internetwirtschaft aus: Google, Apple und Facebook. Denn der Erfolg dieser drei Internetgiganten hängt wesentlich davon ab, wie viele Daten ihnen zur Verfügung stehen.[200] So proklamierte etwa der Gründer von facebook *Zuckerberg:* „privacy is no longer a social norm".[201]

Im alltäglichen Off-Line-Leben sind vielfältige Handlungen ohne Identifizierung und auch ohne nachträgliche Identifizierbarkeit möglich – erst die Weiterentwicklung im Bereich der Datenspeicherung und -verarbeitung ermöglicht bei Handlungen im Inter-

---

196 Immer wieder wird in Zeiten des Web 2.0. der Hang zum digitalen Exhibitionismus diskutiert, von einem digitalen Striptease wird gesprochen, *Kerkmann* „Digitaler Striptease nimmt zu", Südkurier v. 16.8.2007, abrufbar unter: www.suedkurier.de/2753465; *Nazari-Khanachayi*, JA 2010, 761.

197 Facebook ist dabei zum zentralen sozialen Netzwerk geworden und entwickelt immer mehr Funktionen mit denen immer mehr Lebensfelder erfasst werden, als Beispiel sei nur der „Gefällt-Mir-Button" genannt. Dazu auch ausführlich *Kurz/Rieger* 2011, 13 ff.

198 *Reißmann* „Privatssphäre ist sowas von Eighties", Spiegel Online v. 10.3.2011, abrufbar unter: http://www.spiegel.de/netzwelt/netzpolitik/0,1518,749831,00.html.

199 *Schramm* v. 22.3.2011, abrufbar unter: http://www.juliaschramm.de/2011/03/.

200 *Kurz/Rieger* 2011, 87 ff.

201 *Johnson,* the guardian, v. 11.1.2010, abrufbar unter: http://www.guardian.co.uk/technology/2010/jan/11/facebook-privacy.

net, theoretisch jedes Verhalten einer bestimmten Person zuzuordnen. Ob eine Handlung unter Beobachtung oder anonym erfolgt, ist aber von großer Bedeutung. Beobachtung kann Handlungen beeinflussen. Zwar verhält sich der Einzelne nicht zwingend unter Beobachtung anders. Nicht zu bestreiten ist aber, dass das Wissen um eine Beobachtung das Handeln beeinflussen kann und auch vielfach tatsächlich beeinflusst wird.[202] Dass alles Handeln nachvollzogen werden kann, war im Offline-Leben undenkbar. Die Möglichkeit anonym zu Handeln ist vielfach wesentlich für die Ausübung von Freiheiten. Zum Teil wird so auch ein Grundrecht auf Anonymität formuliert.[203] Schließlich wird der Rückzug ins Private auch als zentral für die Selbstentfaltung des Menschen erachtet.

Doch ist auch zu beachten, dass sich die Vorstellungen von Privatheit verändern. Während für Erwachsende klassisch die Wohnung als Innerer Bereich der Privatsphäre verstanden wird, nämlich weil er gänzlich ihrer Kontrolle unterliegt, ist für Kinder diese kein privater Raum – sie haben über sie auch keine Macht. „Online dagegen haben sie viel eher das Gefühl, privat zu sein, beziehungsweise sie haben gelernt, mit dem, was sie preisgeben, sehr gezielt den Zugang zu einem Online-Raum zu kontrollieren“.[204]

Die Bedingungen moderner Datenverarbeitung bedrohen Anonymität und Privatheit des Einzelnen, denn sie müssen erst hergestellt werden, da die digitale Kommunikation dem Grunde nach vollständig nachvollziehbar ist. Um das Internet als freies Netz und vor allem die Freiheit im Netz zu erhalten, bedarf es Vorkehrungen, Maßnahmen zum Schutz der Freiheit im Internet. Erforderlich ist dabei auch Eigeninitiative der Nutzer.[205]

1.1.3.2 Das Internet als Motor der Freiheit und als Kontrollinstrument

Dem Internet kommt nicht nur im Bereich der Selbstdarstellung eine herausragende Stellung zu, auch hat es die Möglichkeiten der Meinungsäußerung vereinfacht und vervielfacht. Das Internet ist so zu einem Instrument geworden, mit welchem unterdrückte Minderheiten, politische Randgruppen oder politisch Verfolgte ihre Kritik einer breiten Öffentlichkeit zugänglich machen können. Es ist so auch zum Motor der Freiheit geworden.

Wie groß die Bedeutung des Internets für die Freiheitsbewegungen ist, wurde insbesondere im Rahmen der Umbrüche in der arabischen Welt 2010/2011 deutlich.[206] Das Internet wurde hier zu einem zentralen Mittel im Freiheitskampf. Zwar wird immer

---

[202] So zeigen sogar physikalische Versuche, dass die Beobachtung die Wirklichkeit verändert, http://idw-online.de/pages/de/news391; auch der Sozialphilosoph *Foucault* argumentierte in Bezug auf die Überwachung von Gefangenen in einem theoretischen Experiment, dass die Hauptwirkung des Panoptikums darin bestünde, „die Schaffung eines bewußten und permanenten Sichtbarkeitszustandes beim Gefangenen, der das automatisierte Funktionieren der Macht sicherstellt“, *Foucault* 1993, 258.

[203] *Brunst* 2009, 280, 320 ff.

[204] *Glaser,* „Seid Netz zueinander!“, c’t soziale netze 2/2012, 8, 12.

[205] Vgl. auch *Brunst* 2009, 514 ff.

[206] *Noll* „Revolution online, Das Internet und der Umbruch in der arabischen Welt“, Sendung v. 19.7 2011, abrufbar unter: http://www.dradio.de/dlf/sendungen/hintergrundpolitik/1488785/.

wieder versucht, durch Kontrolle sozialer Netzwerke, das Ausforschen von YouTube-Videos, das Sperren bestimmter Seiten, eine staatliche Kontrolle über das Internet herzustellen. Eine vollständige Kontrolle ist jedoch auf Grund der dezentralen Struktur des Internets letztlich nicht möglich. Kontrolle ist vielmehr davon abhängig, ob die Betreiber der Angebote, über die kommuniziert wird, mit staatlichen Stellen kooperieren.

Ein Blick auf die *Volksrepublik China* zeigt jedoch, dass durchaus eine weitgehende Kontrolle des Internets realisierbar ist.[207] Auch gibt es mittlerweile zahlreiche Unternehmen, die sich darauf spezialisiert haben, Lösungen für die Überwachung der Kommunikation im Internet zu entwickeln.[208] Letztlich ermöglicht das Internet es gerade, da es zentrales Informationsorgan für weite Teile der Bevölkerung und auf Grund seiner Funktion auch Basis für die Organisation von Versammlungen und politischem Protest ist, auch die Bevölkerung zu überwachen und zu kontrollieren. Schließlich hinterlässt jede Handlung im Netz digitale Spuren.[209] So wurden etwa im arabischen Frühling vielfach Netzaktivisten Opfer staatlicher Repression.[210] Das Internet kann so, wie es Motor der Freiheit ist, auch mächtiges Überwachungs- und Kontrollinstrument sein.

1.1.3.3 Neue oder veränderte Formen der Kriminalität

Mit der Verbreitung des Internets innerhalb der Bevölkerung und in allen Lebensbereichen hat es auch Einzug gehalten in die Welt der Kriminalität.[211] So eröffnet die Informationstechnologie mit neuen Instrumenten zur Informationsverarbeitung und Kommunikation neue Wege der Organisation und Durchführung von Straftaten.[212] Auch sind neue Formen der Kriminalität entstanden, wie etwa Viren- und Hackerangriffe oder Computerbetrug. Diese neuen Formen der Kriminalität werden als Informations- und Kommunikationskriminalität (Abk.: IuK-Kriminalität) bezeichnet. Zur IuK-Kriminalität zählen Computerbetrug (§ 263a StGB), Betrug mit Zugangsberechtigungen zu Kommunikationsdiensten, Fälschung beweiserheblicher Daten (§§ 269 StGB),

---

[207] In China wurde eine umfassende Internet-Zensur aufgebaut. Errichtet wurde eine „Great Firewall of China", die etwa mittels Blockade von IP-Adressen und dem Filtern und Blockieren von Schlüsselbegriffen durch Backbone Provider eine weitgehende Kontrolle des Datenverkehrs im Internet ermöglicht. Wesentlich für die Kontrollierbarkeit ist die Zusammenarbeit von privaten Konzernen mit der chinesischen Regierung, dazu etwa *Briegleb,* heise online v. 25.11.2009, abrufbar unter: http://www.heise.de/-868608.html.

[208] Zur Unterstützung des *Gaddafi*-Regimes in Libyen bei der Überwachung des Internets und die erfolgte Unterstützung durch ausländische Unternehmen, *Haupt,* heise online v. 30.4.2011, abrufbar unter: http://www.heise.de/-1333681.html.

[209] Vgl. oben Kap. 1.1.2.3.

[210] So wurde der ägyptische Blogger *Maikel Nabil Sanad* zu zwei Jahren Haft verurteilt auf Grund eines kritischen Blogeintrags verurteilt, dies kritisieren *Reporter ohne Grenzen,* Pressemitteilung v. 15.12.2011, abrufbar unter: http://www.reporter-ohne-grenzen.de/presse/pressemitteilungen/meldung-im-detail/artikel/rog-kritisiert-verurteilung-des-bloggers-maikel-nabil-sanad-zu-zwei-jahren-haft/.

[211] *Sievers*, 2002, 26.

[212] *Roßnagel* 2011b, 36; Es wurde bereits darauf verwiesen, dass mit digitalen Gütern insbesondere das Urheberrecht vor neue Herausforderungen gestellt wurde, vgl. oben Fn. 80.

Täuschung im Rechtsverkehr bei Datenverarbeitung (§ 270 StGB), Datenveränderung und Computersabotage (§§ 303a, 303b StGB) sowie Ausspähen, Abfangen von Daten (§ 202 StGB).

In der Kriminalitätsstatistik wird die Computerkriminalität aufgeführt. Darunter werden neben den IuK-Delikten alle Straftaten zählen bei denen die EDV zur Planung, Vorbereitung oder Ausführung der Tat eingesetzt wurde, sowie das Herstellen, Überlassen, Verkaufen, Verbreiten, Verschaffen oder zugänglich machen sogenannter „Hacker-Tools", welche darauf angelegt sind, „illegalen Zwecken zu dienen" (§ 202c StGB).

Die Fallzahlen im Bereich Computerkriminalität sind steigend. Im Jahr 2010 stiegen sie im Vergleich zum Vorjahr um 12,6 Prozent auf 84.377 Fälle. Die Aufklärungsquote lag im Jahr 2010 bei 35,8 Prozent.[213] Trotz dem deutlichen Anstieg an Delikten, liegt der Anteil der Computerkriminalität an den in der Kriminalstatistik erfassten Fällen insgesamt bei lediglich 1,42 Prozent (2011 wurden insgesamt 5 933 278 Straftaten registriert). Auch in der PKS 2012 ist die Tendenz im Bereich der Computerkriminalität weiter steigend. Es wurden nunmehr 87.871 Vergehen im Vergleich zu 84.981 im Jahr 2011 erfasst (Steigerung um 3,4 Prozent).[214]

Bezüglich des hohen Anstiegs an registrierten Fällen seit 2007 ist darauf hinzuweisen, dass diese auch auf dem Einsatz neuer Software, mit der strafrechtlich relevante Handlungen im Internet systematisch technisch gesichert werden können, basiert.[215] Der Anteil an Straftaten, die mit dem Tatmittel Internet begangen wurden, lag im Jahr 2012 mit 229.408 Fällen bei etwa 4,09 Prozent.

Überwiegend werden mit dem Tatmittel Internet Betrugsdelikte (2012: 70,8 Prozent) begangen. Die Verbreitung pornographischer Schriften über das Internet bewegt sich mit 2,2 Prozent in einem niederen Bereich.

Die Aufklärungsquote sowohl für den Bereich der Computerkriminalität als auch der IuK-Kriminalität ist 2012 im Gegensatz zu 2011 leicht zurückgegangen. Sie liegt aktuell bei 29,9 bzw. 26,5 Prozent.[216]

---

213 *Bundesministerium des Inneren,* Polizeiliche Kriminalstatistik 2010, S. 4, veröffentlicht am 20.5.2011, abrufbar unter: http://www.bmi.bund.de/SharedDocs/Downloads/DE/Broschueren/2011/PKS2010.pdf; für IuK-Kriminalität lag die Aufklärungsquote bei 33 Prozent. Im Vergleich dazu lag insgesamt die Aufklärungsquote im Jahr 2010 bei 56 Prozent.

214 *Bundesministerium des Inneren,* Polizeiliche Kriminalstatistik 2012, S. 70; abrufbar unter: http://www.bmi.bund.de/SharedDocs/Downloads/DE/Broschueren/2013/PKS2012.html?nn=3314802.

215 *Albrecht/Kilchling* 2011, 88.

216 *Bundesministerium des Inneren,* Polizeiliche Kriminalstatistik 2012, S. 4; abrufbar unter: http://www.bmi.bund.de/SharedDocs/Downloads/DE/Broschueren/2013/PKS2012.html?nn=3314802.

1.1.3.4 Cyberwar

Die Technisierung beschränkt sich nicht nur auf die einfache Kriminalität, sondern prägt heute auch die Kriegsführung. Der Begriff Cyberwar (auch Cyberkrieg) beschreibt die hochtechnisierte Form der Kriegsführung im Informationszeitalter.[217] Instrumente des Cyberkriegs sind das Eindringen in fremde Computersysteme zum Zwecke der Informationsgewinnung (Hacken), die Veränderung von Inhalten von Webseiten zu Propagandazwecken (sog. „Defacement"), Denial-of-Service-Attacken[218] oder das Einschleusen kompromittierter Soft- und Hardware. Auch der Einsatz von Strahlungsemissionen, um die Funktionsfähigkeit elektronsicher Geräte zu stören, ist eines der Instrumente des Cyberkriegs. So wurden etwa im Kosovo-Krieg das serbische Luftabwehrsysteme durch Einsatz hochfrequenter Mikrowellenstrahlung und Viren von der *NATO* manipuliert. Daran zeigt sich, dass Cyberwar längst keine Zukunftsvision mehr ist, sondern schon heute die Kriegsführung entscheidend prägt.[219]

Cyberwar meint jedoch nicht allein Fälle in denen tatsächlich ein zwischenstaatlicher Konflikt mittels IuK-Technologien geführt wird, sondern auch die Bedrohung durch Angriffe aus dem Internet und zwar nicht zwingend durch andere Staaten. Derartige Angriffe haben ein hohes Schadenspotential und erfordern dabei nur einen geringen Aufwand. Sie können potentiell von einigen wenigen oder unzähligen Tätern durchgeführt werden und sind daher schwer über Verteidigungskonzepte wie Frühwarnung, Abschreckung und Vergeltung abzuwehren.[220] Beispielsweise wird das deutsche Regierungsnetz durchschnittlich vier bis fünfmal am Tag angegriffen.[221] Erforderlich ist aufgrund der hohen Abhängigkeit von Informations-/ Kommunikations-Infrastrukturen und -systemen, dem enormen Schadenspotenzial, der eingeschränkten Möglichkeiten der Gefahrenabwehr, ein präventives Handeln zur Vermeidung von Risiken.[222] Neben der Bedrohung der Handlungsfähigkeit von Staaten durch Angriffe auf das Internet, entstehen durch IT-Angriffe jährlich Schäden in Milliardenhöhe.[223] Hier verschwimmen vielfach, auf Grund der Perspektive auf den Schaden, die Grenzen zwischen einfachen Kriminellen und kriegerischen Akten. Fakt ist in jedem Fall, dass die techni-

---

[217] *Berndiek* definiert Cyberwar als „Versuche eines Staates (…) einen anderen Staat mit Hilfe des Internets nachhaltig zu schädigen", *Berndiek* 2012, 7.

[218] Dabei wird durch eine Überbelastung der Infrastruktur ein Zusammenbruch eines digitalen Systems verursacht.

[219] Dies diagnostizierte *Paetsch* schon 1999, „Der Krieg aus dem Netz", Spiegel online v. 30.8.1999, abrufbar unter: http://www.spiegel.de/netzwelt/web/0,1518,38605,00.html.

[220] *Roßnagel* 2003, 24.

[221] *Kempf* (bitkom) in Bezug auf eine Aussage des Innenministers *De Maiziere*, Statement zur Pressekonferenz „Trends in der Internet-Sicherheit", v. 1.3.2011, abrufbar unter: http://www.bitkom.org/files/documents/BITKOM_PK_IT-Sicherheit_Vortrag_Prof__Kempf_01_03_2011.pdf.

[222] *Roßnagel* 2003, 24. Zur Präventionsidee und ihren Auswüchsen in der Kriminalitätsbekämpfung, siehe auch ausführlich, Kap. 1.4.2.1, S. 59 ff.

[223] Allein in Deutschland wird der Schaden durch Hacken vom *BKA* auf 62 Mio. Euro geschätzt; *Christely,* Kulturzeit v. 6.10.2011, abrufbar unter: http://www.3sat.de/page/?source=/kulturzeit/themen/157398/index.html.

sierte Gesellschaft durch ihre Abhängigkeit von Technologien neue Verletzungspotentiale eröffnet hat. Das Internet zählt heute zu einer der kritischen Infrastrukturen.[224]

So erklärt sich auch, dass weltweit an Strategien zur Abwehr von Cyber-Attacken gearbeitet wird. Auch die Bundesregierung hat 2011 eine neue „Cyber-Sicherheitsstrategie" beschlossen.[225] Gegründet wurde in diesem Rahmen ein „Cyber-Abwehrzentrum", das an das *BSI* angegliedert ist.[226] Die *NATO* hat bereits 2007 das *NATO Cooperative Cyber Defence Centre of Excellence* gegründet[227] und erwähnt in ihrem neuen strategischen Konzept den digitalen Krieg als potentielle Bedrohung der euroatlantischen Sicherheit.[228] Auch die *Vereinten Nationen* führen erste Gespräche über eine Ächtung des digitalen Krieges.[229]

1.1.4 Technik verändert die Gesellschaft

Die Gesellschaft ist heute digitalisiert, weltweit vernetzt und nahezu in allen Lebenslagen online. Die neuen technischen Möglichkeiten haben die Gesellschaft verändert. Für die Verwirklichungsbedingungen von Freiheit und Sicherheit bedeutet dies neue Chancen wie neue Risiken.

So kann das Internet als Motor der Freiheit dienen. Ursprünglich als freier Raum, der nicht kontrollierbar ist, gewachsen, ermöglicht die Digitalisierung des gesellschaftlichen Lebens aber auch beliebige Handlungen nachzuvollziehen. Der Freiheitsraum droht so zum Überwachungsraum zu werden. Entscheidend sind dafür letztlich die rechtlichen Rahmenbedingungen.

Auch für die Sicherheit ergeben sich Chancen und Risiken: so wird durch neue Bedrohungslagen und neue Formen der Kriminalität die Gewährleistungsfähigkeit von Sicherheit in Frage gestellt. Auf der anderen Seite bietet die moderne Datenverarbeitung auch optimierte Instrumente zur Verfolgung von Straftaten.

Die Digitalisierung hat viele Gesichter. Fest steht jedoch, sie stellt die Gewährleistung von Freiheit und Sicherheit vor neue Herausforderungen.

1.3 Globalisierung

Die Verwirklichungsbedingungen von Freiheit und Sicherheit haben sich nicht nur durch die Digitalisierung verändert, sondern sind auch durch die zunehmende Welt-

---

[224] So der Innenminister *De Maiziere* Anfang 2011, zitiert nach *Lutz,* „Strategien gegen den Cyberwar, Die Welt kompakt v. 24.2.2011, abrufbar unter: http://www.welt.de/print/welt_kompakt/print_politik/article12630494/Strategien-gegen-den-Cyber war.html

[225] *Krempl,* heise online v. 23.2.2011, abrufbar unter: http://www.heise.de/-1195666.html; *Bundesministerium des Inneren,* „Cyber-Sicherheitsstrategie für Deutschland", 2/2011, abrufbar unter: www.bmi.bund.de.

[226] Direkt beteiligt sind daneben das Bundesamt für Verfassungsschutz (BfV) sowie das Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK).

[227] http://www.ccdcoe.org/. Der Sitz ist Tallinn, Estland.

[228] http://www.*NATO*.int/lisbon2010/strategic-concept-2010-eng.pdf.

[229] *Ladurner,* Die Zeit v. 16.6.2011, Cyberwar – der Wurm als Bombe, S. 3, abrufbar unter: http://www.zeit.de/2011/25/Cyberwar/.

weite Verflechtung von Politik, Wirtschaft und Kultur geprägt. Durch die Globalisierung verdichten sich die weltweiten Beziehungen kontinuierlich. Auch dies beeinflusst die Realisierbarkeit von Freiheit und Sicherheit in der Bundesrepublik Deutschland.

Durch eine deutliche Reduzierung von Transport- und Kommunikationskosten und eine Senkung der Energiekosten haben sich die globalen Verflechtungen in den letzten Jahrzehnten rapide verstärkt.[230] Hinzu kommt, dass die Zollkosten immer weiter reduziert wurden. Mit den zu Ende des zweiten Weltkriegs ausgehandelten GATT-Abkommen (General Agreement on Tariffs and Trade)[231] wurden von 1947 bis 1994 schrittweise in fast allen Marktsegmenten die Zölle gesenkt. Dies beschleunigte insgesamt die Globalisierung. Das Zollniveau erreichte einen historischen Tiefstand. Zusätzlich wird die Liberalisierung der Märkte durch binationale und interregionale Integration vorangetrieben. In diesem Zusammenhang ist insbesondere auf den Binnenmarkt innerhalb der *Europäischen Union* zu verweisen, bei dem es sich um die ökonomisch bedeutendste Freihandelszone handelt.[232]

1.3.1 Liberalisierung des Welthandels

Die Liberalisierung des Welthandels und insbesondere die wachsende ökonomische Bedeutung des Außenhandels veranschaulichen den Effekt, welcher unter dem Begriff Globalisierung verstanden wird.

Der Warenexport nahm im Zeitraum zwischen 1960 und 2008 real um den Faktor 15,1 zu, während die Weltwarenproduktion sich nur um den Faktor 5,2 erhöhte. Der Anteil der exportierten Waren am Welt-Bruttoinlandsprodukt erhöhte sich so von 9,7 Prozent

---

230 Die Darstellung knüpft an die Darstellung der Globalisierung auf den Seiten der Bundeszentrale für politische Bildung an, *Hartmann,* v. 11.10.2010, abrufbar unter: http://www.bpb.de/nachschlagen/zahlen-und-fakten/globalisierung/52498/voraussetzungen.

231 Ausführich zum GATT-Regime als Instrument des freien Welthandels *Dolzer,* in: *Vitzthum,* VR 2010, Rn. 63 ff. Mit der Gründung der Welthandeslorganisation/ World Trade Organisation (WTO) als Internationaler Organisation wurde das GATT-Regime um eine Internationale Organisation ergänzt. Der Grundstein für die Weltwirtschaftsordnung wurde mit den Vereinbarungen von Bretton Woods 1944 geschaffen in dem als drei Pfeiler der Weltwirtschaftsordnung der Internationale Währungsfonds (IWF), Weltbank und WTO entwickelt wurden. IWF und Weltbank wurden Sodann im darauffolgenden Jahr gegründet, während die Schaffung einer Internationalen Handelsorganisation am amerikanischen Widerstand scheiterte; vgl. *Hobe* 2008, 394. Erst mit dem Übereinkommen zur Errichtung WTO im Jahr 1994 konnte eine Welthandelsorganisation in Gestalt einer internationalen Organisation geschaffen werden, die mit dem GATT-Regime heute die weltweite Wirtschaftsordnung prägt.

232 Ausführlich zu den Handelsgewichteten Zollbelastungen, der Geltung des Meistbegünstigungsprinzips etc., *Hartmann* (Bundeszentrale für politische Bildung), Globalisierung, Handelsgewichtete Zollbelastungen, http://www.bpb.de/wissen/JX7BR1,0,0,Handelsgewichtete_Zollbelastungen.html.

im Jahr 1970 auf 26,3 Prozent im Jahr 2008.[233] Der grenzüberschreitende Warenhandel hat sich allein zwischen 1990 und 2000 auf 85 Prozent vervielfacht.[234]

Nicht nur die Ausrichtung auf den Export hat sich im Sinne einer globalen Vernetzung verändert, sondern auch die Struktur von Unternehmen wurde globalisiert: Waren es 1970 noch unter 10.000 transnationale Unternehmen, sind es 2008 schon 82.000 (weltweit). Diese transnationalen Unternehmen sind bedeutende Akteure der Globalisierung und haben sie vorangetrieben. Denn sie sind es, die über die organisatorischen, technischen und finanziellen Ressourcen verfügen, um eine Strategie des „*Global-Sourcing"* zu verfolgen.[235]

Flankiert, bestärkt und zum Teil auch ins Leben gerufen wurde die Globalisierung unter anderem durch politische Entscheidungen, die zu einer Öffnung des Welthandels führten und die heute gültige Welthandelsordnung auf den Weg brachten,[236] wie die GATT Abkommen die zur Senkung der Zölle führten. Voraussetzung der Globalisierung sind neben politischen Entscheidungen, die technischen Entwicklungen, die eine weltweite Vernetzung durch vergünstigte und schnellere Transport- und Kommunikationswege erst ermöglicht haben.[237]

1.3.2 Internationalisierung der Politik

Bildeten zu Beginn des 20. Jahrhunderts völkerrechtliche Verträge als bilaterale Abkommen noch die Ausnahme, prägen heute immer wieder unilaterale Entscheidungen der *Vereinten Nationen* die nationale Politik. Zudem werden nationale Entscheidungen verstärkt durch supranationale überlagert. Dies gilt auch im Bereich des Sicherheitsrechts.

Mit der Gründung des Völkerbunds nach Ende des Ersten Weltkrieges wurde der Eintritt in die Ära des modernen Völkerrechts eingeleitet.[238] Der Völkerbund scheiterte zwar mit dem zweiten Weltkrieg. Eine zweite auf Universalität angelegte internationale Organisation mit dem Ziel der universellen Friedenssicherung wurde dann mit den *Vereinten Nationen* kurz nach dem Ende des Zweiten Weltkrieges gegründet. Damit

---

[233] Die Darstellung rekurriert auf die umfassende Analyse von Fakten und Zahlen zur Globalisierung auf den Seiten der Bundeszentrale für politische Bildung, *Hartmann,* v. 11.10.2010, abrufbar unter: http://www.bpb.de/nachschlagen/zahlen-und-fakten/globalisierung/.

[234] Die Außenhandelsquote stieg um mehr als das Doppelte von 19,7 Prozent im Jahr 1970 auf 53,2Prozent im Jahr 2008; *Hartmann* (Bundeszentrale für politische Bildung), Globalisierung, http://www.bpb.de/wissen/3MGD0S,0,0,Anzahl_Transnationaler_Unternehmen.html.

[235] *Hartmann* (Bundeszentrale für politische Bildung), Globalisierung, Anzahl transnationaler Unternehmen, abrufbar unter: http://www.bpb.de/wissen/3MGD0S,0,0,Anzahl_Transnationaler_Unternehmen.html.

[236] *Dolzer,* in: *Vitzthum,* VR 2010, Rn. 63 ff.; *Hobe* 2008, 393 ff.

[237] So kostete etwa ein dreiminütiges Gespräch von *New York* nach *London* im Jahr 1930 knapp 245 US-Dollar, 40 Jahre später kostete ein solches Gespräch dann etwas über 30 US-Dollar. Im Jahr 2005 kostete es dann lediglich 30 US-Cent. Die Kosten reduzierten sich damit um 99,88 Prozent: Zahlen nach *Hartmann* (Bundeszentrale für politische Bildung), Globalisierung, Transport und Kommunikationskosten, v. 3.3.2010, abrufbar unter: http://www.bpb.de/nachschlagen/zahlen-und-fakten/globalisierung/52499/transport-und-kommunikation.

[238] *Hobe* 2008, 44 ff.

wurde auch der Grundstein für die Universalisierung des Völkerrechts gelegt.[239] Heute gehören den *Vereinten Nationen* fast alle Staaten an.[240] Für alle Mitgliedstaaten bindende Beschlüsse kann der Sicherheitsrat erlassen − dies allerdings nur zur Friedenssicherung im Fall einer Friedensgefährdung. Ansonsten kann er allein unverbindliche Empfehlungen aussprechen.[241] Die *Vereinten Nationen* haben insgesamt stark an Bedeutung gewonnen und prägen heute die internationale Politik.

Ein wichtiger Akteur neben den *Vereinten Nationen* ist auf dem Gebiet der Friedenssicherung die *NATO*, die zum Teil auch eng mit den *Vereinten Nationen* kooperiert.[242] Daneben gibt es zahlreiche weitere regionale völkerrechtliche Organisationen wie etwa die Organisation für Sicherheit und Zusammenarbeit in Europa[243], die *Afrikanische Union* oder die *Organisation Amerikanischer Staaten,* die der allgemeinen politischen Zusammenarbeit gewidmet sind. Auch gibt es weitere universelle oder zumindest interkontinentale Organisationen, die einen gemeinsamen Zweck verfolgen und so eine Entpolitisierung einzelner Sachbereiche erlauben, wie die *Welternährungsorganisation (FAO)*, der *Internationale Währungsfonds (IWF)*, die *Weltbank (IBRD)* oder die *Zivilluftfahrtorganisation (ICAO)*[244].

Als wichtige Akteure der Internationalisierung der Politik sind darüber hinaus noch die *World Trade Organisation (WTO)*[245], die insbesondere für die Liberalisierung des Welthandels eine zentrale Rolle einnimmt, der *Internationale Strafgerichtshof (IStGH)*[246] und internationale Verträge wie etwa das Kyoto-Protokoll[247] zu nennen.

---

[239] *Hobe* 2008, 50; die Charta der Vereinten Nationen wurde am 26.6.1945 in San Francisco unterzeichnet und beinhaltete die Ausweitung des schon im Völkerbundpakt niedergelegten Kriegsverbots zu einem allgemeinen Gewaltverbot.

[240] Aktuell gibt es 193 Mitgliedstaaten, eine Mitgliederliste ist abrufbar unter: http://www.unric.org/de/pressemitteilungen/4116-die-mitgliedstaaten-der-vereinten-nationen .

[241] *Klein/Schmahl* in *Vitzthum,* VR, 2010, Abschnitt 5, Rn. 150; allg. zum Aufbau des Sicherheitsrats Rn. 140 ff; siehe auch *Hobe* 2008, 133.

[242] Die *North Atlantic Treaty Organiszation* (*NATO*) mit Sitz in Brüssel wurde durch den Vertrag von Washington am 4.4.1949 gegründet. Aktuell umfasst sie 26 Mitgliedstaaten. Sie diene ursprünglich als Verteidigungsbündnis. Im Juni 2003 wurde eine Neuorientierung der *NATO* beschlossen, verursacht durch die vorangegangen *NATO* –Einsätze im ehemalgien Jugoslawien. Dabei wurde unter anderem der Aufbau einer schnell einsetzbaren *NATO*-Eingreif-Truppe beschlossen. Die *NATO* hat sich nunmehr als Organisation zur regionalen Friedenssicherung etabliert und wird auch von den Vereinten als solche (nämlich als „regional arrangement" im Sinne von Art. 53 UN-Charta) eingeordnet, dazu *Hobe* 2008, 143 f.

[243] Akz. OSZE. Diese hat ihren Sitz in Wien und ist 1995 aus der früheren *KSZE (Konferenz für Sicherheit und Zusammenarbeit in Europa)* hervorgegangen, die im Kalten Krieg im Rahme internationaler Konferenzen den Dialog zwischen Ost und West befördern sollte. Ausführlich zur OSZE, *Hobe* 2008, 145 f.

[244] *Klein/Schmahl* in: *Vitzthum,* VR 2010, Abschnitt 5, Rn. 9.

[245] Vgl. Fn. 231.

[246] Das Römische Statut des Internationalen Gerichtshof wurde am 17.7.1998 von 120 Mitgliedsstaaten der Vereinten Nationen verabschiedet, 2002 trat es nach der erfolgten 60. Ratifikation in Kraft. Aktuell haben bereits mehr als die Hälfte der Staaten den Vertrag ratifiziert; ausführlich zur Schaffung des Statuts des IStGH, *Hobe* 2008, 270; der aktuelle Ratifikationsstand ist abrufbar unter: http://www.icc-cpi.int/stateparties.html.

Gerade auch die Umweltpolitik zeigt, dass es einer weltumfassenden Zusammenarbeit bedarf, da Herausforderungen wie das Ozonloch nicht unilateral bewältigt werden können, sondern multilateral angegangen werden müssen.

1.3.2.1 Von der Souveränität des Einzelstaats zum Weltregime

Die Internationalisierung der Politik spiegelt sich im Wandel des Völkerrechts. Zwar ist auch noch heute „überkommenes Leitprinzip der Völkerrechtsordnung (…) das in der Liste der UN-Grundsätze an *erster* Stelle genannte Prinzip der *souveränen Gleichheit aller Mitglieder".*[248] Doch das Verständnis von Souveränität[249] hat sich im 20. Jahrhundert grundlegend geändert.

Klassisch galt im Völkerrecht die Souveränität eines Staates als unantastbar. Sollte diese verletzt werden, hatte ein Staat das Recht sich zu verteidigen. Eine Einmischung in die inneren Angelegenheiten eines Staates war damit grundsätzlich untersagt.

In der Charta der Vereinten Nationen wird nunmehr dem Sicherheitsrat das Recht zugestanden im Fall der Bedrohung des Weltfriedens einen Eingriff in die Souveränität eines anderen Staates zu legitimieren (Art. 39 VN-Ch.). In der jüngeren Vergangenheit wurden vermehrt innere Angelegenheiten als Bedrohung des Weltfriedens interpretiert und darauf fußend Resolutionen erlassen, mittels derer in die Souveränität von Staaten eingegriffen wurde.[250] Hier zeigt sich, eine Tendenz, dass auch innere Angelegenheiten als Bedrohung des Friedens verstanden werden und zum militärischen Einschreiten ermächtigen.[251]

Ob, wie manche vermuten, bereits eine Abkehr von diesen Entwicklungen festzustellen ist, wird sich erst noch zeigen.[252] Jedenfalls ist eine Zurückhaltung in der Folge einer sichtbar werdenden Überforderung der Vereinten Nationen erkennbar, was sich gerade auch in den Konflikten in Syrien zeigt. Hier konnte sich der Sicherheitsrat bis dato nicht zu einem Einschreiten entscheiden. Die Zustimmung zur Beendigung des Völkermordes im Kosovo-Krieg im Jahr 1999 wird aber als eine grundsätzliche Akzeptanz dieses Prinzips gedeutet.[253]

Dass zumindest grundsätzlich an dieser Betrachtung festgehalten wird, zeigt sich auch durch die Beschlüsse des Sicherheitsrats zu einem Vorgehen zur Unterstützung der

---

[247] Beschlossen am 11.12.1997. Es handelt sich um ein Zusatzprotokoll zur Klimarahmenkonvention der Vereinten Nationen (UNFCCC). Es ist zum 16.2.2005 in Kraft getreten. Das Kyoto-Protokoll ist der erste Vertrag der völkerrechtlich verbindlich Zielwerte bzgl. des Ausstoßes von Treibhausgasen festlegt. Eine deutsche Fassung des Protokolls ist abrufbar unter: http://www.bmu.de/files/pdfs/allgemein/application/pdf/protodt.pdf .

[248] *Vitzthum* in: *Vitzthum,* VR 2010, Abschnitt. 1, Rn. 45.

[249] Äußere Souveränität beschreibt die Eigenschaft der Staatsgewalt keinem fremden Willen, sondern nur dem Völkerrecht unterworfen zu sein; *Vitzthum* in: *Vitzthum,* VR 2010, Abschnitt. 1, Rn. 46

[250] So etwa die sog. Humanitären Interventionen der Vereinten Nationen in Ruanda, Somalia, dem früheren Jugoslawien, in Kambodscha und Haiti, dazu *Hobe* 2008, 58 f.

[251] Vgl. *Isensee* 2003, 14; *Hobe* 2008, 59.

[252] *Hobe* 2008, 59.

[253] Vgl. Fn. 252.

lybischen Rebellen im Frühjahr 2011.[254] Ohne die internationale Unterstützung wäre die Revolution voraussichtlich gescheitert.

Es kann daher auch der militärische Einsatz der USA und Großbritanniens im Irak wegen vorgeblich vorhandener Massenvernichtungswaffen nicht als generelle Trendwende weg von der Kooperationsordnung hin zu einem „hegemonialen Internationalismus“ [255] gedeutet werden.

Nicht nur im Bereich des militärischen Eingreifens ist ein Wandel vom zwischenstaatlichen Krieg zum multinationalen Eingriff aus humanitären Gründen festzustellen, sondern es ist zudem ein Machtzuwachs der Vereinten Nationen zu erkennen. Richteten sich klassisch die Instrumente der Organisation allein gegen Staaten, sind heute auch einzelne Personen von ihnen betroffen. So sind Individuen von der Resolution 1373 des Sicherheitsrates betroffen und nicht Staaten. Diese verlangt, dass, um die Finanzierung terroristischer Handlungen zu bekämpfen, Gelder und sonstige finanzielle Vermögenswerte von Personen, die terroristische Handlungen begehen oder zu begehen versuchen oder sich an deren Begehung beteiligen, eingefroren werden. Zu diesen Zwecken führen die Vereinten Nationen sogenannte Terrorlisten.[256] Damit haben die Vereinten Nationen erstmals ein Instrument erlassen, mit dem sie zwar vermittelt durch die Mitgliedstaaten, aber letztlich ohne diesen eine Entscheidungsmöglichkeit zu überlassen, gegenüber einzelnen Personen handelt.

An diesem Beispiel wird deutlich, dass sich internationale Politik und internationales Recht durch die wachsende Bedeutung der Vereinten Nationen grundlegend verändert haben. Das Völkerrecht hat sich von einer *„Koexistenz-* zu einer *Kooperationsordnung“* gewandelt.[257] Die Souveränität der Einzelstaaten wird immer stärker durchdringbar. Der Staat öffnet sich immer weiter für eine internationale Kooperation, etwa zur Bekämpfung staatenintern begangener schwerster internationaler Verbrechen. Bezeichnet wird diese Entwicklung als Prozess der Staaten hin zu mehr Kooperationsoffenheit.[258]

1.3.2.2 Europäische Integration

Auf der Ebene der Vereinten Nationen wird weiter von Völkerrecht, internationalem Recht oder auch zwischenstaatlichem Recht gesprochen – auch wenn sich das Verständnis dieses und die Bedeutung der Einzelstaaten, wie aufgezeigt wurde, stark verändert haben. Wie weit die Kooperationsoffenheit reichen kann und wie stark sich die internationale Kooperation verdichtet hat, zeigt sich insbesondere innerhalb der Euro-

---

254 Res. 1970 VN SR, v. 26.2.2011.

255 *Hobe* 2008, 59 wirft hier die Frage auf, ob dies der Fall sein könnte (m. w. Nachw. Fn. 54).

256 Ausführlich zu den Terrorlisten und ihren Auswirkungen auf das nationale Recht *Meyer*/*Macke*, HRRS 2007, 445.

257 *Hobe* 2008, 16.

258 *Hobe* 2008, 60.

päischen Gemeinschaften, heute der Europäischen Union. Diese ist nicht mehr nur internationale Organisation, sondern hat supranationalen Charakter.[259]

Die Mitgliedstaaten der Europäischen Union haben der Europäischen Union Souveränität verliehen. So kann die Europäische Union Rechtsakte erlassen, die unmittelbar in den einzelnen Mitgliedstaaten Geltung haben.[260] Die Macht der Nationalstaaten wird beschränkt zu Gunsten eines europaweiten Verbundes. Selbst der Bereich des Polizeirechts, der zwar noch weitgehend der Regelungsbefugnis der einzelnen Mitgliedstaaten zuzuordnen ist, ist von einer immer enger werdenden Kooperation geprägt und es ist eine Angleichung des Rechts zu beobachten. Es werden zudem zunehmend Sicherheitsinstrumente durch europäische Rechtsakte eingeführt, so etwa die Vorratsdatenspeicherung.

Die Rechtsgrundlage für die europäische Regelung der Vorratsdatenspeicherung ist allerdings nicht in der polizeilichen und justiziellen Zusammenarbeit zu suchen. Vielmehr wird sie damit begründet einheitliche Anforderungen für die Telekommunikationsdiensteanbieter zu schaffen, also mit einer Harmonisierung der wirtschaftlichen Zusammenarbeit in der Union.

Die wirtschaftliche Zusammenarbeit ist letztlich die Wurzel des Europäischen Einigungsprozesses. Die Europäische Union wurde ursprünglich als Wirtschaftsunion gegründet.[261] Durch eine wirtschaftliche Verflechtung sollten neue militärische Konflikte verhindert werden. Ziel war es ursprünglich einen freien Binnenmarkt[262] zu ermöglichen. Heute gehen die Kompetenzen der Europäischen Union weit darüber hinaus. Die

---

[259] Eine supranationale Organisation unterscheidet von einer klassischen internationalen Organisation dadurch, dass ihr Hoheitsrechte verliehen wurden und sie so zur selbständigen Ausübung durch ihre Exekutivorgane ermächtigt ist. Sie kann damit unmittelbare Verpflichtungen der Bürger in den Mitgliedstaaten begründen. Von einem Staat unterscheidet sich eine supranationale Organisation dadurch, dass sie nicht über das „wesentlichste Recht" verfügt nämlich über die Art und den Umfang der Übertragung von Hoheitsrechten zu entscheiden (sog. Kompetenz-Kompetenz), *Hobe* 2008, 151; Das *BVerfG* bezeichnet sie als „Staatenverbund"; BVerfGE 89, 155; Zur Supranationalität der Europäischen Union ausführlich: *Oppermann,* in: *Oppermann/Classen/Nettesheim* EuR 2009 § 5 Rn. 9 ff.

[260] Zur Durchgriffswirkung des sekundären Unionsrechts *Herdegen* 2011, § 5, S. 71.

[261] Die Europäischen Gemeinschaften (EG) wurden als Europäische Gemeinschaft für Kohle und Stahl (EGKS) 1952, als Europäische Wirtschaftsgemeinschaft (EWG, später EG) EGKS und als Europäische Atomgemeinschaft (Euroatom) 1957 von sechs Staaten gegründet (sog. Römische Verträge). Die EGKS hatte eine Laufzeit von 50 Jahren und lief so im Jahr 2002 schließlich aus. Die Gemeinschaften bildeten die erste Säule der mit dem Maastrichter Vertrag gegründeten Europäischen Union. Die zwei weiteren Säulen bildeten die Gemeinsame Außen- und Sicherheitspolitik (GASP) und die Polizeiliche und Justizielle Zusammenarbeit in Strafsachen (PJZS). Mit dem Vertrag von Lissabon, der im Jahr 2007 gefasst und im Jahr 2009 in Kraft getreten ist, wurde die Säulenstruktur aufgelöst. Ausführlich zur Entwicklung der EG/EU auch *Nettesheim,* in: *Oppermann/Classen/Nettesheim* EuR 2009, § 19; *Herdegen* 2011, § 4, S. 42 ff.

[262] Als Grundziel wird im EGV die Herstellung eines Gemeinsamen „Marktes", Art. 2 EGV, genannt. Dabei handelt es sich um einen im Kern freien und nach innen offenen europäischen Wirtschaftsraumes. Der mit der Einheitlichen Europäische Akte eingefügte Begriff des Binnenmarktes (Art. 14 II EGV) ist aber mit dem Begriff des gemeinsamen Marktes identisch, *Nettesheim,* in: *Oppermann/Classen/Nettesheim* EuR 2009, § 19, Rn. 8.

Europäische Union besitzt vielmehr Rechtssetzungskompetenzen in nahezu allen Lebensbereichen. Allein die Strafverfolgung und Gefahrenabwehr liegt, wie bereits angedeutet, noch überwiegend in den Händen der Mitgliedstaaten.[263]

Die Rechtsprechung des *Europäischen Gerichtshofs* ist für die nationalen Gerichte bindend. So hat auch das *Bundesverfassungsgericht* in seiner „Solange-Rechtsprechung" deutlich gemacht, dass es in Bezug auf europäische Rechtsakte von seiner Rechtssprechungskompetenz keinen Gebrauch machen wird, solange auf europäischer Ebene ein vergleichbarer Schutz gewährleistet werde.[264]

Kritisiert wird am Prozess der Europäischen Vergemeinschaftung immer wieder ein strukturelles Demokratiedefizit.[265] Mit dem Vertrag von Lissabon wurden zwar die Kompetenzen, insbesondere das Beteiligungsrecht des *Europäischen Parlament*s gestärkt wurde, vielfach werden aber dennoch Entscheidungen durch den Rat gefasst. Auch in der Eurokrise wurde kritisiert, dass die gefassten Entscheidungen nicht demokratisch legitimiert seien.[266]

1.3.3 Neue Freiheiten - Neue Unsicherheiten

Die weltweite Vernetzung in Wirtschaft und Politik sowie die zunehmende Überlagerung nationalen Rechts durch internationales, vornehmlich aber supranationales Recht, hat viele neue Freiheiten ermöglicht. So war beispielsweise das Reisen oder Arbeiten im grenzüberschreitenden innereuropäischen Verkehr nie so einfach wie heute; Dieser Gewinn an Freiheit ist ein Ergebnis der europäischen Integration. Ähnliches hat die Globalisierung ermöglicht: weltweites Reisen und Arbeiten und damit verknüpft auch ein verstärkter inter-kultureller Austausch. Die Welt in der, der Einzelne lebt, ist größer geworden, da das andere Ende der Welt greifbar geworden ist.

Doch die Liberalisierung der Märkte wie auch die Internationalisierung der Politik haben nicht nur positive Effekte. Sie haben so neben neuen Freiheiten, auch neue Unsicherheiten hervorgebracht und Risiken befördert. Zunächst wird es für den Einzelnen immer schwerer nachzuvollziehen, wer welche politische Entscheidung gefällt hat und warum welches Recht gilt. Die starke Verkettung von Politik und Wirtschaft und der Fokus auf stetiges Wachstum führen dazu, dass die globale Wirtschaftsordnung für den Einzelnen undurchschaubar geworden ist. Die Fragilität des Finanzmarktes bestimmt heute die politischen Entscheidungen in zahlreichen Bereichen. Zu beobachten

---

[263] Zur Polizeikooperation innerhalb der Europäischen Union *Classen,* in: *Oppermann/Classen/Nettesheim* EuR 2011, § 33 Rn. 76.

[264] BVerfGE 73, 339 (387); 102, 147 (162f.); 125, 250 (306); Ausführlich zur Solange-Rspr. des *BVerfG* unten S.170 ff.

[265] *Schäfer*, Leviathan 2006, 350; *Degenhardt* 2011, 52 ff.; dass es sich dabei vornehmlich um eine rechtspolitische Frage handelt, stellt *Härtel* 2006, 39 (generell zur demokratischen Legitimation i.R.d. europäischen Rechtssetzung, S. 27 ff.).

[266] *Collignon* 2010, 6 ff.

ist zudem eine Vergrößerung der Schere zwischen Arm und Reich – sowohl im internationalen Vergleich als auch bei Analyse der deutschen Marktwirtschaft.[267]

Zudem kann auch die Globalisierung und die damit verbundene intensive Ausbreitung westlicher Wertevorstellungen, Leitbilder, Lebens- und Konsumstile als ein „Nährboden" für die Entwicklung terroristischer Gewalt gesehen werden.[268] Der vom Westen propagierte „Trend zur Universalisierung der eigenen Werte" und die militärischen Interventionen in Afghanistan und im Irak werden kritisch verfolgt und ihr steht das „in allen Weltreligionen beobachtbare Bestreben entgegen, kulturelle Identitäten zu bewahren".[269] Zudem führen die weltweite Verfügbarkeit von Informationen und die enge Verknüpfung dazu, dass terroristische Akte weit über den Tatort hinaus ihr Drohpotential entfalten.

1.4 Ausweitung der Sicherheitsvorsorge als Kehrseite hoher Verletzlichkeit

Objektiv haben sich durch Technisierung und Globalisierung die Gefahrenpotentiale vervielfältigt. Die Entwicklungen verlaufen rasant und in zum Teil unüberschaubarer Geschwindigkeit. Es entsteht ein Gefühl hoher Verwundbarkeit.

Terrorakte, Finanzkrise Umweltkatastrophen, Veränderungen des Klimas, die Bedrohung durch atomare Katastrophen, die Abhängigkeit von Informations- und Kommunikationstechnologien etc. − die Bedrohungen sind vielfältig, das Wissen über Risiken und Unglücksfälle nimmt stetig zu und damit wächst auch das Bedürfnis des Einzelnen nach Schutz gegen diese (potentiellen) Gefahren.

Die terroristischen Anschläge von New York, London und Madrid haben die Verwundbarkeit der westlichen Zivilisation gezeigt.[270] Sie haben Angst geschürt und so in der Gesellschaft eine Bereitschaft für eine Ausdehnung von Sicherheitsmaßnahmen, unabhängig von ihrer Effektivität, geschaffen. Insofern lässt sich formulieren, dass der Terrorismus die Präventionsidee forciert hat[271] − auch wenn der Präventionsgedanke an sich schon im Bereich des Umweltschutzes oder zur Vorsorge gegen andere Großrisiken, wie etwa die Bedrohung durch atomare Unglücke, bekannt ist. So ist auch der Terrorismus letztlich nur sichtbarer Anlass der fortgeschrittenen Präventionsstrategien:

In Deutschland wird die Bedrohung durch den internationalen, islamisch-fundamentalistischen Terrorismus als (aktuelle) Sicherheitsgefährdung kommuniziert[272] –selbst wenn hier bislang noch kein Attentat „geglückt" ist und so das statistische Risiko Opfer eines islamisch-fundamentalistischen Anschlags (in der Bundesrepublik) zu werden derzeit bei null liegt.[273] Die Antwort auf derartige kommunizierte

---

[267] *DIW Berlin,* Pressemitteilung v. 15.6.2010, abrufbar unter: http://www.diw.de/de/diw_01.c.357516.de/themen_nachrichten/einkommensentwicklung_in_deutschland _die_mittelschicht_verliert.html.

[268] *Hirschmann* APuZ 2001 (Bd. 51), 7 ff.

[269] *Hirschmann* APuZ 2001 (Bd. 51), 7 ff.

[270] *Isensee* 2003, 8.

[271] *Pütter*, CILIP 2007, 3.

[272] Zur Securitization-Theory, vgl. oben S. 13 f.

[273] *Zeh/Trojanow* 2009, 7 ff.; http://www.tagesspiegel.de/politik/chronologie-anschlaege-in-deutschland-fast-immer-vereitelt/4591238.html. Der Versuch zwei Regionalzüge in die Luft zu sprengen

Sicherheitsgefährdungen sind immer neue Sicherheitsstrategien, die immer stärker ins Vorfeld der Gefahrenabwehr reichen und mit denen insgesamt ein dichtes Netz an Erfassung und Registrierung geschaffen wird.

Die Wurzeln für diese Betonung der Sicherheit liegen aber tiefer, nämlich in der Veränderung der Lebensbedingungen, die den Eindruck einer hohen Verwundbarkeit erzeugen. Weltweite Vernetzung und Digitalisierung vermitteln das Gefühl, dass sich die Angriffspunkte vervielfacht hätten. Die hohe Verunsicherung verursacht ein gesteigertes Bedürfnis nach Sicherheitsvorkehrungen. Somit soll die Tendenz hin zu mehr Sicherheit hier nicht allein als Reaktion auf erfolgte terroristische Anschläge erklärt werden,[274] auch wenn sie vielfach als Auslöser und Rechtfertigung für die Verschärfung staatlicher Sicherheitsmaßnahmen dienen. Grundlegend für die beschriebene Entwicklung ist der generelle Wandel in den „Wahrnehmungsmustern und Handlungskonzepten", der nicht nur auf den Bereich des Terrorismus begrenzt ist, sondern alle Bereiche des gesellschaftlichen Lebens erfasst hat: weg von der reinen Gefahrenabwehr hin zu einer Vorsorge gegen Risiken.[275] Und so wurden in den vergangenen Jahren neue oder ausgedehnte Überwachungsbefugnisse geschaffen.[276]

Im Bereich der Polizeiarbeit hat ein Wandel hin zu verstärkt präventivem Vorgehen bereits im Rahmen der Bekämpfung der organisierten Kriminalität Anfang der 1990er Jahre eingesetzt.[277] Erste Entwicklungen in diese Richtung gehen noch weiter zurück: So wurde schon in den 1970er Jahren die Vision entwickelt und verfolgt, möglichst so

---

scheiterte 2006wegen Konstruktionsfehler (sog. Kofferbomber), dazu etwa http://www.spiegel.de/thema/kofferbomber/; Auch die Düsseldorfer Zelle, ebenso wie die Sauerland-Gruppe wurden noch im Vorfeld eines Versuchs festgenommen. Allein der Anschlag auf US-Soldaten am Frankfurter Flughafen im März 2011 kann als „geglückter" Terroranschlag bezeichnet werden. Allerdings war dies die Tat eines fanatischen Einzeltäters und keiner organisierten terroristischen Vereinigung.

274 *Jakab* 2011, 131 ff. wirft die Frage auf, ob es sich überhaupt um ein „neues Produkt des modernen Staates" handelt, oder ob ähnliche Erscheinungen nicht schon in der Antike zu beobachten waren. Sie kommt dabei zu dem Schluss, dass das Strafrecht in *Platons* Nomoi zumindest in wenigen Fällen zum Mittel der Vorverlagerung der Strafbarkeit gegriffen hat. Dies widerspricht jedoch nicht der Annahme, dass der durchschlagende Erfolg der Präventionsidee heute mit den veränderten Verwirklichungsbedingungen und den neuen Bedrohungslagen zu begründen ist.

275 *Roßnagel* 2003, 20; vgl. zur Ausweitung des Sicherheitsbegriffs oben S. 12 ff., 50 f.

276 *Hornung,* PVS 2012, 377.

277 Diese Entwicklung setzte mit der Etablierung der „vorbeugenden Bekämpfung von Straftaten" als Polizeiaufgabe ein. Die Polizeigesetze der Länder wurden an einen Musterentwurf eines einheitlichen Polizeigesetzes in einem ersten Schritt ab 1977 und dann an eine veränderte Fassung des Musterentwurfs ab 1986 angepasst. Diese zweite Fassung reagierte auf das Volkszählungsurteil und zielte darauf eine länderangeglichene, einheitliche gesetzliche Grundlage zu schaffen. Zudem wurden neue Ansätze zur Bekämpfung organisierter Kriminalität eingefügt; ausführlich zu den Musterentwürfen *Zimmermann* 2005, 65 ff. In der StPO wurden entsprechende Befugnisse zur Bekämpfung der organisierten Kriminalität 1992 eingeführt. Schon seit 1994 gibt es Ansätze BND und Verfassungsschutz an der Bekämpfung der Organisierten Kriminalität zu beteiligen. 1998 wurde die Ermächtigung zur akustischen Überwachung von Wohnungen im Rahmen der Bekämpfung der Organisierten Kriminalität eingeführt und dafür die Verfassung geändert; *Götz,* in: *Isensee*/*Kirchof*, HStR IV 2006, § 85 Rn. 9.

viele kriminalitätsrelevante und gesellschaftliche Daten zu sammeln wie möglich, damit die Polizei Straftaten nicht nur aufklären, sondern verhindern kann.[278]

Insofern kann auch nicht davon gesprochen werden, dass konkret seit dem 11. September 2011 eine Wende hin zu einem Präventionsstaat vollzogen wurde. Diese Entwicklung hin zu verstärkter Prävention und einer Ausdehnung der Sicherheitsmaßnahmen hat sich schrittweise vollzogen.

Es wird im Folgenden zunächst auf die Bedrohung durch den internationalen, islamistisch-fundamentalistischen Terrorismus und Instrumente zu dessen Bekämpfung eingegangen (Kap. 1.4.1) bevor ganz generell die neuen Elemente der Polizeiarbeit im 21. Jahrhundert mit der erkennbaren Tendenz zur Aufweichung des liberalen Polizeirechts und der zunehmenden Digitalisierung der Polizeiarbeit dargestellt werden (Kap. 1.4.2). Abschließend wird in einem dritten Abschnitt der Frage nachgegangen, ob die aufgezeigten Entwicklungen geeignet sind, die vermehrt aufgeworfene These, wir befänden uns auf dem Weg in eine Sicherheitsgesellschaft, begründen können (Kap. 1.4.3).

1.4.1 Bedrohung durch internationalen Terrorismus

In Deutschland wurde erstmals eine sogenannte terroristische Bedrohung in den 1970er Jahren („Deutscher Herbst“) registriert. Nach dem faktischen Ende der Roten Armee Fraktion, wurde in der Bundesrepublik die Bedrohung durch Terrorismus zunächst nicht mehr zentral wahrgenommen. Dies änderte sich mit den Anschlägen in New York im Jahr 2001, in Madrid im Jahr 2004 und in London im Jahr 2005. Mit diesen erlebte die gesamte westliche Welt ein bis dato nicht bekanntes Maß terroristischer Gewalt.

In Afghanistan wurden im Jahr 2010 über 3.300 terroristische Attacken gezählt, im Irak über 2.700.[279] Über 75 Prozent der terroristischen Taten werden in Südostasien und im Nahen Osten verübt. In der Bundesrepublik wurden bislang keine islamistisch-fundamentalistischen Terroranschläge verübt. Dennoch wird die Bedrohung als gegenwärtig wahrgenommen und umfassende Sicherheitsmaßnahmen werden als Reaktion auf die Bedrohungslage akzeptiert. Sämtliche geplanten islamistisch-fundamentalistischen Attentate in der Bundesrepublik konnten rechtzeitig verhindert werden.[280] Trotzdem wird der internationale Terrorismus als akute Sicherheitsgefährdung kommuniziert.[281]

---

[278] So die Vision des damaligen Präsidenten des BKA *Herold*, dazu: *Roßnagel* 1983, 85 ff., 207; *Lisken,* NVwZ 2002, 513, 514; *Weichert* 2011a.

[279] *Dpa,* „Zahl der Toten nach Terroranschlägen weltweit gesunken“, Zeit Online v. 19.8.2011, abrufbar unter: http://www.zeit.de/gesellschaft/zeitgeschehen/2011-08/terrorismus-statistik.

[280] Vgl. oben Fn. 273.

[281] So wurde etwa im Winter 2010/2011 wurde vom damaligen Innenminister *De Maiziere* eine ausdrückliche Terrorwarnung für Deutschland ausgesprochen, *Lißmann* „Innenminister ruft Bevölkerung zu Wachsamkeit auf“, Zeit Online v. 17. 11.2010, abrufbar unter: http://www.zeit.de/politik/deutschland/2010-11/terrorwarnung-de-maiziere; dazu auch schon oben S. 14.

Mit der Verhaftung der Kofferbomber im Jahr 2006,[282] der Sauerlandgruppe im Jahr 2007,[283] und der Düsseldorfer Zelle 2011,[284] wurden mehrfach vermeintliche Attentäter gefasst. Trotz dieser Erfolge, werden eben diese Fälle von Innenministerien und Polizei als Argument für die Begründung weiterer Eingriffsbefugnisse herangezogen.[285] Mit dem Bekanntwerden der Aktivitäten der Zwickauer Terrorzelle wurde im Herbst 2011 erstmals in Deutschland eine terroristische Bedrohung von Rechtsradikalen wahrgenommen.[286] Dies führte ganz ähnlich wie die Bekämpfung des islamistisch-fundamentalistischen Terrors zur Forderung nach neuen Eingriffsbefugnissen und einer Verbesserung der Zusammenarbeit der Nachrichtendienste.[287]

Der Begriff „Terrorismus" ist politisch hoch umstritten. Bislang fehlt es auch an einer universell gültigen und völkerrechtlich verbindlichen Definition.[288] Weitgehend Einigkeit besteht allein dahingehend, dass unter Terrorismus eine Gewaltstrategie nichtstaatlicher Akteure verstanden wird, systematisch eine Gesellschaft oder bestimmte Gruppen in Panik und Schrecken zu versetzen, um (nach eigener Aussage) politische Ziele durchzusetzen.[289] In das Grundgesetz hat der Begriff Terrorismus erstmals mit einer Verfassungsänderung im Jahr 2006 Eingang gefunden.[290] An einer Legaldefinition fehlt es jedoch auch hier.

---

[282] Der Attentäter hatte Koffer mit vermeintlichem Sprengstoff in mehreren Regionalzügen deponiert. Die Bomben explodierten jedoch nicht mangels explosiven Stoffen. Der Attentäter wurde zu lebenslanger Haft verurteilt; *Faigle,* Zeit Online v. 9.12.2008, abrufbar unter: http://www.zeit.de/online/2008/50/kofferbomber-urteil.

[283] Als Sauerlandgruppe wird eine in Deutschland agierende Untergruppe der radikalen Vereinigung „*Islamische Dschihad-Union"* bezeichnet. Die Zelle umfasste vier junge Männer, von denen drei 2007 im Sauerland festgenommen wurden. Informationen zu der „Terrorzelle" und dem Strafverfahren gegen die Männer vor dem *OLG Düsseldorf*, sind unter http://www.spiegel.de/thema/sauerland_gruppe/ abrufbar.

[284] Mitgliedern der sogenannten Düsseldorfer Zelle wird vorgeworfen, mit Splitterbomben Anschläge in Deutschland geplant zu haben. Dazu http://www.spiegel.de/thema/duesseldorfer_zelle/.

[285] *Kirsch,* heise online v. 7.5.2011, abrufbar unter: http://www.heise.de/-1239551.html bzgl. Der Ermittlungen zur Düsseldorfer Zelle; Selbst der (Terror)Anschlag des Einzeltäters *Breivik* in *Norwegen* 2011 der aus nationalistischen Gründen über 90 Menschen tötete, wurde dafür genutzt, die Wiedereinführung einer Vorratsdatenspeicherung zu fordern, *Jansen,* „Attentat in Norwegen", tagesspiegel v. 26.7.2011, abrufbar unter: http://www.tagesspiegel.de/politik/attentat-in-norwegen-was-taugen-deutsche-vorschlaege-fuer-sicherheitsmassnahmen/4435652.html.

[286] http://www.spiegel.de/thema/*Braun*e_zelle_zwickau/.

[287] *Wilkens,* heise online v. 18.11.2011, abrufbar unter: http://www.heise.de/-1381525.html .

[288] *Schneckener* verweist darauf, dass in der Literatur über 100 verschiedene Definitionen zu finden seien, *Schneckener* 2008, 27. Auch auf Ebene der Vereinten Nationen konnte keine Klärung erzielt werden, sondern wurden bislang lediglich spezifische terroristische Akte definiert, die als international geächtet gelten. Es gibt vierzehn Anti-Terrorismuskonventionen, die aber keine konkrete Definition des Begriffs Terrorismus enthalten, dazu etwa *Rötzer,* Telepolis v. 3.2.2002, abrufbar unter: http://www.heise.de/tp/artikel/11/11744/1.html; vgl. auch http://www.auswaertiges-amt.de/DE/Aussenpolitik/GlobaleFragen/TerrorismusOK/TerrorismusbekaempfungVN.html.

[289] Definiert hier nach *Schneckener* 2008, 27, der im Folgenden auch die einzelnen Bestandteile näher konkretisiert.

[290] Gesetzes zur Änderung des Grundgesetzes vom 28.8.2006 (BGBl. 2006 I, 2034). Hier wurde in Art. 73 I Nr. 9a GG die Kompetenz des Bundes zur Abwehr von Gefahren des internationalen Terrorismus eingeführt, dazu *Uhle*, DÖV 2010, 989, 990.

Das Entstehen von Terrorismus wird als Ausdruck gesellschaftlicher und internationaler Konflikt- und Problemlagen erklärt. Die individuellen Ursachen sind dabei vielfältig.[291] Vielfach wird ein Kontext zu den weltweit eskalierenden Gewaltkonflikten gezogen.[292] Andere verweisen auf kulturelle und religiöse Unterschiede, die soweit sie nicht beachtet und respektiert würden, Terror hervorbrächten.[293]

Terrorismus an sich ist kein neues Phänomen – was der Rückblick auf den deutschen Herbst oder die Vielzahl blutiger Terroranschläge in Israel,[294] Irland[295] oder Spanien[296] in den vergangenen Jahrzehnten belegen. Es lassen sich aber Entwicklungstrends feststellen, die die Bekämpfung des Terrorismus heute erschweren. Erkennbar sind eine Internationalisierung/Transnationalisierung,[297] eine Zunahme der Bedeutung nichtstaatlicher Unterstützung (verbunden mit einer starken Diversifizierung der Finanzierung)[298] und schließlich eine Verstärkung medialer Effekte sowie ein wachsendes Zerstörungspotenzial.[299] Erschwert wird die Arbeit der Sicherheitsbehörden, da es weder starre Organisationsstrukturen, die ermittelt werden könnten, gibt, noch klare Täterprofile oder Tatprofile erkennbar sind.[300] Vielmehr handelt es sich beim modernen islamistisch-fundamentalistischen Terrorismus letztlich um ein sehr unklares Phänomen, das in vielerlei Gestalt auftreten kann. Entsprechend ist auch kein klares Mittel ersichtlich, mit dem Polizeibehörden eindeutig und effektiv gegen terroristische Aktivitäten vorgehen können. Vielmehr ist auf Grund der Vielgestaltigkeit letztlich kaum ein Mittel denkbar, das nicht irgendeinen Nutzen verspricht.[301] Um zu verhindern, dass der Staat ausufernde Eingriffsbefugnisse erhält, ist auf Grund der leichten Argumentation

---

[291] *Schneckener* 2008, 25 f. hier spielen verschiedenste gruppenpsychologische, organisationssoziologische, soziokulturelle, politische und ökonomische Faktoren zusammenspielen.

[292] *Schneckener* 2008, 26.

[293] *Isensee* 2003, 20 ff., meint gar: „Der Hass steigt hervor aus der Religion des Islam“ (21), er setzt dabei zwar nicht Islamismus und Islam gleich. Dennoch meint er, dass das „aufklärerisch-gefällige Bild“, das häufig vom Islam gemacht würde nicht der Realität entspreche. Der Islam ist aber keinesfalls nur Geburtsstätte des Hasses, wie er es darstellt. Auch das Christentum war zu Zeiten der Kreuzzüge eine Keimstätte für Hass und ist es noch heute, soweit es fundamentalistisch ausgeprägt ist. Insofern, ist m.A. nicht einer bestimmten Religion eine besondere Aggressivität zuzuschreiben, sondern es sind fundamentalistische Gesinnungen, denen Hass und Terror entspringen. Dies gilt auch für politischen Terrorismus.

[294] Der Freiheitskampf des von Israel besetzten Palästina ist seit Jahrzehnten geprägt von Terroranschlägen. Zum Palästinakonflikt generell, *Sisk* 2011.

[295] In Irland wurde vorwiegend in den 80er und 90er Jahren ein blutiger Kampf zwischen dem katholischen Norden und dem evangelischen Süden geführt. Hierbei wurden viele Terroranschläge verübt, dazu *O'Ballance* 1981; *Feldman* 1991.

[296] Seit etwa 40 Jahren kämpft im spanischen Baskenland die Untergrundorganisation *ETA* mit terroristischen Mitteln für die Unabhängigkeit des Region, dazu SZ v. 20.10.2011, „Terror im Baskenland – ETA kündigt Ende der Gewalt an“, abrufbar unter: http://www.sueddeutsche.de/politik/terror-im-baskenland-eta-kuendigt-ende-der-gewalt-an-1.1169748.

[297] *Schneckener* 2008, 29.

[298] *Schneckener* 2008, 29 ff.

[299] *Schneckener* 2008, 32.

[300] *Schneckener* 2008, 33 ff.

[301] *Schneckener* 2008, 43 ff.; eine Sammlung von zahlreichen Nachweisen zum Thema Terrorismus als Herausforderung für die Politik der inneren Sicherheit bei *Jakowatz* 2010.

damit, dass es sich um ein Mittel im Kampf gegen den Terrorismus handelt, gerade bei diesen genau zu überprüfen, welche Bedeutung ihnen tatsächlich und spezifisch für die Ermittlungsarbeit gegen terroristische Aktivitäten zukommt.[302]

Infolge der Anschläge vom 11. September 2001 wurden in der Bundesrepublik zwei sogenannte Anti-Terror-Pakete verabschiedet.[303] Das erste beinhaltete eine Verstärkung der Finanzausstattung von Bundeswehr, Nachrichtendiensten, Bundesgrenzschutz, Bundeskriminalamt und Generalbundesanwaltschaft. Zudem wurde das Religionsprivileg im Vereinsgesetz gestrichen und die Strafbarkeit der Mitgliedschaft in ausländischen terroristischen Organisationen eingeführt. Schwerpunkt des zweiten Pakets war die verstärkte Einbeziehung der Nachrichtendienste in die Bekämpfung des Terrorismus und die Ausweitung der informationellen Befugnisse der Nachrichtendienste.[304] Beispielsweise wurde der Verfassungsschutz zum Einsatz des so genannten IMSI-Catchers befugt, dessen Einsatz bis dato rechtlich umstritten war.[305]

Diesen Gesetzen kommt eine hohe symbolische Bedeutung zu. Sie sollen dem Bürger zeigen, dass die Politik auf Geschehnisse schnell reagiert und mit neuen Instrumenten für die Sicherheit seiner Bürger sorgt.[306] Da umgehende Reaktionen gefordert sind, wohnt diesem politischen Aktionismus die Tendenz inne, dass die Gesetzgebungsverfahren in sehr hohem Tempo durchgeführt werden.[307]

Problematisch an solch unmittelbaren Reaktionen des Gesetzgebers ist, dass diese in einer emotionalisierten Lage verabschiedet werden und insofern kein Raum für eine tiefgreifende Diskussion bleibt und damit auch die Qualität der Gesetze leidet.[308] So machte *Fetscher* bereits im Jahr 1981 eine Beobachtung, die letztlich heute noch uneingeschränkt Aktualität besitzt: „Die Reaktion der deutschen Öffentlichkeit ist weit stärker als die in irgendeinem anderen Land. Das hängt mit unserer Geschichte, mit dem fehlenden demokratischen und nationalen Selbstbewusstsein, einem tiefsitzenden Unsicherheitsgefühl zusammen. Die nüchterne, vorwiegend kriminaltechnische und organisatorische Frage, wie man am besten und schnellsten den Terror bekämpfen kann, wird allzu rasch und allzu leicht mit der Bereitschaft kombiniert, Gesetze und sogar Verfassungsartikel im Interesse der

---

302 *Schneckener* 2008, 43 ff. fordert unabhängige und regelmäßige Evaluationen, um ein unverträgliches Ausufern staatlicher Eingriffsbefugnisse im Namen des Terrorismus zu verhindern.

303 1. ÄndG zum Vereinsgesetz v. 4.12.2001 (BGBl. 2001 I, 3319); Einführung des § 129b StGB mit 34. StrÄndG v. 22.8.2002, BGBl I, 3390; 2. Paket eingeführt mit Terrorismusbekämpfungsgesetz v. 9.1.2002, BGBl I, 361; ausführlich zu den Änderungen *Nolte*, DVBl. 2002, 573.

304 *Götz,* in: *Isensee*/*Kirchof*, HStR IV 2006, § 85 Rn. 11.

305 Ein IMSI-Catcher ermöglicht es den Standort einer Person und Geräte- und Kartenummer des genutzten Handys zu ermitteln. Zu der technischen Funktionsweise ausführlich, *Fox*, DuD 2002, 212.

306 Zum politikwissenschaftlichen Erklärungsmodell „Securitization", vgl. oben S. 13 f.

307 Die erlassenen Rechtsakte werden auch als „Schnellschußgesetze" bezeichnet, zu diesem Effekt in Bezug auf Rechtsakte nach IRA-Anschlägen in Großbritannien oder die Verabschiedung des Kontaktsperregesetzes während der Entführung von Hans-Martin Schleyer in nur drei Tagen, *Roßnagel* 1983, 95.

308 *Roßnagel* 1983, 95.

‚besseren Abwehr' zur Disposition zu stellen und neue, den aktuellen Bedürfnissen angepasste Gesetze zu verabschieden."[309]

1.4.2 Elemente neuer Sicherheitsstrategien

Mit welchen neuen Sicherheitsstrategien auf die Bedrohung durch den Terrorismus und auf andere Sicherheitsgefährdungen reagiert wurde, wird im Folgenden aufgezeigt. Einige der neuen gesetzlichen Befugnisse wurden vom *Bundesverfassungsgericht* als verfassungswidrig erachtet, wobei stets nicht die Maßnahme generell, sondern sie immer nur ihre konkrete Ausführung als verfassungswidrig beurteilt wurden.

Überblicksartig sind als Elemente der neuen Sicherheitsstrategie zu nennen:[310]

- Präventive Telefonüberwachung (§ 33a Nds.SOG; für nichtig erklärt *BVerfG* Urt. v. 16.3.2005),[311]
- Terrorlisten nach UN- und EG-Recht,[312]
- Abschussbefugnis bei Flugzeuganschlägen (für nichtig erklärt, *BVerfG* Urt. v. 15.2.2006),[313]
- (längerfristige) Observation, §§ 163 e, f StPO,[314]
- Akustische und teilweise auch optische Wohnraumüberwachung, der sogenannte „Große Lauschangriff", § 100c StPO (einschränkend *BVerfG* Urt. v. 3.3.2004),[315]
- Ausweitung der Telefonüberwachung, z. B. in Bayern,[316]
- Funkzellenabfrage sowie Auskunft über Verbindungsdaten und Standortbestimmung von Handys, §§ 100a, g, i StPO,[317]
- DNA-Analyse zur Straftatenaufklärung, § 81e-81g stopp i.V.m. DNA-Identifikationsgesetz (DNA-IFG),[318]

---

309 *Fetscher* 1978, 8.

310 Die Aufzählung im Folgenden orientiert sich an *Gusy*, VerwArch 2010, 309, 319 – sie beschränkt sich rein auf Befugnisse, die wesentlich i.R.d. Terrorismusbekämpfung eingeführt wurden und klammert so ausländerrechtliche, religionsrechtliche und vereinsrechtliche Befugnisse aus. Dazu weitere Nachw. bei *Gusy* VerwArch 2010, 309, Fn. 69; Eine umfassende Darstellung der Ausweitung sicherheitsrechtlicher Reglungsansprüche im Kontext der Terrorismusbekämfpung findet sich auch bei *Saurer*, NVwZ 2005, 275.

311 BVerfGE 113, 348.

312 Beruht auf VN-Res. 1267/1969 (abrufbar unter: http://www.un.org/sc/committees/1267/AQList.htm); in Unionsrechts wurden diese zunächst mit 2009/231/GASP überführt; der *EuGH* hat die ursprünglich bestehende EU-Verordnung Nr. 881/2002 Umsetzung für nichtig erklärt, *EuGH*, Urt. v. 3. 9. 2008 - C-402/05; letztlich erfolgte eine erneute Umsetzung der Listen mit 2009/468/GASP; vgl. auch schon oben Fn. 256.

313 BVerfGE 115, 118.

314 Eingeführt mit Art. 1 Gesetz zur Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen sowie zur Umsetzung der Richtlinie 2006/24/EG, v. 21.12.2007 (BGBl. 2007 I, 3198).

315 BVerfGE 109, 279.

316 *Kuri,* heise online v. 14.12.2005, abrufbar unter: http://www.heise.de/-158077.html.

317 Vgl. Fn. 314.

- Rasterfahndung, § 98a, b StPO: Auswertung staatlicher Dateien unabhängig von ihrem Zweck im Hinblick auf Terrorismus- und andere Gefahren (einschränkend dazu *BVerfG* Beschl. v. 4.4.2006),[319]
- Kompetenz des Bundeskriminalamts zur Terrorbekämpfung (Art. 73 Abs. 1 Nr. 9a GG[320] - in Folge dessen wurde das Bundeskriminalamtgesetz neugefasst und dabei wurden auch zahlreiche neue Befugnisse geschaffen[321]). Durch das Terrorismusbekämpfungsgesetz[322] erhielten daneben BfV, MAD und BND erheblich erweiterte Befugnisse für Eingriffe in die informationelle Selbstbestimmung, in Art. 10 Abs. 1 und Art. 13 Abs. 1 GG,[323]
- Verknüpfung von Polizei und Nachrichtendiensten im präventiven Netzwerk, etwa im Gemeinsamen Terrorismusabwehrzentrum (GTAZ)[324] sowie die Einrichtung gemeinsamer Dateien, wie die Anti-Terror-Datei,[325]
- Vorratsspeicherung von Telekommunikationsverkehrsdaten (§ 113a TKG; für nichtig erklärt, *BVerfG* Urt. v. 2.3.2010),[326]
- Flächendeckende Kfz-Kennzeichenerfassung zum Abgleich mit Fahndungsdateien (einschränkend *BVerfG* Urt. v. 27.2.2008),[327]
- Online-Durchsuchungen, § 5 Abs. 2 Nr. 11 VSG NRW einschränkend *BVerfG* Urt. v. 27.2.2008;[328] Neuregelung im Anschluss an das Urteil etwa in § 20k BKAG)
- Flächendeckende Kfz-Kennzeichenerfassung zum Abgleich mit Fahndungsdateien (einschränkend *BVerfG* im Urt. v. 27.2.2008),[329].

---

318 Gesetz v. 27.12.2003 (BGBl. 2003 I, 3007).

319 BVerfGE 115, 320.

320 Neueingeführt mit Gesetz v. 28.8.2006 (BGBl. 2006 I, 2034).

321 Wie heimliche Online-Durchsuchungen in § 20 BKAG; die Änderungen erfolgte mit „Gesetz zur Abwehr von Gefahren des internationalen Terrorismus durch das Bundeskriminalamt“ v. 25.12.2008 (BGBl. 2008 I, 3083); zur neuen/ veränderten Rolle des BKA, *Schwegel* 2009.

322 „Gesetz zur Bekämpfung des internationalen Terrorismus“ v. 9.1.2002 (BGBl. 2002 I, 361).

323 *Hofmann,* in: *Schmidt-Bleibtreu/Klein*, GG 2011, Art. 1, 57.

324 Das GTAZ wurde Ende 2004 gegründet. Nähere Informationen zum GTAZ sind auf den Seiten des *BMI* abrufbar: http://www.bmi.bund.de/SharedDocs/Standardartikel/DE/Themen/Sicherheit/Terrorismus/GTAZ.html; eine umfassende Darstellung der Organisation, Arbeitsweise und der rechtlichen Grundlagen findet sich bei *Klee* 2010, 112 ff.

325 Die Anti-Terror-Datei wurde eingeführt mit Gesetz zur Errichtung einer standardisierten zentralen Antiterrordatei von Polizeibehörden und Nachrichtendiensten von Bund und Ländern vom 22.12.2006 (BGBl I, 3409); Gesetz zur Errichtung einer standardisierten zentralen Anti-Terror-Datei von Polizeibehörden und Nachrichtdiensten des Bundes und der Länder (Anti-Terror-Dateigesetz – ATDG). Ausführlich zur Anti-Terrordatei, ihrem Aufbau, Zweck, Organisation und Arbeitsweise, *Klee* 2010, 145 ff. *Pütter*, CILIP 2007, 3 kritisiert, dass mit der Kombination von polizeilichen und nachrichtendienstlichen Informationen die Eingriffsschwellen des Polizeirechts unterlaufen würde.

326 BVerfGE 125, 260.

327 BVerfGE 120, 378.

328 BVerfGE 120, 274.

Neben diesen Eingriffs-Befugnissen für Polizeibehörden wurden im Zuge der Terrorismusbekämpfung auch neue oder verschärfte Straftatbestände geschaffen (§§ 129a, b StGB).[330] Etwa wurde mit der Normierung der Strafbarkeit des Besuchs eines Terror-Lagers (mit der Absicht sich in der Begehung einer schweren staatsgefährdende Gewalttat unterweisen zu lassen, zu einer terroristischen Vereinigung Beziehungen aufnimmt) in § 89b StGB[331] die Strafbarkeit einer Handlung schon in das Vorfeld der Verletzung eines Rechtsguts verlagert. Zudem beinhaltet der Straftatbestand einen Gesinnungsaspekt, der in der Praxis schwierig nachweisbar ist.[332]

Insgesamt kann eine starke Ausweitung staatlicher Eingriffsbefugnisse und eine zunehmend präventive Ausrichtung der Polizeiarbeit festgestellt werden. Es wurden nicht nur Ermittlungen im Gefahrenvorfeld legitimiert, sondern auch neue Instrumente zur umfassenden Erhebung personenbezogener Daten entwickelt. Die Mehrzahl der neueingeführten Instrumente und Maßnahmen bezieht sich auf Instrumente bei denen personenbezogene Daten erhoben werden. Viele dieser Instrumente erfassen schon von ihrer Konzeption her auch viele Unverdächtige, haben also eine große Streubreite.[333]

Isensee vertritt die Ansicht, dass eine Ausweitung staatlicher Eingriffsbefugnisse erfolgt sei.[334] Vielmehr sei der Datenschutz in Folge der Begründung des Grundrechts auf informationelle Selbstbestimmung expandiert. Das Recht der Gefahrenabwehr habe sich in Folge des Volkszählungsurteils vollständig gewandelt. Bis dato sei das polizeiliche Erheben und Nutzen von Daten über Personen und die Weitergabe dieser als schlichthoheitliches Handeln verstanden worden, erst in der Folge des Urteils sei dieses zu Eingriffen geworden, die einer Gesetzesgrundlage bedürfen. Der Datenschutz führe dazu, dass die objektive Aufgabe des Staates sich über Realien und deren Entwicklung zu informieren, vernachlässigt werde.[335] Richtig ist zwar, dass das *Bundesverfassungsgericht* mit dem Volkszählungsurteil die Grundlage des Datenschutzes geschaffen hat.[336] Diese Entscheidung war jedoch in Anbetracht der fortschreitenden Digitalisierung dringend geboten und änderte letztlich nichts an der Bewertung, dass die Allgemeine Handlungsfreiheit auch im Informationszeitalter gelte. Letztlich muss gerade diese Entscheidung als Reaktion auf Realien und gesellschaftliche Entwicklungen

---

329 BVerfGE 120, 378.

330 Fassung aufgrund des Gesetzes zur Umsetzung des Rahmenbeschlusses des Rates vom 13. Juni 2002 zur Terrorismusbekämpfung und zur Änderung anderer Gesetze vom 22.12.2003 (BGBl. 2003 I, 2836) m.W.v. 28.12.2003.

331 § 89b StGB eingef. m.W.v 4. 8. 2009 durch G v. 30. 7. 2009 (BGBl. 2009 I, 2437).

332 *Schäfer,* in: MüKo StGB, 2011, § 89b Rn. 4. In Rn 5 weist *Schäfer* zutreffend darauf hin, dass in Anbetracht der Beweisschwierigkeiten, die in der Literatur erhobene Kritik, dass die Vorschrift letztlich darauf ziele eine flächendeckende verdeckte Überwachung der Kommunikation zu ermöglich, „nicht ohne Weiteres von der Hand" zu weisen sei.

333 *Gusy*, VerwArch 2010, 309, 320.

334 Allerdings bereits in einer Publikation aus dem Jahr 2003. Er bezieht sich hier aber auch auf die Ausweitung von Sicherheitsmaßnahmen nach dem elften September, *Isensee* 2003, 39; ähnlich auch *Jäger*, Kriminalistik 1995, 189, 191.

335 *Isensee* 2003, 40 Insofern bedürfe es einer Desensibilisierung der Datenschutzgarantie und fordert eine Differenzierung nach der Schutzbedürftigkeit von Daten nach Sphären.

336 Ausführlich dazu unten, Kap. 2.1.3.1.

beurteilt werden.[337] Jedenfalls ändert aber diese Betrachtung nichts an dem Fakt, dass zahlreiche neue Ermittlungsinstrumente eingeführt wurden, die früher so technisch nicht möglich waren und die überwiegend darauf zielen Gefahren bereits im Vorfeld zu erkennen, um sie zu verhindern.

1.4.2.1 Sicherheit durch Prävention – Abkehr vom liberalen Polizeirecht

„Ein Terminus hat es geschafft, in den postmodernen Gesellschaften universell akzeptiert zu werden und einen sich selbst legitimierenden Anspruch zu erlangen: Prävention. Über Partei-, Ressort- und Ländergrenzen hinweg ist man sich einig: Vorbeugen ist besser als heilen.“*[338]*

Prävention bedeutet, „etwas Unerwünschtem zuvorzukommen, seinen zukünftigen Eintritt zu verhindern oder zumindest, wenn es nicht vollständig verhindert werden kann, seine nachteiligen Auswirkungen zu begrenzen“.[339] Damit verkörpert der Präventionsgedanke den menschlichen Wunsch, das Leben in sichere Bahnen zu lenken. So kann die postmoderne Konjunktur der Prävention als Zeichen für das zunehmende Interesse, „Schadenspotenziale für Gesellschaft und Individuum beherrschbar und berechenbar zu machen“, verstanden werden.[340] Die Prävention kann als Antwort auf das gesteigerte Gefühl der Verwundbarkeit gesehen werden.[341] Dies gilt insbesondere auch für die präventive Verhinderung von Straftaten.[342]

Die Präventionsidee an sich ist zwar nicht neu, sie hat jedoch Konjunktur.[343] Rückblickend wurde der Präventionsgedanke von der sogenannten modernen Schule des ausklingenden 19. Jahrhunderts im Sinne *Franz von Liszts* bis zur unmittelbaren Gegenwart immer wieder betont. [344]

---

337 Unter anderem aufgrund der Systemveränderungen durch den Wegfall der Handlungsschranken, die bis dato eine konkrete Gefahr verlangten und nur gegen Störer und Notstandspflichtige zulässig war, *Podlech*, Leviathan 1984, 85, Fn. 2 ff.

338 *Strasser/van der Brink,* APuZ 46/2005, 3.

339 *Pütter*, CILIP 2007, 3, erläutert hier auch ausführlich inwiefern zwischen verschiedenen Präventionsbegriffen und -praktiken (z.B. primär, sekundär, tertiär) unterschieden werden kann.

340 *Strasser/van den Brink,* APUZ 46/2005, 3 f., abrufbar unter: http://www.bpb.de/apuz/28688/auf-dem-weg-in-die-praeventionsgesellschaft; *Hesse* 1994, 187 f.

341 Zur hohen Verletzlichkeit der Gesellschaft im globalisierten und digitalen Zeitalter, vgl. oben, S. 50 f.; vgl. dazu auch *Sieber,* ZStW (119) 2007, 17.

342 Vgl. oben S. 59 ff.; Die Ausdehnung des Präventionsgedankens wird auch als „Weg in die Präventionsgesellschaft“ beschrieben. So etwa *Strasser/van den Brink,* APuZ 46/2005, 3 ff.; *Huster/Rudolph* 2008, die den Weg vom Rechtsstaat zum „Präventionsstaat“ nachzeichnen. Als Schritt auf dem Weg in einen Präventionsstaat wurde in den Medien etwa die Novelle des BKAG von 2008 aufgefasst: *Neuber,* Telepolis v. 13.11.2008, abrufbar unter: http://www.heise.de/tp/artikel/29/29132/1.html.

343 Die Präventionsidee hat unter dem durch den Soziologen *Beck* in den Diskurs eingeführten Begriff der „Risikogesellschaft“ Aufmerksamkeit erfahren (*Beck* 1986). Dieser vertritt die Ansicht, dass gerade aufgrund der vielfältigen Gefährdungen, die technischer und wissenschaftlicher Fortschritt mit sich führen, die Bedeutung des Präventionsgedankens wachse; kritisch zum „Siegeszug“ der Präventionsidee, *Hassemer,* HRRS 2006, 130, 132 f.

344 *Müller-Dietz,* JZ 2011, 85, 93.

Die Präventionslogik fußt auf der Annahme, dass Prävention stets das mildere Mittel im Vergleich zu reaktiven Maßnahmen sei. Über diese Annahme besteht ein breiter gesellschaftlicher Konsens und präventives Handeln scheint so alternativlos. Dass die Effizienz präventiver Instrumente kaum überprüfbar ist, ändert nichts an der Überzeugungskraft der Präventionslogik. Mit dem Bild von Unsicherheit werden präventive Instrumente gerechtfertigt.[345] Abwehrmaßnahmen gegen Gefahren werden zu Beweisen für das Vorliegen einer Gefahr.[346]

In der fragilen, krisenschwangeren Postmoderne, die von Zukunftsängsten verschiedenster Provenienz heimgesucht wird, brauche es so nicht viel, diagnostiziert *Müller-Dietz,* um Gefahrenszenarien zu entwerfen, denen unter allen Umständen vorzubeugen als allgemeine gesellschaftliche staatliche und rechtliche Pflicht empfunden wird.[347] Es ist das bereits festgestellte Gefühl der Verwundbarkeit, bedingt durch Digitalisierung, Globalisierung und veränderte Bedrohungslagen, die zu einem gesteigerten Sicherheitsbedürfnis geführt haben und der Präventionsidee Vorschub leisten.

Dem Präventionsgedanken, so logisch er erscheinen mag, wohnt jedoch eine Gefahr inne, nämlich ihre generelle Grenzenlosigkeit.[348] So wird man nie genug wissen und nie genug kontrollieren können, um jedes Gefahrenszenario zu verhindern. Denn die Voraussetzung wirksamer Prävention ist, dass man über das erforderliche Wissen verfügt, um Prognosen treffen zu können. „Man muss innerhalb der sozialen Wirklichkeit sowohl die zukünftigen potentiellen Gefährdungen diagnostizieren als auch jene Faktoren bestimmen, durch deren Beeinflussung das Diagnostizierte verhindert werden kann. Beides verlangt, möglichst viel über soziale Sachverhalte zu wissen und die Wirkungszusammenhänge zu kennen.“[349] Daran wird der expansive Charakter der Präventionslogik deutlich: „Wer vorbeugen will, weiß nie genug.“[350]

Der durchschlagende Erfolg der Präventionslogik im Rahmen der Einführung neuer Sicherheitsstrategien, spiegelt sich im Bruch mit dem klassischen liberalen Polizeirecht.[351] Zwar wird auch das herkömmliche Strafrecht unter anderem durch den Prä-

---

345 Etwa mit der Argumentation, das Internet würde zum rechtsfreien Raum, wenn es keine Vorratsdatenspeicherung gebe, wie es etwa Bundesinnenminister *Friedrich* im April 2011 konstatiert hat, zitiert nach: *Borchers,* heise online v. 4.4.2011, abrufbar unter: http://heise.de/-1221444.

346 *Strasser/van den Brink,* APuZ 46/2005, 3, 4 mit Verweis auf den Schriftsteller *Schneider*, Kultur der Angst, Die Zeit v. 24.2.2005, abrufbar unter http://www.zeit.de/2005/09/Irak (S. 3); in diesem Sinne auch *Kotzur* EuGRZ 2011, 105, 106.

347 *Müller-Dietz* JZ 2011, 85, 93; Dies umschreibt letztlich einen Securitization-Prozess, wie er auf Grund der hohen Vulnerabilität der Gesellschaft aktuell leicht gelingt, vgl. dazu oben S. 13 f.

348 Dies gilt auch für Präventionsmedizin. Auch hier akzeptiert die Präventionslogik maximal faktische Limits, so *Kersten*, JZ 2011, 161, 167; „Es wird Zeit, das totalitäre Potential der Präventionsidee sichtbar zu machen. Vorsorge ist prinzipiell unbegrenzt“, verlangt *Geyer,* FAZ Online v. 1.3.2009, 5 in seiner Rezension zum Roman “Corpus Delicti“ von *Zeh*.

349 *Pütter*, CILIP 2007, 3 ff.

350 *Prantl* 2008, 117; ähnlich formuliert *Pütter*, CILIP 2007, 3 ff. „Wer der Präventionslogik folgt, erzeugt einen Sog nach immer mehr Wissen“.

351 Vgl. *Voß,* KritV 2010, 137, 158, der darlegt, dass die präventive Sicherheitsordnung mit der politischen Philosophie des liberalen Rechtsstaats breche; dazu auch *Gusy* 2011, 396.

ventionsgedanken legitimiert,[352] und auch das polizeiliche Handeln ist primär auf Prävention ausgerichtet, da ihre originäre Aufgabe die der Gefahrenabwehr ist. Es kann dennoch ein Wandel vom ehemals liberalen Polizeirecht hin zu einem präventiven Gefahrenvorsorgerecht festgestellt werden.

Mit dem „Kreuzberg-Urteil"[353] erfolgte Ende des 19. Jahrhunderts die Abkehr vom Polizeistaat hin zum liberalen Polizeirecht durch eine restriktive Auslegung der polizeilichen Aufgaben.[354] Hier hat auch der moderne Polizeibegriff seinen Ursprung. Das *Preußische Oberverwaltungsgericht* stellte in der Entscheidung fest, dass die polizeiliche Generalklausel nur zur Abwehr von Gefahren ermächtige.[355] Es entwickelte den Grundsatz der Verhältnismäßigkeit.[356] Die Gerichtsentscheidung war ein „Signal des Abschieds vom Polizeistaat".[357] Sie war grundlegend für die Entpolizeilichung der Verwaltung und die Begrenzung polizeilicher Machtbefugnisse.

Wesentlich war nach dem Kreuzbergurteil, dass eine Ermächtigung zum polizeilichen Handeln (unter der Generalklausel) an das Vorliegen einer Gefahr geknüpft ist. Eine solche wird der klassischen polizeirechtlichen Definition zu Folge angenommen, wenn eine Sachlage gegeben ist, aus der heraus im konkreten Fall der Eintritt oder die Intensivierung eines Schadens wahrscheinlich ist. Das heißt, es muss innerhalb vernünftiger Lebenserfahrung mit dem Schadenseintritt gerechnet werden.[358]

Seit den 1980er Jahren wurde dieser enge polizeiliche Präventionsauftrag schrittweise aufgelöst: „Vorsorge für die Gefahrenabwehr" und die „vorbeugende Bekämpfung von Straftaten" wurden vermehrt zu polizeilichen Aufgaben erklärt und damit der Präventi-

---

352 Spezialpräventiv soll auf den einzelnen Delinquenten eingewirkt werden und generalpräventiv die Allgemeinheit vom Normbruch abgehalten werden; *Pütter*, CILIP 2007, 3; Strafe wird in Anlehnung an *Franz von Liszts* als Prävention durch Repression verstanden, damit wurde grundlegend der Präventionsgedanke im deutschen Rechtssystem verankert, *Strasser/van den Brink,* APuZ 46/2005, 3.

353 PrOVG vom 14.06.1882; PrOVGE 9, 353; neu abgedruckt in DVBl 1985, 219; vgl. zu diesem auch *Pieroth/Schlink/Kniesel* 2012, § 1 Rn. 10.

354 Sieht das in Anbetracht dessen „manche Errungenschaften in Gefahr, welche seit dem Kreuzberg-Urteil des *Preußischen* O*VG* als unangefochten gegolten hatten" *Gusy,* in: 2011, 396.

355 Gegenstand der Entscheidung war eine Polizeiverordnung mit der das Berliner Polizeipräsidium die Bebauung von Grundstücken am Berliner Kreuzberg über eine bestimmte Höhe verboten hatte. Damit sollte zur „Förderung des allgemeinen Wohls", der Blick auf das Kreuzbergdenkmal freigehalten werden. Die Polizeiverordnung wurde für unwirksam erklärt, da nicht zu ästhetischen Eingriffen ermächtigt sei.

356 *Pieroth/Schlink/Kniesel* 2012, § 1 Rn. 12 f.

357 *Pieroth/Schlink/Kniesel* 2012, § 1 Rn. 13 ff.

358 Eine Gefahr liegt nach allgemeiner Ansicht vor, „wenn eine Sachlage oder ein Verhalten bei ungehindertem Ablauf des objektiv zu erwartenden Geschehens mit Wahrscheinlichkeit ein polizeilich geschütztes Rechtsgut schädigen wird", *Wurm,* in: *Staudinger*, BGB Komm 2007, § 839, Rn. 636; *Pieroth/Schlink/Kniesel* 2012, Rn. 2; Kritik am Gefahrenbegriff übt etwa *Freund* der feststellt „auch der Gefahrenbegriff ist gefährlich", GA 2010, 193; dazu auch *Müller,* JZ 2011, 85, 93.

onsauftrag in das Vorfeld einer Gefahr verlagert.[359] Hier müssen keine Anhaltspunkte für eine konkrete Gefahr vorliegen, sondern es genügen Gefahrenprognosen.

Deutlich wird dies etwa in den Entscheidungen des *Bundesverfassungsgerichts* zur Online-Durchsuchung. Das Gericht führt hier aus, dass der als besonders schwerwiegend beurteilte Grundrechtseingriff, schon zulässig wäre, „wenn sich noch nicht mit hinreichender Wahrscheinlichkeit feststellen lässt, dass die Gefahr schon in näherer Zukunft eintritt, sofern bestimmte Tatsachen auf eine im Einzelfall drohende Gefahr für ein überragend wichtiges Rechtsgut hinweisen." Erforderlich sei allerdings, dass zumindest Tatsachen gegeben seien, die zum einen „den Schluss auf ein wenigstens seiner Art nach konkretisiertes und zeitlich absehbares Geschehen zulassen, zum anderen darauf, dass bestimmte Personen beteiligt sein werden, über deren Identität zumindest so viel bekannt ist, dass die Maßnahme gezielt gegen sie eingesetzt und auf sie konzentriert werden kann". Lediglich eine weitgehende Verlagerung in „das Vorfeld einer im Einzelnen noch nicht absehbaren konkreten Gefahr" genüge den verfassungsrechtlichen Anforderungen nicht.[360] Trotz dieser Beschränkung handelt es sich um eine Ausweitung der Eingriffsbefugnisse ins Gefahrenvorfeld.[361]

Die Notwendigkeit einer Ausweitung polizeilicher Befugnisse ins Gefahrenvorfeld, wird von *Isensee* mit den Herausforderungen, vor denen die Polizeiarbeit durch das Phänomen des Terrorismus gestellt ist, begründet.[362] Zum einen bestünde die Schwierigkeit, dass die Abschreckungswirkung von Strafandrohungen (bei Selbstmordattentätern) versage und es daher erforderlich sei, Anschlagspläne frühzeitig aufzudecken und zu verhindern.[363] Darüber hinaus ließe sich bei terroristischen Anschlägen nicht konkret sagen, was genau, zu welchem Zeitpunkt und wo passieren wird; etwa Hinweise auf einen bevorstehenden Sprengstoffanschlag auf ein Großereignis, die aber noch nicht so konkret sind, als dass die im Polizeirecht übliche Gefahrenprognose möglich ist. Daher sei es geboten, die Anforderungen für das Tätigwerden der Polizei dem anzupassen.[364] In dieser Argumentation schlägt sich die Präventionslogik nieder, die Versicherheitlichungen[365] den Weg ebnet: durch die Skizzierung hoher und unberechenbarer Sicherheitsrisiken wird ein Handeln im Vorfeld des Eintretens einer Gefahr verlangt. Das Abwarten bis sich eine Gefahr realisiert, wird in Anbetracht der mit Drohszenarien terroristischer Akte verbundenen Ängste als verantwortungslos verstanden. Dies ist durchaus überzeugend: denn wer möchte verlangen, dass erst abgewartet werden soll bis eine Bombe in einer Menschenmenge explodiert und hunderte oder tausende in den Tod reißt. Diese Perspektive, die aus dem Umweltrecht bereits bekannt ist, ist aber neu im Polizeirecht. Hier konstatiert sich der Wandel vom eingeschränkten Gefahrenabwehrrecht hin zu einem Gefahrenvorsorgerecht. An die Stelle

---

[359] *Pütter*, CILIP 2007, 3; Dass sich polizeiliche Eingriffsbefugnisse weit ins Gefahrenvorfeld vorverlagert haben, stellen auch *Arzt/Eier*, DVBl. 2010, 816, 817 fest; ausführlich zur Entgrenzung des neuen Sicherheitsrechts auch ausführlich *Sieber,* ZStW (119) 2007, 28 f.

[360] BVerfGE 120, 274 (328f.).

[361] Ausführlich dazu *Darnstädt*, DVBl. 2011, 263.

[362] *Isensee* 2003, 16.

[363] *Götz,* in: *Isensee*/*Kirchof*, HStR IV 2006, § 85 Rn. 15.

[364] Dazu auch *Darnstädt*, DVBl. 2011, 263.

[365] Zum Begriff und dem Erklärungsmodell oben S. 13 ff.

von Machtbegrenzung durch exakte Festlegung der Eingriffsvoraussetzungen ist eine Vermehrung der Straftatbestände, eine Verschärfung der Strafdrohungen und eine Vereinfachung der Strafzumessungsvoraussetzungen getreten.[366] Dieses Anknüpfen im Vorfeld einer Straftat bedeutet auch eine Erweiterung des Kreises der Verdächtigen.[367] Ermöglicht wird dies nicht zuletzt durch die technischen Entwicklungen, die es erlauben, die zu Präventionszwecken erforderlichen großen Informationsmengen zur erheben, zu speichern und zu verarbeiten.[368]

1.4.2.2 Digitalisierung der Polizeiarbeit

Umfangreiche Prävention bedarf umfassender Datenverarbeitung. Insofern ist die Informatisierung sowohl Vorbedingung als auch Begleiterscheinung der Verschiebung der Polizeiarbeit hin zu einer Gefahrenvorsorge.

Die Digitalisierung oder Informatisierung der Polizeiarbeit schreitet konstant voran. Auch die Polizei versucht, alle neuen Techniken für ihre Zwecke zu nutzen.[369] Aufgrund der Vielzahl neueingeführter Kontroll- und Aufklärungsinstrumente, wird das moderne Polizeirecht teilweise als Polizeiinformationserhebungs- und -verarbeitungsrecht bezeichnet.[370] Fest steht jedenfalls, dass seit den 1970er Jahren eine starke Zunahme polizeilicher Informationseingriffe, gerade im Rahmen der vorbeugenden Bekämpfung von Straftaten, zu verzeichnen ist.[371]

Die Informatisierung der Polizeiarbeit ist jedoch nicht so jung, wie es in Anbetracht der zahlreichen neuen datenverarbeitenden Maßnahmen, den Anschein haben könnte und ist insofern keineswegs allein ein Phänomen des 21. Jahrhunderts. Die Informationsautomation der Polizei entwickelte sich bereits seit den 1960er Jahren.[372]

Im Namen der Bekämpfung des RAF-Terrorismus baute der damalige Präsident des Bundeskriminalamts *Herold*[373] dieses zu einer handlungsmächtigen Zentralstelle um und trieb die Digitalisierung der Polizeiarbeit voran. Wesentlich dafür war der Aufbau einer zentralisierten informationstechnischen Struktur, die sukzessive auf- und ausgebaut wurde. Im Jahr 1972 wurde das „Informationssystem der Polizei", kurz INPOL,

---

366 *Voß,* KritV 2010, 137, 158; Zu der Vielzahl an Rechtsakten, die auf internationaler und nationaler Ebene in Folge der Terroranschläge vom 11.9.2001 erlassen wurden, *Koepp-Kerstin/Will* 2009, 13.

367 „Eine Maßnahmestrategie zur Gewährleistung der inneren Sicherheit betrifft die Aufrüstung des Staates: Hier sind zwei Grundstrategien erkennbar: Der Kreis der Verdächtigen wird erweitert, und die Vernetzung aller Behörden nimmt zu. (…) Die polizeirechtliche Entwicklung entfernt sich so zunehmend vom liberalen Polizeirecht. (…) Der Grundsatz der Unschuldsvermutung wird mehr und mehr aufgehoben. Polizeiliches Handeln orientiert sich nichtmehr an konkreten Gefahren. die Folge ist, dass Polizeiarbeit zur Vorfeldarbeit wird und sich dadurch gegen alles richten muss. " *Möllers* 2009, 131, 159.

368 *Pordesch,* in: *Roßnagel* 1989, 88.

369 *Roßnagel* 2011b, 36.

370 *Gusy*, VerwArch 2010, 309, 320 in Anlehnung an *Möstl*, DVBl. 2007, 581 ff. *Gusy* räumt jedoch ein, dass diese Feststellung überzogen erscheint, dennoch sei eine Akzentverlagerung erkennbar.

371 *Arzt/Eier*, DVBl. 2010, 816, 817; Schon damals konnten Tendenzen hin zu einer verstärkten „vorbeugenden Kontrolle" beobachtet werden, dazu etwa *Roßnagel* 1983, 206 ff.

372 Die kurze historische Darstellung im Folgenden beruht im Wesentlichen auf der umfassenden Darstellung der geschichtlichen Entwicklung bei *Weichert* 2011a.

373 Präsident des *BKA* von 1971-1981.

in Betrieb genommen.[374] Anfang der 1980er Jahre traten neben die hierarchischen Datenbanken relationale Verarbeitungsstrukturen mit dem Ziel grundsätzlich jede Information mit jeder anderen Information verknüpften zu können.[375] INPOL war zunächst allein auf die Verarbeitung von Texten ausgelegt. Erst mit einer Neukonzeption Ende der 1980er Jahre wurden andere Datenformaten, wie Bildern oder Ton, eingebunden.[376] Seitdem wurde INPOL noch darüber hinausgehend um weitere Funktionalitäten erweitert.

INPOL ist noch heute geprägt durch die Vision *Herolds* so viele kriminalitätsrelevante und gesellschaftliche Daten zu sammeln wie nur möglich. Seine Idee war, dass die Polizei möglichst vor dem Täter am Tatort sein sollte.[377] Es handelt sich insofern um ein Instrument, das im Sinne der Präventionslogik konstruiert wurde.

Im Folgenden werden mit INPOL und Anti-Terror-Datei sowie der Onlineüberwachung exemplarisch unterschiedliche Instrumente der digitalen Polizeiarbeit vorgestellt, um zu vermitteln in welchem Ausmaß Polizeiarbeit heute informatisiert erfolgt und welche und wie viele Daten hier verfügbar sind und verarbeitet werden. Abschließend wird noch ein Blick auf die Ausweitungen der Datenbanken und Datenverarbeitung auf Europäischer Ebene geworfen.

1.4.2.2.1 INPOL und Anti-Terror-Datei

INPOL ist die zentrale Verbunddatei von Bundeskriminalamt, Landeskriminalämtern, Landespolizeien, Bundespolizei, Zoll mit Grenzkontrollaufgaben und Zollkriminalamt. Das Bundeskriminalamt führt diese als „Zentralstelle".[378] Kennzeichen einer solchen Verbunddatei ist, dass die Daten jeweils von Länder- oder Bundespolizeibehörden auf Grund spezifischer polizeirechtlicher oder strafprozessualer Rechtsgrundlage erhoben wurden und dann von diesen dezentral in das Verbundsystem eingegeben werden. Sie stehen dann allen Verbundteilnehmern zum Abruf zur Verfügung. Die datenschutzrechtliche Verantwortlichkeit liegt daher jeweils bei der Stelle, die die Daten eingegeben hat.[379]

---

374 *Borchers,* heise online v. 8.3.2011, abrufbar unter: http://www.heise.de/-1203978.html.

375 Etwa durch die PIOS-Dateien (Personen, Institutionen, Objekte, Sachen) auf Bundesebene; SPUDOKs (Spurendokumentationen) für komplexe Ermittlungen. In diesen werden jeweils sämtliche Erkenntnisse für alle beteiligten Ermittler verfügbar gehalten.

376 INPOL-neu im Jahr 2003, *Schulzki-Hadouti,* heise online v. 29.7.2003, abrufbar unter: http://www.heise.de/-82901.html.

377 *Herold* wünscht sich einen „Kriminalatlas" in den neben zahlreichen täter- und tatbezogenen Daten auch solche der Kriminalgeografie, der Sozialforschung einfließen sollten. Damit sollte es nach seiner Vorstellung ermöglicht werden vorsorgende Strukturentscheidungen zu treffen und die Kriminalität zu reduzieren, vgl. dazu *Weichert* 2011a; *Lisken,* NVwZ 2002, 513, 514 (Fn. 14 mit Verweisen auf eigene Veröffentlichungen *Herolds*).

378 *Arzt/Eier*, DVBl. 2010, 816, 818

379 § 11 Abs. 2 S. 1 BKAG.

INPOL besteht aus verschiedenen Datensätzen. Zu den wichtigsten gehören (in Klammer ist jeweils die Zahl der erfassten Personen gesetzt):[380]

- die Personenfahndung (4,4 Mio.)
- der Kriminalaktennachweis (KAN, 4.3 Mio.)
- Innere Sicherheit (früher APIS, 1,5 Mio.)
- die Haftdatei (500.000)
- die DNS-Auskunftsdatei (DAD – Gendatenbank, 800.000)
- der Erkennungsdienst (ED, 5,9 Mio.)
- das Automatisiertes Fingerabdruckidentifikationssystem (AFIS-P, 2,5 Mio.)
- APOK (Organisierte Kriminalität, 270.000)
- die Falldatei Rauschgift (1 Mio.)[381]
- Fedok (Finanzermittlungen, 7.000.)
- FUSION (Rockerkriminalität, 58.000.)
- Schleusungs-, Dokumentenkriminalität (DOMESCH, 120.000)
- Gewalttäterdateien (u.a. linksmotivierter (1.900), rechtsmotivierter (1.300))
- Gewalttäter Sport (11.000.)
- USA (80.000)
- Kinderporno (47.000)

> Schließlich wird das Violent Crime Linkage Analysis System (ViCLAS) in Deutschland flächendeckend eingesetzt. Dabei handelt es sich um eine Software zur Fallanalyse, mit der Straftaten von Wiederholungstätern im Bereich schwerer Gewaltkriminalität unter fallanalytischen Gesichtspunkten recherchiert werden, um Einzeltaten schnellstmöglich einem Wiederholungstäter zuordnen zu können.[382]

Wie die Auflistung der Datensätze zeigt, beinhaltet schon INPOL zahlreiche Daten über Gefährder. Als spezifisches Mittel im Kampf gegen den internationalen Terrorismus wurde mit der Anti-Terror-Datei eine weitere Datenbank geschaffen, die über die Möglichkeiten von INPOL hinaus, eine unmittelbare Verknüpfung von Polizei- und Geheimdiensterkenntnissen ermöglicht. Ziel der Anti-Terror-Datei ist es, Muster und Strukturen des islamistischen Terrorismus zu erkennen (im Sinne einer Voraberkennung möglicher Gefährder und geplanter Attentate). Sie ist damit ein zentrales Instrument der Terrorismusbekämpfung.[383]

---

[380] Die Aufzählung und die Zahlen sind soweit keine näheren Angaben gemacht sind, zitiert nach *Weichert* 2011a; Die Angaben entsprechen den Angaben die in einer Antwort auf eine kleine Anfrage im Jahr 2009 gemacht wurden, BT Drs. 16/13563.

[381] BT Drs. 16/13563, 22.

[382] *BKA,* „Viclas als unterstützende Falldatenbank“, abrufbar unter: http://www.bka.de/DE/ThemenABisZ/OperativeFallanalyse/Viclas/viclas__node.html?__nnn=true

[383] *Borchers,* c't v. 28.2.2007, abrufbar unter: http://www.heise.de/-302578.html mit Auflistung sämtlicher in der Anti-Terror-Datei zusammengeführten Datenbanken.

Die Anti-Terror-Datei[384] ist die erste Verbunddatei, die von Polizeien und Nachrichtendiensten gemeinsam genutzt wird. Daten des Bundesnachrichtendiensts, des Militärischen Abschirmdiensts, des Bundesamtes für Verfassungsschutz, der Verfassungsschutzbehörden der Länder sowie der Bundespolizei, des Zollkriminalamts, des Bundeskriminalamtes und der Landeskriminalämter sind hier zusammengestellt. Sobald „tatsächliche Anhaltspunkte" dafür vorliegen, dass eine Person Mitglied oder Unterstützer einer terroristischen Gruppierung ist, oder politisch motivierte Gewalt mit internationalem Bezug befürwortet, werden dessen Daten, wenn sie im Bestand einer der beteiligten Behörden sind, in die Anti-Terror-Datei eingetragen (soweit die Eintragung erforderlich ist für die Aufklärung und Bekämpfung des internationalen Terrorismus mit Bezug zur Bundesrepublik Deutschland*)*. Es können darüber hinaus auch Verbände, Gruppierungen, Bankverbindungen, Telekommunikationsanschlüsse, Internetseiten etc., sobald der Verdacht besteht, dass sie mit einer terrorverdächtigen Person in Zusammenhang stehen, eingetragen werden. Auch „Kontaktpersonen"[385] können in der Anti-Terror-Datei gespeichert werden. Im Jahr 2007 waren 13.000 Personen[386] in der Anti-Terror-Datei erfasst, vier Jahre später sind es über 18.000 Personen.[387]

Die Anti-Terror-Datei ist unter anderem wegen ihrer großen Streubreite, auf Grund datenschutzrechtlicher Bedenken, und wegen Verstoßes gegen das Trennungsgebot von Polizei- und Geheimdiensten, heftig kritisiert worden.[388] So gibt es grundsätzliche verfassungsrechtliche Bedenken gegen die Beurteilung von Personen als Gefährder – ob in der Anti-Terror-Datei oder in den Gefährder-Dateien in INPOL. Denn hier werden Personen mit vermeintlich „gefährlichen Neigungen" (etwa Teilnahme an einem Terror-Lager oder wiederholtem Auftreten im „Schwarzen Block") durch die Speicherung in entsprechenden Datenbanken als Gefährder deklariert, obwohl es an sich im Strafrecht nur eine Anknüpfung an konkrete Handlungen oder Taten gibt. Eine Anknüpfung an Neigungen gibt es allein bei der Sicherungsverwahrung, wo allerdings das Vorliegen dieser Neigungen sorgsam geprüft wird.[389]

Nach dem Vorbild der Anti-Terrordatei wurde im Jahr 2012 die Verbunddatei Rechtsextremismus (RED) als Reaktion auf die Mordserie der Zwickauer Terrorzelle NSU, eingerichtet.[390] Diese erfasst bei der Inbetriebnahme über 9000 Einträge und wurde auf 20.000 Datensätze beschränkt.

---

384 *Stubenrauch* 2009 befasst sich ausführlich mit der Verfassungsmäßigkeit der Anti-Terror-Datei.

385 Personen, die „nicht nur flüchtig oder in zufälligem Kontakt in Verbindung stehen und durch sie weiterführende Hinweise für die Aufklärung oder Bekämpfung des internationalen Terrorismus zu erwarten sind", § 2 S.1 Nr. 3 ATDG.

386 *Krempl,* heise online v. 30.3.2007, abrufbar unter: http://www.heise.de/-163746.html.

387 BT-DRs 17/6223, S. 7.

388 *Markowitz/Bergemann* 2009; kritisch auch *Weisser* NVwZ 2011, 142, 144.

389 So wird etwa gefragt, ob die Einordnung einer Person als „Gefährder" nicht ein Unwerturteil darstellt, dass das die Menschenwürde verletzt, da es Bürger mit einem Makel belegt, den diese unwiderleglich mit sich tragen, so *Darnstädt*, DVBl. 2011, 263, 269.

390 *Borchers,* heise online v. 20.9.2012, abrufbar unter: http://heise.de/-1712082; sie beruht auf dem Gesetz zur Bekämpfung des Rechtsterrorismus, BT-Drs. 17/8672.

1.4.2.2.2 Online-Durchsuchung

Bei einer Online-Durchsuchung werden, anders als bei einer Beschlagnahme von IT-Hardware oder Speichermedien, auf einem von den verdächtigten Personen weiter genutzten informationstechnischen System sämtliche Handlungen und gespeicherten Daten heimlich erfasst und zur Auswertung an die Ermittler übertragen. Technisch wird das System des Verdächtigen mit einem sogenannten trojanischen Pferd infiltriert, was es den Ermittlern ermöglicht auf den Rechner des Verdächtigen zuzugreifen und die auf dem System vorhandenen Daten auszulesen oder zu verändern.[391]

Rechtlich ist die Einführung dieses Instruments heftig umstritten.[392] Die erste Einführung einer Ermächtigungsgrundlage für Online-Durchsuchungen wurde vom *Bundesverfassungsgericht* als verfassungswidrig beurteilt.[393] Im Nachgang des Urteils wurde eine neue Ermächtigung zur Durchführung von Online-Durchsuchungen in § 20 k BKAG geschaffen. Im Oktober 2011 wurde bekannt, dass für Online-Durchsuchungen eine Software eingesetzt wurde, deren Fähigkeiten über die nach dem Urteil des *Bundesverfassungsgerichts* zulässigen hinausgeht.[394]

1.4.2.2.3 Datensammlung und -verarbeitung auf EU-Ebene

Auf europäischer Ebene ist eine gemeinsame Sicherheitspolitik erst im Entstehen. In den Art. 26, 31 EUV werden ausdrücklich die Aufklärung und Abwehr terroristischer Bestrebungen, als Konkretisierung der Funktion des Raums der Freiheit, der Sicherheit und des Rechts, genannt. Neben der europäischen Polizeibehörde Europol[395] ist ein wesentliches Instrument der europäischen Sicherheitspolitik das Schengen Informationssystem (SIS). Ziel dieses Systems ist die Aufrechterhaltung der öffentlichen Sicherheit in dem durch das Schengener Abkommen begründeten innereuropäischen Raum, der frei ist von Grenzkontrollen. Es soll insofern die polizeiliche Fahndung nach Personen und Sachen trotz offener Grenzen durch das SIS gewährleistet werden. Dafür werden Namen und Aliasnamen, körperliche Merkmale, Geburtsort und Geburtsdatum, Staatsangehörigkeit und Hinweise darauf, ob eine Person bewaffnet oder gewalttätig ist, gespeichert. In technischer Hinsicht ist das System so aufgebaut, dass es eine Zentralstelle (Straßburg) gibt auf die in jedem Mitgliedstaat angesiedelten Stellen zugreifen können. Zugriff haben darüber hinaus Europol und Eurojust.

Neben SIS wurden zur Erleichterung des zwischenstaatlichen Datenaustauschs mit der Schwedischen Initiative[396] und dem Prümer Vertrag[397] weitere Instrumente zur Verein-

---

391 *Hansen/Pfitzmann*, DRiZ 2007, 225.

392 Grundlegend dazu *Lorenz* 2008; vgl. zur Zulässigkeit einer Online-Durchsuchung de lege ferenda *Gudermann* 2010, 195 ff.

393 BVerfGE 120, 274; Im Urteil begründete das Gericht das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme.

394 *Gieselmann,* heise online v. 9.10.2011, abrufbar unter: http://www.heise.de/-1357769.html; *Roßnagel/Skistims,* ZD 2012, 3 ff.

395 https://www.europol.europa.eu/; zu Europol etwa *Wainwright*, Die Polizei 2010, 206; *Seong* 2005.

396 RB 2006/960/JI v. 18.12.2006.

397 Es handelt sich um ein zwischenstaatliches Abkommen vom 27.5.2005 zwischen den Mitgliedstaaten der EU und Norwegen; der Vertragstext ist abrufbar unter: www.bmj.de/SharedDocs/Downloads/DE/pdfs/Pruemer_Vertrag.pdf?__blob=publicationFile.

fachung des Datenaustauschs geschaffen. Auch bestehen Bestrebungen europaweite Datensammlungen für Sicherheitszwecke zu errichten, die allerdings überwiegend dezentral in den Mitgliedstaaten gespeichert werden (sollen). Zu nennen sind neben der Vorratsspeicherung von Telekommunikationsverkehrsdaten[398], die Speicherung der Flugverkehrsdaten (PNR)[399] und Banktransaktionsdaten (TFTP/Swift-Abkommen)[400].

Neben diesen Systemen, in denen zu Strafverfolgungszwecken Daten gespeichert, übermittelt oder verarbeitet werden, wurden mit EURODAC, Visa-Informationssystem (VIS), Advance Passenger Information (API), Neapel II, Customs Information System (CIS) weitere europäische Instrumente zum Daten Management geschaffen.[401] Auch auf die in diesen Systemen gespeicherten Daten haben zum Teil die Polizeibehörden der Mitgliedstaaten Zugriff.

1.4.2.3 Fazit: Polizeiarbeit als digitalisierte Gefahrenvorsorge

Insgesamt kann die moderne Ermittlungsarbeit charakterisiert werden durch die Fassung neuer Eingriffsbefugnisse, das zunehmend präventive und proaktive Vorgehen und die Digitalisierung der Ermittlungsarbeit. Dabei werden, wie etwa bei TFTP-Speicherung, Kfz-Kennzeichenscanning oder Online-Durchsuchungen, private Unternehmen in die Polizeiarbeit miteinbezogen. Der qualitative Unterschied zur klassischen Polizeiarbeit bei der auch schon auf das Wissen, auf Informationen und Spuren Privater zurückgegriffen wurde, besteht darin, dass Private systematisch in die Ermittlungsarbeit miteinbezogen werden. Darüber hinaus zeigt sich eine immer engere Kooperation zwischen Polizei und Geheimdiensten – wie sie sich etwa auch in der Antiterrordatei spiegelt.[402] Kritisiert wird hier, dass das Trennungsgebot zwischen Polizei und Geheimdiensten verwischt werde.[403]

Schließlich kann festgestellt werden, dass eine Vielzahl der neuen Sicherheitsmaßnahmen europarechtlich geprägt sind.

Abschließend ist zu konstatieren, dass die Ermittlungsbefugnisse der Strafverfolgungsbehörden, der Gefahrenabwehrbehörden und der Nachrichtendienste stark aus-

---

398 RL 2006/24/EG des Europäischen Parlaments und des Rates vom 15. März 2006 (Abl. L 105 vom 13. April 2006, S. 54).

399 Ausführlich zu den PNR-Abkommen aus 2004 und 2007 und dem Richtlinienentwurf aus dem Jahr 2011, *Boehm*/*Hornung* 2012.

400 http://register.consilium.europa.eu/pdf/de/09/st16/st16110.de09.pdf dazu *Krempl,* heise online v. 30.9.2009, abrufbar unter: http://www.heise.de/-872553.html.

401 Sämtliche Europäischen Instrumente wurden von der EU-Kommission evaluiert. Der Evaluationsbericht beinhaltet auch eine Kurzdarstellung zum jeweiligen Instrument, seinen Zwecken, den gespeicherten Daten und den Behörden die Zugriff auf die Daten haben; MEMO 10/349, v. 20.7.2010.

402 In Anlehnung an *Weichert*, der die hier aufgezeigten Merkmale als Trends in der Informatisierung der Polizeiarbeit beschreibt, *Weichert* 2011a.

403 *Weisser* NVwZ 2011, 142, 144; Grundsätzlich zum Trennungsgebot etwa: *Albert,* ZRP 1995, 105; *Nehm* NUW 2004, 3289; *Klee* 2010.

geweitet wurden.[404] Klassisches Polizei-, Ordnungs- und Strafrecht haben sich hin zu einer proaktiven Verbrechensbekämpfung entwickelt[405].

Daran zeigt sich letztlich, wie die schrittweise Erweiterung des Sicherheitsbegriffs[406] als ein politischer Prozess Reaktionen in der politischen Begrifflichkeit nach sich zieht und wie diese begrifflichen Neuerungen politische Konsequenzen zur Folge haben.[407] In einem schleichenden Prozess werden Freiheitsräume Schritt für Schritt weiter reduziert. Dieser kann auch metaphorisch als „Salamitaktik" beschrieben werden.[408].

Treffend beschreibt *Saurer* die vollzogenen Entwicklungen: „in der Konsequenz des ganzheitlich-umfassenden Regelungsanspruchs der Terrorismusbekämpfung (ist) für eine Vielzahl von Rechtsgebieten die signifikante Ausweitung terrorismusspezifischer Befugnis- und Organisationsnormen festzustellen. Dieser Prozess der Verrechtlichung spezifischer Anti-Terrorstrategien findet gleichzeitig auf mehreren Ebenen der Rechtserzeugung statt, so im Recht der Länder, des Bundes, der Europäischen Union und der Vereinten Nationen. Das Zusammentreffen dieser prägenden Entwicklungen hebt das Sicherheitsrecht qualitativ auf eine neue Stufe."[409]

1.4.3 Auf dem Weg in die Sicherheitsgesellschaft?

Es zeigt sich, dass sich insbesondere seit den Anschlägen vom 11.September 2001 politisch die Maßstäbe der Bewertung neuer Sicherheits- und Überwachungsinstrumente verschoben haben.[410] Die aufgezeigte Tendenz mit dem Fokus auf Sicherheit, legt die Frage nahe, ob wir uns damit, auf dem Weg in die Sicherheitsgesellschaft befinden.[411] Dies kann an dieser Stelle jedoch nicht abschließend beantwortet werden, denn Sicherheitsstrategien sind nur ein Element einer Sicherheitsgesellschaft. Feststellen lässt sich jedoch, dass der Sicherheitsbegriff eine Ausweitung erfahren hat und dazu dient, immer weitere Sicherheitsinstrumente zu legitimieren. Insgesamt hat so die Sicherheitsarchitektur in der Bundesrepublik Deutschland einen starken Wandel erfahren, in dem vielfach Sicherheit der Vorrang vor Freiheit eingeräumt wird.[412] Der erweiterte

---

404 *Grafe* 2007, 5.
405 *Hassemer* 2007, 32.
406 Vgl. oben S. 59 ff.
407 *Daase* 2010, 8.
408 *Fuchs* 2010.
409 *Saurer*, NVwZ 2005, 275, 282.
410 *Hornung,* PVS 2012, 377.
411 *Albrecht* 2010a; Sicherheitsgesellschaft ist nicht deckungsgleich mit dem Begriff der Überwachungsgesellschaft. Der Fokus liegt hier nicht allein auf der Überwachung durch den Staat oder die Gesellschaft insgesamt, sondern geht darüber hinaus: Sicherheit wird als Gemeinschaftsaufgabe verstanden, und nicht als öffentliches Gut. Der Verdacht wird, insoweit sind die Merkmale einer Überwachungs- und Sicherheitsgesellschaft deckungsgleich, depersonalisiert und es werden permanente räumliche und situative Kontrollen durchgeführt. Über den Begriff der Überwachungsgesellschaft geht eine Sicherheitsgesellschaft aber insofern hinaus, als hier Sicherheit zu einem Regime des täglichen sozialen Lebens wird, *Fuchs* 2010.
412 In diesem Sinne formuliert *Albrecht*s, dass die neuen Instrumente der Polizeiarbeit als die politische Entscheidung für einen Vorrang von Sicherheit vor Freiheit charakterisiert werden können, *Albrecht* KritV 2010, 137, 143.

Sicherheitsbegriffs und vielfältige neue Strategien zur Gewährleistung von Sicherheit prägen so zu Beginn des 21. Jahrhunderts die gesellschaftliche Realität.

1.5 Sicherheit vs. Freiheit – der Verfassungsstaat vor neuen Herausforderungen

In einer hochkomplexen, weltweit vernetzen und digitalisierten Welt, haben der Einzelne und die Gesellschaft insgesamt das Bewusstsein verloren, Herr über der Entwicklungen zu sein und über ausreichend wirkungsstarke Instrumente zu verfügen, um auf Gefahren reagieren zu können.[413] Auf diesem Eindruck der Verwundbarkeit fußt der Erfolg der Präventionsidee, der heute das Leben des Einzelnen wie auch das gesellschaftliche Zusammenleben prägt. Bedeutend für diesen Prozess sind die neuen Möglichkeiten der Informationsgewinnung und -verarbeitung, die die Ausdehnung informeller Befugnisse erst ermöglicht haben. Mit den Terroranschlägen verbreitete sich sodann die Meinung, dass eine Bedrohung vor allem aus der Sphäre der Gesellschaft und nicht so sehr von Seiten des Staats besteht. Dies hat das Verständnis von Sicherheit beeinflusst und dazu geführt, dass sich die Gewichte verschoben haben. Und zwar von einer Sicherheit vor dem Staat hin zu einer Sicherheit durch den Staat.[414]

Fraglich ist, ob diese Tendenz mit den verfassungsrechtlichen Grundsätzen vereinbar ist. Oder verdrängt die Sicherheitsgesellschaft den Rechtsstaat?[415] Inwieweit ist die Ausdehnung der Sicherheitsarchitektur mit der Verfassung vereinbar? Es gilt daher zu untersuchen, inwiefern das Grundgesetz Freiheit(en) konstituiert und inwieweit ihm die Pflicht zur Gewährleistung von Sicherheit immanent ist.

Sind politische Entscheidungen, die auch als Sicherheit vor Freiheit charakterisiert werden können, überhaupt verfassungskonform? Stehen die Entwicklungen hin zu einem Fokus auf Sicherheit, wie sie in den kriminalpolitischen Entwicklungen hin zu Prävention statt Reaktion zu erkennen sind, noch im Einklang mit den verfassungsrechtlichen Vorgaben zum Ausgleich von Freiheit und Sicherheit? Dies sind die zentralen Fragen, die die veränderten Verwirklichungsbedingungen an die verfassungsrechtliche Gewährleistung von Freiheit und Sicherheit stellen.

Zu beachten ist, dass das Verhältnis von Freiheit und Sicherheit nicht nur durch eine zunehmend präventive Ausrichtung der staatlichen Sicherheitsvorsorge vor neue Fragen gestellt wird, sondern dass Digitalisierung und Globalisierung das gesamtgesellschaftliche Leben kennzeichnen. So sind es multinationale Unternehmen, die heute (weltweit) das Wirtschaftsleben bestimmen. Vor allem im Bereich der neuen Medien haben sich wenige große Unternehmen herausgebildet, die weltweit die digitale Ordnung prägen. Für diese Unternehmen, ist das Wissen um ihre Kunden und zwar jedes

---

413 *Roßnagel* 2003, 21; Die Überschrift dieses Abschnitts ist angelehnt an den Titel eines Aufsatzes, *Nazari-Khanachayi*, JA 2010, 761 „Sicherheit vs. Freiheit – der moderne Rechtsstaat vor neuen Herausforderungen".

414 *Horn* 2003, 438.

415 *Götz,* in: *Isensee*/*Kirchof*, HStR IV 2006, § 85 Rn. 16 meint dass schon die Befürchtung des Abdriftens in einen Rechtsstaats-fernen Präventionsstaat nicht gerechtfertigt sei.

einzelnen Kunden viel wert. Personenbezogene Informationen haben einen enormen Wirtschaftswert entwickelt.[416]

Auch diese Entwicklung muss, selbst wenn sie nicht entscheidend für die Gewährleistung von Freiheit und Sicherheit im modernen Verfassungsstaat ist, mit berücksichtigt werden. Denn letztlich wird die Freiheit des Einzelnen nicht nur durch eine zunehmende Sicherheitsvorsorge seitens des Staates bedroht, sondern auch durch eine Vielzahl wissbegieriger Unternehmen. Insofern droht nicht allein das Abdriften in einen Überwachungs*staat*, sondern in eine Überwachungs*gesellschaft*. Denn es ist nicht ein "Big Brother", der droht die Freiheitswahrnehmung aller Bürger umfassend zu überwachen, sondern es sind neben dem Staat auch unzählige Private. Letztlich ist aber auch in dieser Hinsicht der Staat verpflichtet, die Freiheit der Bürger – auch gegenüber Privaten – zu schützen. Fraglich ist aber wie weit diese Pflicht reicht.

[416] Personenbezogene Daten haben - insbesondere im Internet - einen eigenen Wert. So können spezialisierte Rechner das Nutzungsverhalten innerhalb eines Werbenetzwerks beobachten, um daran anschließend Nutzungsprofile zu bilden, die dann wiederum genutzt werden könne, um den Nutzer zielgenau anzusprechen. Über die dadurch erzielten Gewinne schweigt die Branche allerdings hartnäckig *Brunst* 2009, 32.

2 Die verfassungsrechtliche Garantie von Freiheit und Sicherheit

Freiheit und Sicherheit sind, auch wenn sie nicht als Grundrechte im Grundgesetz normiert sind, zwei zentrale Begriffe des Verfassungsrechts. Das Grundgesetz verpflichtet den Staat zu beidem. Wie genau diese Verpflichtung jedoch ausgestaltet ist – also was etwa die Verpflichtung zur Freiheitsgewährleistung unter den Bedingungen moderner Datenverarbeitung beinhaltet – oder wie weit die Pflicht des Staates reicht, Schutz vor terroristischen Anschlägen und damit Sicherheit zu gewähren, verlangt nach einer genauen Analyse der verfassungsrechtlichen Vorgaben. Erst diese ermöglicht es, die Frage zu beantworten, ob sich aufgrund der veränderten Verwirklichungsbedingungen und der neuen Sicherheitsarchitektur ein solches Ungleichgewicht zwischen Freiheit und Sicherheit gebildet hat, dass die Architektur, wie sie das Grundgesetz zur Wahrung von Freiheit und Sicherheit vorgibt, einzustürzen droht.

Es wird daher im Folgenden untersucht, wie und in welchem Rahmen das Grundgesetz Freiheit und Sicherheit garantiert. Da die grundrechtlichen Gewährleistungen zunehmend durch Unionsrecht geprägt sind[417] und bei der Auslegung der Grundrechte auch die Europäische Menschenrechtskonvention (EMRK)[418] und die europäische Grundrechtecharta (EU-GRCh.)[419] zu berücksichtigen sind,[420] werden diese ebenfalls kurz dargestellt. Zudem gilt es ein Augenmerk auf die europäischen Grundrechtsgewährleistungen zu legen, da europäisches Recht an sich vom *Bundesverfassungsgericht* nicht anhand der Grundrechte überprüft werden kann.

---

[417] So gilt der grundsätzliche Vorrang des Unionsrechts im Fall der Kollision von innerstaatlichem und Europäischem Unionsrecht. Geboten ist insofern eine unionsrechtskonforme Auslegung; Ausführlich dazu *Ehlers*, in: *Schulze/Zuleeg/Kadelbach*, EuR 2010, § 11 insbesondere Rn. 10 ff.; 34 ff.; Das *BVerfG* hat jedoch keinen vorbehaltlosen Vorrang des Unionsrechts eingeräumt, sondern diesen in seiner Rechtsprechung von Solange I, II über Bananenmarktordnung, Maastricht, Lissabon-Vertrag und schließlich die Vorratsdatenspeicherung schrittweise erweitert und wieder eingeschränkt. Vgl. Fn. 264 mit Nachweisen aus der Rspr.; vgl. auch unten Kap. 4.3.

[418] Europäische Menschenrechtskonvention v. 4.11.1950; Konvention Nr. 005 des Europarates; die EMRK-Rechte sind mit dem Inkrafttreten des Vertrages von Lissabon als allgemeine Grundsätze nunmehr auch Teil des Unionsrechts geworden, Art. 6 Abs. 3 EUV.

[419] Die Grundrechtecharta ist weitgehend der EMRK nachgebildet. So sollen auch die EMRK sowie die Rspr. des *EGMR* als Auslegungshilfe für die Grundrechtecharta (Art. 62 Abs. 3 EU-GRCh.). Die Grundrechtecharta ist anwendbar, wenn Primär- oder Sekundärrecht der EU durch Organe oder Einrichtungen der EU oder durch die Mitgliedstaaten durchgeführt wird, vgl. Art. 51 EU-GRCh., das heißt sie ist u. a. dann anwendbar, wenn Mitgliedstaaten durch Erlass eines Rechtsaktes EU-Vorgaben umsetzen oder aufgrund von EU-Recht Verwaltungstätigkeiten wahrnehmen, vgl. dazu *Derksen* 2011, 6; ausführlich zur Bindung der Mitgliedstaaten an die Unionsgrundrechte *Nusser* 2011.

[420] *Jarass,* in: *Jarass/Pieroth,* GG Komm 2011, Art. 1 Rn. 29; *Sodan,* in: *Sodan,* GG Komm 2011, Vorb. Art. 1 Rn. 2a; aus der Rspr des *BVerfG*E 107, 395 (408); 110, 339 (342); „Die Bestimmungen des Grundgesetzes sind jedoch völkerrechtsfreundlich auszulegen. Der Konventionstext und die Rechtsprechung des EGMR dienen auf der Ebene des Verfassungsrechts als Auslegungshilfen für die Bestimmung von Inhalt und Reichweite von Grundrechten und rechtsstaatlichen Grundsätzen des Grundgesetzes. Die völkerrechtsfreundliche Auslegung erfordert keine schematische Parallelisierung der Aussagen des Grundgesetzes mit denen der EMRK“, BVerfGE 128, 326 (LS 2).

A. Moser-Knierim, *Vorratsdatenspeicherung,* DuD-Fachbeiträge,
DOI 10.1007/978-3-658-04156-4_2, © Springer Fachmedien Wiesbaden 2014

2.1 Freiheit

Das deutsche Grundgesetz gewährleistet zahlreiche Freiheiten, es garantiert aber nach dem Wortlaut nicht generell „Freiheit".[421] Berechtigt ist aber die Frage, ob nicht Freiheit eine Art Strukturprinzip der Verfassung ist. Oder ob sich eine Garantie einer abstrakten Freiheit nicht sogar als Staatszielbestimmung darstellt.[422]

Im Grundgesetz-Entwurf von Herrenchiemsee fand sich noch ein eigenständiger Grundsatz der Freiheit: „Alle Menschen sind Frei". Dieser bildet zwar rechtshistorisch die Grundlage von Art. 2 Abs. 1 GG, wurde aber so nicht wörtlich übernommen.[423] Mit der allgemeinen Handlungsfreiheit und der freien Entfaltung der Persönlichkeit enthält die Verfassung jedoch zumindest eine im Ansatz abstrakte Freiheitsgewähr. Daneben werden Teilaspekte der Freiheit durch einzelne Grundrechte und die Menschenwürdegarantie geschützt. Anknüpfungspunkte zur Begründung eines Strukturprinzips Freiheit lassen sich aus den Staatsfundamentalbestimmungen ableiten.

Insofern ist zu untersuchen, ob und welche Freiheit(en) durch die grundgesetzlichen Vorgaben geschützt sind. Dabei sind in Anbetracht der Fragestellung, ob und wie sich das Verhältnis von Freiheit und Sicherheit im digitalen Zeitalter verschoben hat, vertieft die für die Freiheitsausübung im digitalen Zeitalter zentralen Freiheitsreche zu erörtern.

2.1.1 Menschenwürdegarantie

Die Menschenwürde ist wie ein „Schlüssel für das Ganze"[424] dem Grundgesetz vorangestellt.

Der Mensch und seine Würde sind im Grundgesetz als oberstes *Konstitutions*prinzip und tragendes *Konstruktions*prinzip verankert.[425] Die Garantie der Menschenwürde in Art. 1 Abs. 1 GG ist Fundamentalnorm[426] des Grundgesetzes. Sie ist nicht nur unauf-

---

421 *Merten,* in: HGR I, 2006, § 27 Rn. 1.

422 *Merten,* in: HGR I, 2006, § 27 Rn. 4 fragt, ob es ein Leitprinzip Freiheit gibt.

423 Art. 2 Abs. 1, abrufbar unter: http://www.verfassungen.de/de/de49/chiemseerentwurf48.htm; *Verfassungsausschuss der Ministerpräsidenten-Konferenz der westlichen Besatzungszonen*, S. 21, 62 ff.

424 So der Abgeordnete der SPD *Carlo Schmid* in der 4. Sitzung des Ausschusses für Grundsatzfragen v. 23.9.1948; hier zitiert nach *Merten,* in: HGR I, 2006, § 27 Rn. 5.

425 *Merten,* in: HGR I, 2006, § 27 Rn.10; *Hofmann,* in: *Schmidt-Bleibtreu/Klein,* GG 2012, Art. 1 Rn. 7, mit zahlreichen Nachw. auch aus der Rspr des BVerfG; Umstritten ist, ob der Menschenwürde auch Grundrechtscharakter zukommt. Die wohl herrschende Meinung bejaht dies: so etwa *Jarass,* in: *Jarass/Pieroth,* GG 2011, Art. 1 Rn. 3; *Höfling*, in: *Sachs,* GG 2011, Art. 1, Rn. 5 ff.; *Sodan,* in: *Sodan,* GG, 2011, Art. 1, Rn. 1; *Hofmann*, in: *Schmidt-Bleibtreu/Klein*, GG 2012, Art. 1, Rn. 8; aus der Rspr: BVerfGE 1, 332 (343); 12, 113(123); 15, 283 (286): a.A. *Dreier,* in: *Dreier,* GG 2004, Art. 1 Abs. 1 Rn. 125 ff. der mit guten Argumenten die Ansicht vertritt, dass es sich bei Art. 1 Abs. 1 um einen Grundsatz handelt und nicht um ein Grundrecht; dazu auch *Will* 2006, 33, die richtigerweise darauf hinweist, dass der Streit nur von begrenzter Relevanz ist, da bei der Rechtsanwendung eine Verletzung der Menschenwürde wie ein subjektives Recht geprüft werden muss.

426 *Schmidt,* in: ErfKomm ArbR, Art. 1 Rn. 9.

hebbar, sondern auch unbeschränkbar.[427] Das Bekenntnis zur unantastbaren Würde des Menschen prägt alle Bestimmungen des Grundgesetzes und bildet die Grundlage des grundrechtlichen Wertesystems.[428] Die Menschenwürde wurde 1949 gegen die Entrechtung und Vernichtung des Menschen durch den Totalitarismus im nationalsozialistischen Regime dem Grundgesetz vorangestellt.[429]

Seit Ende 1960er und 1970er Jahren wurde verstärkt auf die Menschenwürde rekurriert und zwar speziell im Rahmen von Argumentationen gegen Tendenzen zu weitreichender Überwachung. In den 1980er Jahren wurde dann unter dem Gesichtspunkt der Würde des Menschen vielfach ein Recht auf ein würdiges Ende des Lebens bei unheilbaren und unerträglichen Leiden diskutiert. Heute wird die Unantastbarkeit der Menschenwürde im Kontext der Humangenetik diskutiert.[430]

Letztlich sind die Ansichten darüber was unantastbar ist, einem ständigen Wandel unterworfen. Sie sind geprägt vom aktuellen Gesellschaftsbild und den Vorstellungen über Identität und Individualität.

Unantastbarkeit heißt jedenfalls, dass die Menschenwürde jeder Abwägung verschlossen ist. Auch „Würde gegen Würde" abzuwägen ist demnach unzulässig.[431]

Fraglich ist, ob und inwieweit durch die Menschenwürdegarantie Freiheit gewährt wird. Vielfach wird die Menschenwürde rein negatorisch durch die Verletzungshandlung bestimmt. Zurückgegriffen wird auf die sogenannte Objektformel.[432] Der Einzelne dürfe nicht zum Objekt staatlichen Handelns werden, sondern müsse in seiner Qua-

---

427 *Dreier,* in*: Dreier,* GG 2004, Art. 1 Abs. 1 Rn. 132; *Will* 2006, 30; Sie ist dem grundrechtlichen Abwägungsprozess entzogen, so *Höfling*, in: *Sachs,* GG 2011, Art. 1, Rn. 11.

428 *Hofmann*, in: *Schmidt-Bleibtreu/Klein*, GG 2011, Art. 1, Rn. 7.

429 *Will* 2006, 29; *Dreier,* in: *Dreier,* GG 2004*,* Art. 1 Abs. 1 Rn. 22; Als Umkehr des nationalsozialistischen Satzes, der Einzelne sei nichts, der Staat/ die Gemeinschaft alles, *Jarass,* in: *Jarass/Pieroth,* GG 2011, Art. 1 Rn. 1.

430 *Will* 2006, 29; *Dreier,* in: *Dreier,* GG 2004, Art. 1 Abs. 1 Rn. 45 ff. beschreibt die Gefahr der Trivialisierung und Inflationierung der Menschenwürdegarantie durch die zunehmende Berufung auf diese, insbesondere in Bezug auf neuartige Herausforderungen (Informationstechnik, Biotechnologie).

431 *Will* 2006, 30; kritisch zu einem grundsätzlichen Verbot der Abwägung „Würde gegen Würde" in Bezug auf das Folterverbot, *Gebauer,* NVwZ 2004, 1405. Das *BVerfG* stellt im Urteil zum Luftsicherheitsgesetz fest, dass die Menschenwürde verletzt werde, da das Leben der Flugzeuginsassen und damit deren Würde objektiviert werde, weil die Passagiere „dadurch, dass ihre Tötung als Mittel zur Rettung anderer benutzt wird, verdinglicht und zugleich entrechtlicht" würden. „Indem über ihr Leben von Staats wegen einseitig verfügt wird, wird den als Opfern selbst schutzbedürftigen Flugzeuginsassen der Wert abgesprochen, der dem Menschen um seiner selbst willen zukommt", BVerfGE 115, 118 (154).

432 Die sog. Objektformel geht zurück auf *Wintrich* 1952, 227, 235; heute vor allem bekannt in der Prägung *Dürigs*, der an das Instrumentalisierungsverbot Kants anknüpfte: *Dürig*, AöR 1956, 117 „Die Menschenwürde ist getroffen, wenn der konkrete Mensch zum Objekt, zu einem bloßen Mittel, zur vertretbaren Größe herabgewürdigt wird"; Sie wurde vom *BVerfG* in stRspr rezipiert: BVerfGE 45, 187 (228); 109, 133 (149f.); 116, 69 (85f.); 117, 71 (89); Die Objektformel ist vielfach heftiger Kritikausgesetzt, da sie nicht ohne moralische Werturteile auskommt, dazu *Sodan,* in: *Sodan,* GG, 2011, Art. 1, Rn. 11; Generell zur Objektformel: *Herdegen,* in: *Maunz/Dürig*, GG 2011, Art. 1, Rn. 36; *Hillgruber,* in: BeckOK GG, Art. 1 Rn. 13.

lität als Individuum respektiert werden. Der Schutz der Menschwürde kann aber nicht allein auf seine abwehrrechtliche Funktion beschränkt werden.[433]

Ob der Gehalt der Menschenwürdegarantie positiv konkretisiert werden kann, ist hoch umstritten. Zum Teil wird die Würde als dem Menschen durch Gott oder die Natur kraft seiner bloßen Existenz verliehene Eigenschaft betrachtet. Als Ursprung der Würde wird in diesem Sinne die Existenz des Menschen selbst gesehen.[434] Diese Wert- oder Mitgifttheorie hat eine hohe Attraktion, da sie absolute Geltungskraft vermittelt und durch die kulturhistorische Genese begründet werden kann.[435] Die Verknüpfung mit Wertvorstellungen – ob christlich oder naturrechtlich begründet – birgt allerdings das Risiko, dass der Würdebegriff zu einem offenen Wertbegriff wird, dessen inhaltliche Konkretisierung durch individuelle Wertvorstellungen geprägt ist.[436]

Grundlegend anders erfolgt die Konkretisierung der Menschenwürde in den modernen Leistungs- und Kommunikationstheorien. Hier wird die Menschenwürde als Ergebnis eines individuellen Identitätsbildungs- und Sozialdarstellungsprozesses begriffen.[437] So wird mit Blick auf die Soziologie angenommen die Würde des Menschen entstünde erst im Prozess der Selbstdarstellung, also in der Interaktion mit anderen.[438] Die Menschenwürde setzt nach dieser Ansicht die Möglichkeit zur Selbstdarstellung voraus.[439] Sie umfasst dementsprechend die Entscheidungsmöglichkeit, wie der Einzelne sich selbst darstellen möchte.[440]

An sämtlichen Theorien ist jedoch zu kritisieren, dass sie letztlich den Umfang der Menschenwürdegarantie einschränken. Sie alle verlangen entweder die Anerkennung von außen auf Grund von Wertvorstellungen oder im Fall der Kommunikationstheorien eine eigene Wertleistung des Einzelnen.[441]

---

433 *Merten,* in: HGR I, 2006, § 27 Rn. 11.

434 *Sodan,* in: *Sodan,* GG, 2011, Art. 1, Rn. 4. Die Mitgifttheorie geht zurück auf *Dürig,* in: *Maunz/Dürig*, Erstkommentierung, 1958, Art. 1 Rn. 18.

435 *Sodan,* in*: Sodan,* GG, 2011, Art.1, Rn. 6; vgl. zur kulturhistorischen Genese Kap. 1.1.

436 *Sodan,* in: *Sodan,* GG, 2011, Art.1, Rn. 6.

437 *Luhmann* 1999, 68; *Hofmann*, AöR 1993; *Gröschner/Wiehart-Howaldt* 1995; *Habermas* 2001, 62; Kritisch zu sämtlichen Würdekonzeptionen *Will* 2006, 33.

438 *Luhmann* 1999, 61 „Als Organismus ist der Mensch schon Individuum (…) – aber nur individuelles Objekt. Selbstbewußte Individualität gewinnt er dadurch, daß er sich als Interaktionspartner selbst darstellt."

439 Nach *Luhmann* 1999, 70, können Freiheit und Würde als „die äußeren und inneren Vorbedingungen der Selbstdarstellung als individuelle Persönlichkeit im Kommunikationsprozeß" bezeichnet werden. Diese Interpretation ermöglicht auch eine klare Abgrenzung zwischen Würde und Freiheit, so d*ers*., 77.

440 *Luhmann* 1999, 75: Es bestehe allein ein Anspruch auf einen „Schutz vor dem Staat". Dies zeige sich zum einen darin, dass dem Staat nur die Achtung und nicht der Schutz der Menschenwürde aufgegeben sei. Zum anderen könne der Staat keinen Schutz vor Privater Tücke gewähren, ausführlich dazu *Luhmann*, S. 76 f., Fn. 60. Das *BVerwG* hat hingegen auch eine Schutzpflichten-Dimension anerkannt BVerwGE 115, 189 (Laserdrome); auch *Hofmann*, in: *Schmidt-Bleibtreu/Klein*, GG 2011, Art. 1, 8 erkennt eine Schutzpflichtendimension von Art. 1 Abs. 1 GG.

441 Kritisch zu allen Ansätzen der Konkretisierung ob positiv oder negativ, *Höfling*, in: *Sachs*, GG 2011, Art. 1, Rn. 13; *Sodan,* in: *Sodan,* GG, 2011, Art.1, Rn. 9; Der Würdeanspruch muss völlig

In jüngerer Zeit wird daher vermehrt zur Konkretisierung der Menschenwürdegarantie auf eine gemischte Formel, auch „Objekt-Subjekt-Formel", zurückgegriffen. Diese kombiniert die Objektformel mit dem modernen Subjektbegriff. Nach dieser sind mit dem in der Menschenwürdegarantie verankerten Wert- und Achtungsanspruch alle staatlichen Maßnahmen unvereinbar, die geeignet sind, die individuelle, psychische und soziale Existenz des Menschen zu zerstören.[442] Gefragt wird sodann danach, ob der Subjektstatus eines Menschen trotz einer Verobjektivierung in spezifischen Unterordnungs- und Abhängigkeitsverhältnissen durch Kompensationsmechanismen hinreichend gesichert wird.[443] Als Subjekt wird dabei die selbstbewusste, selbstverantwortliche und sich selbst entfaltende Person begriffen.[444]

Auch wenn sich die Theorien in der inhaltlichen Bestimmung der Menschenwürdegarantie stark unterscheiden, ist ihnen allen gemein, dass sie eine enge Verknüpfung zwischen Würde und Freiheit anerkennen. Die Menschenwürde verlangt stets die Achtung des Individuums in seiner Eigenständigkeit und Eigenwertigkeit und dessen Selbstbestimmung und -verantwortung, wie auch seiner Selbstentfaltung.[445] Voraussetzung dafür ist, dass der einzelne frei ist, um sich entsprechend entfalten zu können.

Auch das *Bundesverfassungsgericht* betont wiederholt, die Menschenwürdegarantie garantiere sich selbst, „in Freiheit (…) zu bestimmen und (…) zu entfalten".[446] Letztlich kann – in Übereinstimmung mit allen Theorien zur Konkretisierung der Menschenwürdegarantie – aus Art. 1 Abs. 1 GG jedenfalls die Verpflichtung des Staates, „geistige Freiheit" zu gewähren, abgeleitet werden.[447]

Auch die EU-GRCh. enthält in Art. 1 S 1 die Garantie der Unantastbarkeit der Menschenwürde.[448] In Art. 1 S. 2 EU-GRCh. wird die Pflicht statuiert die Menschwürde zu achten und zu schützen.[449]

2.1.2 Freiheitsgrundrechte

Das Grundgesetz schützt in Art. 2 Abs. 1 GG, die freie Entfaltung der Persönlichkeit des Einzelnen, „soweit er nicht die Rechte anderer verletzt und nicht gegen die verfassungsmäßige Ordnung oder das Sittengesetz verstößt".

Bei der Verfassungskonstitution war es das Ziel der Abgeordneten die Freiheit möglichst umfassend zu schützen. „Freie Entfaltung umfasst alles", hieß es damals.[450] Mit

---

unabhängig von theoretischen Konstruktionen gewährt werden *Merten,* in: HGR I, 2006, § 27 Rn. 11 mit weiteren zahlreichen Nachweisen.

442 Diese geht zurück auf *Kersten* 2004, 444; dazu auch *Sodan,* in: *Sodan,* GG, 2011, Art.1, Rn. 14.

443 *Höfling*, in: *Sachs*, GG 2011, Art. 1, Rn. 16.

444 *Kersten* 2004, 475 f.; *Höfling*, in: *Sachs*, GG 2011, Art. 1, Rn. 15.

445 *Merten,* in: HGR I, 2006, § 27 Rn. 11.

446 BVerfGE 45, 187 (22/); siehe auch BGHZ 35, 2, (8).

447 *Hofmann*, in: *Schmidt-Bleibtreu/Klein*, GG 2011, Art. 1, Rn. 5.

448 Zwar erstreckt sich nach seinem Wortlaut die Schrankenbestimmung des Art. 52 EU-GRCh. auf alle Rechte und Freiheiten, dennoch ist die Menschenwürde uneinschränkbar, *Schorkopf,* in: *Ehlers/Becker* § 15 Rn. 13.

449 *Frenz* 2009, Rn. 320; ausführlich zum Schutz der Würde des Menschen durch europäisches Recht, vgl. *Schorkopf,* in: *Ehlers/Becker* § 15.

diesem Hintergrund reiht sich die Freiheitsgarantie des Art. 2 Abs. 1 GG historisch in die neuzeitlichen Verfassungsentwicklungen ein. Wie auch in der Bill of Rights und der Déclaration des Droits de l'Homme et du Citoyen wird hier ganz allgemein die Freiheit des Einzelnen anerkannt und als eine kulturell dem Staate vorgegebene Grundbedingung verstanden.[451] Der Staat sollte verpflichtet werden, die Freiheit des Einzelnen zu achten. Damit steht die Funktion als Abwehrrecht gegenüber dem Staat bei Art. 2 Abs. 1 GG wie auch bei allen anderen Freiheitsgrundrechten im Vordergrund (sog. „status negativus").[452] In dieser Funktion dienen alle Freiheitsrechte dem Schutz von Freiheitsräumen und beschränken damit als objektiv geltendes Recht zunächst den Handlungs- und Entscheidungsspielraum des Staates. Sie sind insofern negative Kompetenznormen.[453] Auch die europäischen Grundrechte, so betont der *Europäischen Gerichtshofs für Menschenrechte*, seien in erster Linie Abwehrrechte.[454]

Darüber hinaus haben die Grundrechte auch eine objektiv-rechtliche Funktion: in den Grundrechten konstatiert sich der hohe Rang, den das Grundgesetz den geschützten Freiheiten und Gütern zuerkennt. Die Gesamtheit der Grundrechte wird auch als objektive Wertordnung[455] bezeichnet und in diesem Sinne wird darin eine objektive Wertenscheidung der Verfassung erkannt.[456] Nach dieser Lehre erschöpft sich die Funktion der Grundreche nicht darin dem Einzelnen Schutz vor Eingriffen in seine Freiheitssphäre zu gewähren, sondern es kann aus ihnen gefolgert werden, dass „sich mit der Entfaltung der Grundrechte als objektive Grundsatznormen die Bestimmungsmacht im Gemeinwesen vom volksgewählten Parlament hin zum *Bundesverfassungsgericht* verschiebt."[457] Dass dem so ist, zeigt letztlich auch die durch die Ewigkeitsgarantie erzeugte Beschränkung der Entscheidungsmacht des Gesetzgebers.

Dies sagt aber noch nichts darüber aus, welche und wie viel Freiheit durch Art. 2 Abs. 1 GG garantiert wird. Denn Art. 2 Abs. 1 GG gewährt keineswegs grenzenlose

---

450 *Murswiek*, in: *Sachs* (Hrsg.), Grundgesetz, Art. 2, Rn. 2 mit weiteren Nachweisen.

451 *Lorenz,* in: BK-GG 2011, Art. 2 Rn. 19.

452 Unterschieden werden aufbauend auf der Statuslehre *Jellineks* drei Funktionen der Grundreche. Im Vordergrund steht ihre Funktion als Abwehrrechte, Erst nachrangig ist ihre Funktion als Leistungsrechte und als staatsbürgerliche Teilhaberreche („status positivus" und „status activus"), *Müller-Franken*, in: *Schmidt-Bleibtreu/Klein*, GG 2011, Vorb. v. Art. 1, Rn. 11 f.; Es handle sich zwar nicht um ihre „ausschließliche, aber doch primäre Funktion", so *Sodan*, in: *Sodan,* GG, 2011, Vorb. v. Art. 1, 11.

453 *Müller-Franken*, in: *Schmidt-Bleibtreu/Klein*, GG 2011, Vorb. v. Art. 1, Rn. 15.

454 *Frenz* 2009, Rn. 319.

455 *Gusy*, AöR 1980 (105), 279, 292, kritisiert am Begriff der Wertordnung, dass er nicht logisch begründbar und so schon aus sich heraus nicht konsensfähig sei. Allerdings ist nicht ersichtlich, warum die Konzeption des Grundgesetzes mit den Grundrechten an seiner Spitze, nicht auch als Wertordnung ausgelegt werden könne. Denn in der Stellung der Grundrechte an der Spitze und den umfassenden Instrumenten zum Schutz kommt auch ein Systemverständnis zum Ausdruck. *Gusys* Kritik ist jedoch insofern zutreffend, als sie verdeutlicht, dass mit einer „Werteordnung" zurückhaltend argumentiert werden sollte. Soweit sich eine Wertordnung unmittelbar aus dem GG ableiten lässt, ist es zulässig, auf sie zurückzugreifen. Dabei sollte allerdings Vorsicht walten, um diese nicht über ihre tatsächlichen verfassungsrechtlichen Grundlagen hinaus zu überlasten.

456 *Müller-Franken*, in: *Schmidt-Bleibtreu/Klein*, GG 2011, Vorb. v. Art. 1, Rn. 15; BVerfGE 7, 205.

457 *Müller-Franken*, in: *Schmidt-Bleibtreu/Klein*, GG 2011, Vorb. v. Art. 1, Rn. 15.

Freiheit, sondern nur in den verfassungsrechtlichen Schranken, welche sich aus den Rechten anderer und der verfassungsmäßigen Ordnung ergeben.

Es wird zwischen zwei Teilgehalten unterschieden: der allgemeinen Handlungsfreiheit und dem allgemeinen Persönlichkeitsrecht. Während sich dieses auf die engere persönliche Lebenssphäre beschränkt, schützt die allgemeine Handlungsfreiheit jegliche Erscheinungsform menschlichen Verhaltens als aktives Element der Persönlichkeitsentfaltung.[458] Die allgemeine Handlungsfreiheit schützt insofern „grundsätzlich jedes Tun oder Unterlassen nach dem eigenen Willen, aber nicht jede Freiheit von staatlichem Zwang".[459] Der Schutzbereich der Freiheitsgrundrechte ist im Zweifel weit auszulegen, im Sinne eines Rechts auf beliebiges Verhalten.[460]

Neben dem „Allgemeinen Freiheitsrecht" aus Art. 2 Abs. 1 GG schützt das Grundgesetz darüber hinaus weitere speziellere Freiheitsrechte.[461] Als Individualfreiheiten werden geschützt: das Recht auf Leben und körperliche Unversehrtheit (Art. 2 Abs. 2), die Glaubens- und Gewissensfreiheit (Art. 4 Abs. 1 und Abs. 2; Art. 7 Abs. 2 und Abs. 3; Art. 140 GG), die Meinungs- und Informationsfreiheit sowie die Wissenschafts-, Forschungs- und Kunstfreiheit (Art. 5 Abs. 1 S. 1, 2 und Abs. 3 GG), die Erziehungsfreiheit (Art. 6 Abs. 2 GG), die Versammlungsfreiheit (Art. 8 Abs. 1 GG), die Vereinigungsfreiheit (Art. 9 Abs. 1 GG), die Telekommunikationsfreiheit (Art. 10 Abs. 1 GG), die Freizügigkeit im Bundesgebiet (Art. 11 Abs. 1 GG), die Berufsfreiheit (Art. 12 Abs. 1 GG), die Unverletzlichkeit der Wohnung (Art. 13 Abs. 1 GG). Diese Grundrechte beschreiben einzelne, partielle Freiheitsräume, welche die Verfassung neben der Allgemeinen Handlungsfreiheit und dem Recht auf freie Entfaltung der Persönlichkeit schützt.

Allein aus der Normierung der Grundrechte an der Spitze der Verfassung lässt sich keine Normenhierarchie oder Wertordnung ableiten.[462] Es besteht auch keine Rangordnung zwischen den einzelnen Freiheitsrechten, die sich aus ihrer Position im Grundgesetz ableiten ließe. Dennoch ist die Stellung der Grundrechte als erstem Teil der Verfassung nicht ohne jede Bedeutung. So lässt sich daraus der Wille des Verfassungsgebers ablesen, dass der „für ein Leben des Einzelnen in Würde und Selbstachtung essentielle Katalog der Grundrechte die Verfassungswirklichkeit bestimmen und die Freiheit des Menschen im Vordergrund stehen sollte."[463]

---

458 *Lorenz,* in: BK-GG 2011, Art. 2 Rn. 15.

459 *Merten*, in: HGR I, 2006, § 27 Rn.18; Dies wird auch deutlich in der Interpretation von Menschenwürde und Freiheit, wie sie zuvor erfolgt ist: Wenn die Menschenwürde die innere Freiheit zur Selbstentfaltung schützt, schützt die allgemeine Handlungsfreiheit die äußere. Freiheit bei der Selbstdarstellung setzt aber keine Freiheit von jeder Determination voraus, sondern erfordert lediglich Freiheit von offensichtlichem Zwang; *Luhmann* 1999, 66, 77 ff.

460 *Kahl*, Der Staat 2004, 167, 168, 199ff. So zumindest bislang die hM (zahlreiche Nachweise bei Kahl, Fn. 16); zunehmend ist jedoch eine Tendenz feststellbar die Schutzbereiche zu verengen, dazu *Ders.,* 169 ff.

461 *Müller-Franken*, in: *Schmidt-Bleibtreu/Klein*, GG 2011, Vorb. v. Art. 1, Rn. 6.

462 *Merten, in:* HGR I, 2006, § 27 Rn.7.

463 *Merten, in:* HGR I, 2006, § 27 Rn. 9.

Die einzelnen Freiheitsrechte weisen einen Regel-Ausnahme-Grundsatz auf, wonach die Freiheit prinzipiell unbegrenzt ist, während die Staatseinwirkung prinzipiell begrenzt ist. Anders lässt sich formulieren, dass die Regel die Liberalität ist und deren Beschränkung nur die Ausnahme bildet.[464] Jeder Eingriff in ein Grundrecht, ob Freiheitsrecht oder nicht, muss gerechtfertigt werden.[465] Das *Bundesverfassungsgericht* geht vom modernen Eingriffsbegriff[466] aus und nimmt an, dass jedes staatliche Handeln, das dem Einzelnen ein Verhalten, das in den Schutzbereich eines Grundrechts fällt, erheblich erschwert oder unmöglich macht, einen Grundrechtseingriff darstellt.[467]

Es wird vertreten, dass mit den Grundrechten die Freiheit negativ definiert würde, als Freiheit von Einwirkungen der Staatsgewalt.[468] Zutreffend ist zwar, dass den Grundrechten zunächst die Funktion als Abwehrrechte gegenüber dem Staat zukommt, allerdings beschränkt sich die Definition der Freiheit, die durch die Grundrechte erfolgt, nicht auf diese Funktion. Vielmehr wird durch die Beschreibung der einzelnen partiellen Freiheitsgarantien Freiheit gerade auch positiv definiert und zwar (unter anderem) als Freiheit im religiösen Glauben und Handeln, zur Meinungsäußerung, der Presse und des Rundfunks, dazu sich zu vereinigen und zu versammeln, Eigentum zu haben, als freie Entfaltung der Persönlichkeit, als Gewissensfreiheit, als Recht auf informationelle Selbstbestimmung und als Telekommunikationsfreiheit.

Anders als im Grundgesetz gewährt Art. 6 EU-GRCh., wie auch Art. 5 Abs. 1 EMRK, jedem Menschen ein Recht auf Freiheit und Sicherheit. Dieses statuiert einen Schutz vor Freiheitsentzug. Es geht insofern „nicht um die allgemeine Entfaltung der Persönlichkeit, sondern um eine Beschränkung der physischen Fortbewegungsmöglichkeiten".[469] Der *Europäische Gerichtshof* hat allerdings die allgemeine Handlungsfreiheit als einen Grundsatz des Gemeinschaftsrechts erkannt.[470] Zudem ist die Garantie des Art. 53 EU-GRCh. zu beachten, dass keine Bestimmung der Charta im Sinne einer

---

464 *Merten, in:* HGR I, 2006, § 27 Rn. 19.

465 Zur Rechtfertigung von Grundrechtseingriffen dienen Grundrechtsschranken. Lediglich dann wenn ein Eingriff nicht von den Grundrechtsschranken gedeckt ist, oder eben deren sog. Schranken-Schranken überschreitet, liegt eine Grundrechtsverletzung vor, *Kloepfer,* Verfassungsrecht II 2010, § 51, Rn. 39.

466 BVerfGE 105, 279 (299 ff.) In Abgrenzung zum klassischen Eingriffsbegriff: „Danach wird unter einem Grundrechtseingriff im Allgemeinen ein rechtsförmiger Vorgang verstanden, der unmittelbar und gezielt (final) durch ein vom Staat verfügtes, erforderlichenfalls zwangsweise durchzusetzendes Ge- oder Verbot, also imperativ, zu einer Verkürzung grundrechtlicher Freiheiten führt."

467 Eine „mittelbar, faktische Wirkung" genügt demnach, so das BVerfGE 105, 279 (300f.).

468 *Isensee,* in: *Isensee/Kirchof* HStR IV, § 71 Rn. 79.

469 *Frenz* 2009, Rn. 1060.

470 *Frenz* 2009, Rn. 1062 ff. m.w.N. Fn. 5. Allerdings hat auch der *EuGH* in der späteren Rspr nicht mehr auf einen übergreifenden Grundsatz der allgemeinen Handlungsfreiheit zurückgegriffen. Vielmehr hat das Gericht nunmehr das generelle Erfordernis eines Schutzes gegen willkürliche oder unverhältnismäßige Eingriffe betont, was den Rechtsordnungen aller Mitgliedstaaten zu entnehmen sei. Eine allgemeine Handlungsfreiheit wie im deutschen Verfassungsrecht gibt es hingegen in anderen Mitgliedstaten nicht. Insofern betont das Gericht nunmehr generell, dass jegliche Eingriffe der öffentlichen Gewalt in die Sphäre der privaten Betätigung von natürlichen oder juristischen Personen aus den gesetzlich vorgesehenen Gründen gerechtfertigt sein müssen. Vgl. zur Gewährleistung der Freiheit der Person durch EMRK und EGCR auch ausführlich *Dörr*, EMRK/GG, Kap. 13.

Verkürzung eines im Unionsrecht bereits anerkannten Menschenrechts ausgelegt werden darf.

Letztlich beinhalten weder die EU-GRCh. noch die EMRK ein mit Art. 2 Abs. 1 GG vergleichbares Auffanggrundrecht und somit auch keine Garantie der allgemeinen Handlungsfreiheit. Schutzlücken sind dadurch aber nicht zwingend gegeben, da die einzelnen europarechtlichen Grundrechtsverbürgungen jeweils einen umfassenden Schutz zahlreicher spezifischer Freiheiten beinhalten. So schützen EU-GRCh. und die EMRK als Individualfreiheiten, das Recht auf Leben (Art. 2 Abs. 1 EMRK), den Schutz vor Folter, Sklaverei und Zwangsarbeit (Art. 3, 4 EMRK); den Schutz des Privat- und Familienlebens sowie der Kommunikation (Art. 7 EU-GRCh.; Art. 8 Abs. 1 EMRK), der Schutz personenbezogener Daten (Art. 8 Abs. 1 EU-GRCh.), die Freiheit eine Ehe zu schließen und eine Familie zu gründen (Art. 9 EU-GRCh.), die Gedankens-, Gewissens- und Religionsfreiheit (Art. 10 Abs. 1 EU-GRCh.; Art. 9 EMRK), die Meinungs-, Informations-und Medienfreiheit (Art. 11 Abs. 1 und Abs. 2 EU-GRCh.; Art. 10 EMRK), die Versammlungs- und Vereinigungsfreiheit (Art. 12 Abs. 1 EU-GRCh.; Art. 11 EMRK), die Kunst- und Wissenschaftsfreiheit (Art. 13 EU-GRCh.), die Freiheit zur Gründung von Lehranstalten sowie die Erziehungsfreiheit (Art. 14 Abs. 3 EU-GRCh.), die Berufsfreiheit (Art. 15 Abs. 1 und 2 EU-GRCh.), die unternehmerische Freiheit (Art. 16 EU-GRCh.), die Eigentumsfreiheit (Art. 17 EU-GRCh.), das Asylrecht (Art. 18 EU-GRCh.) sowie den Schutz bei Abschiebung (Art. 19 EU-GRCh.).

2.1.3 Zentrale Freiheitsrechte im digitalen Zeitalter

Fraglich ist, ob die umfassenden Freiheitsrechte, wie sie im Grundgesetz vor über sechzig Jahren formuliert wurden, auch jene für die freie Entfaltung des Einzelnen im digitalen Zeitalter erforderlichen Freiheitsräume ausreichend zu schützen vermögen. Es werden daher die für die freie Entfaltung des Einzelnen unter den Bedingungen des digitalen Zeitalters besonders bedeutenden Freiheitsrechte vertieft untersucht. Im Einzelnen werden das Recht auf informationelle Selbstbestimmung, das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme und das Telekommunikationsgeheimnis erörtert. Dabei wird auch berücksichtigt, inwiefern diese durch die jüngeren Garantien in EMRK und EU-GRCh. geprägt sind. Notwendig ist diese abstrakte Untersuchung für die folgende Untersuchung der Vorratsdatenspeicherung, da hier die rechtlichen Grundlagen für die im Folgenden durchzuführende Abwägung aufgezeigt und dargestellt werden. Ohne ein Verständnis davon inwieweit das (verfassungs-)rechtliche System der Bundesrepublik Freiheit und Sicherheit schützt und garantiert, ist es nicht möglich, ein spezifisches sicherheitspolitisches Instrument in dieses einzuordnen.

2.1.3.1 Informationelle Selbstbestimmung

Das Grundrecht auf informationelle Selbstbestimmung ist nicht ausdrücklich im Grundrechtskatalog normiert. Es wurde 1983 vom *Bundesverfassungsgericht* im Volkszählungsurteil anerkannt und zwar als (Grund-)Recht, „grundsätzlich selbst zu entscheiden, wann und innerhalb welcher Grenzen persönliche Lebenssachverhalte of-

fenbart werden“, und „selbst über die Preisgabe und Verwendung persönlicher Daten bestimmen zu können“.[471]

Es handelt sich um eine Ausprägung des Allgemeinen Persönlichkeitsrechts, die als solche im Grundgesetz verankert ist. Lediglich die Ausprägung als ein Recht über personenbezogene Daten selbst zu bestimmen, ist hierbei neu und als Reaktion auf die technischen Neuerungen zu sehen.[472] Abgeleitet wird es aus Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG.

Entsprechend fußt das informationelle Selbstbestimmungsrecht auf dem Gedanken der Selbstbestimmung.[473] Eine allgemeine Unsicherheit darüber, ob die eigenen Verhaltensweisen staatlich beobachtet, notiert und in unterschiedlichen Zusammenhängen verwendet werden, ist mit dem Selbstbestimmungsgrundsatz nicht in Übereinstimmung zu bringen. Deshalb erfasst der Schutzbereich des Grundrechts auch, dass jeder Einzelne erwarten darf, nicht zum bloßen Objekt heimlicher Beobachtungstätigkeit des Staates zu werden.[474]

Zu den zentralen Erkenntnissen des Volkszählungsurteils gehört die Feststellung, dass es kein „belangloses“ Datum gibt. Denn entscheidend für das Eingriffsgewicht der Erhebung oder Verwendung eines personenbezogenen Datums ist nicht allein ihr punktueller Informationsgehalt. Vielmehr kommt es auch auf Nutzungs- und Verwendungsmöglichkeiten an.[475] „Diese hängen einerseits von dem Zweck, dem die Erhebung dient, und andererseits von den der Informationstechnologie eigenen Verarbeitungs- und Verknüpfungsmöglichkeiten ab. Dadurch kann ein für sich gesehen belangloses Datum einen neuen Stellenwert bekommen“.[476]

Hinter der informationellen Selbstbestimmung verbirgt sich neben diesen individualrechtlichen Aspekten auch eine Umschreibung der Struktur der Gesellschaft.[477] Es handelt sich also nicht nur um ein individuelles Schutzrecht. Denn informationelle Selbstbestimmung ist eine „elementrare Funktionsbedingung eines auf Handlungs- und Mitwirkungsfähigkeit seiner Bürger begründeten freiheitlich-demokratischen Gemeinwesens“, so das *Bundesverfassungsgericht*.[478] Daher genügt es nicht, dass das Gewicht der für eine Einschränkung maßgebenden Allgemeininteressen allein die für den Betroffenen zu erwartenden Beeinträchtigungen überwiegt. Es sind vielmehr auch andere denkbare Nachteile einzubeziehen, die das staatliche Gemeinwesen erleidet, da

---

471 BVerfGE 65, 1. Die Wurzeln in der Literatur sind älter, dazu *Trute* 2003, 162 Fn. 27.
472 So auch *Benda*, DUD 1984, 86, 89
473 BVerfGE 65, 1 (1, LS 1; 43).
474 *Neumann* 1993, 125.
475 Es handelt sich insofern um eine Abkehr von der bis dahin vertretenen Sphärentheorie, ausführlich dazu *Desoi/Knierim*, DÖV 2011, 398; *Simitis*, NJW 1984, 394 ff., 402; *Simitis,* in: *Simitis,* BDSG Komm 2011, § 1, Rn. 65 ff.
476 BVerfGE 65, 1, 45.
477 *Simitis*, NJW 1984, 394 ff., 399; vgl. dazu auch *Gusy* 2011, 410.
478 BVerfGE 65, 1, (43).

der Staat für seine Funktionsfähigkeit auf die informationelle Selbstbestimmung seiner Bürger angewiesen ist.[479]

2.1.3.1.1 Personenbezug von Daten

Da es sich bei dem informationellen Selbstbestimmungsrecht um ein Individualrecht handelt, ist es nur anwendbar, soweit Gegenstand der Erhebung oder Verarbeitung ein personenbezogenes Datum ist.[480] In § 3 Abs. 1 BDSG werden sie als „Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person" definiert. Art. 2 a) der EU-Datenschutzrichtlinie[481] definiert sie als „alle Informationen über eine bestimmte oder bestimmbare natürliche Person ("betroffene Person"); als bestimmbar wird eine Person angesehen, die direkt oder indirekt identifiziert werden kann, insbesondere durch Zuordnung zu einer Kennnummer oder zu einem oder mehreren spezifischen Elementen, die Ausdruck ihrer physischen, physiologischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität sind."

Es besteht weitgehend Einigkeit, dass der Personenbezug relativ zu bestimmt ist.[482] Das heißt, es wird kein abstraktes Urteil gefällt, ob ein Datum personenbezogen ist, sondern jeweils gefragt, ob die verarbeitende Stelle einen Personenbezug herstellen kann, also ob sie über das erforderliche Zusatzwissen verfügt, um einen solchen zu erzeugen. Danach ist eine Person bestimmbar, wenn die Identität von der verantwortlichen Stelle mit Hilfe von zusätzlichen, ihr gerade zur Verfügung stehenden oder zugänglichen Informationen, festgestellt werden kann.[483] Das gleiche Datum kann daher für eine verantwortliche Stelle personenbezogen sein, während es für eine andere Stelle nicht personenbezogen ist.[484] Für diese relative Betrachtungsweise spricht ganz eindeutig, dass, wenn es nicht auf die Möglichkeiten der jeweils verarbeitenden Stelle an-

---

479 *Baumann*, DVBl. 1984, 612, 614.

480 *Jarass,* in: *Jarass/Pieroth,* GG 2011, Art. 2 Rn. 43; *Damann,* in: *Simitis,* BDSG Komm 2011, § 3 Rn. 20 (für die Anwendbarkeit des BDSG kommt es darauf an, ob eine Person „bestimmt oder bestimmbar ist); *Pahlen-Brandt*, DuD 2008, 34.

481 RL 95/46/EG des Europäischen Parlaments und des Rates v. 24.10.1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr, Abl. Nr. L 281 v. 23.11.1995, S. 0031 – 0050; zu den Ansätzen einer Reform des Europäischen Datenschutzrechts in der Datenschutz-Grundverordnung, unten S. 91 f.

482 *Spindler/Nink,* in: *Spindler/Schuster,* 2011, § 11 TMG, Rn. 5, 5a; *Polenz,* in: *Kilian/Heussen* 2011, Teil 13 Rn. 68; *Dammann*, in: *Simitis,* BDSG Komm 2011, § 3 Rn. 32; a.A.: *Pahlen-Brandt* davon aus, dass ein Datum schon dann personenbezogen ist, wenn eine Zuordnung zu einem Individuum nur theoretisch möglich ist (sog. „objektive Theorie") *Pahlen-Brandt*, DuD 2008, 34, 38f. Schließlich stellt eine vermittelnde Ansicht nur dann allein auf das Wissen der verantwortlichen Stelle ab, wenn die Verarbeitung der Daten auch nur in einem geschlossenen Netzwerk stattfindet, dazu ausführlich *Forgó*/*Krügel*, MMR 2010, 17, 18; einen vermittelnden Ansatz vertritt auch *Buchner*, in: *Taeger/Gabel,* BDSG, § 3, Rn. 13; Gegen eine „objektive Theorie" spricht jedoch, dass theoretisch möglich eine Zuordnung zu einer Person immer sein könnte. Zudem besteht die Schwierigkeit, dass sollte im Sinne der objektiven Betrachtung jegliches Zusatzwissen relevant sein, es für die verarbeitende Stelle überhaupt nicht absehbar ist, ob es sich nun um ein personenbezogenes Datum handelt und das Datenschutzrecht Anwendung findet oder nicht.

483 *Hornung*, DuD 2004, 218; *Dammann*, in: *Simitis,* BDSG Komm 2011, § 3 Rn. 22, 32.

484 *Roßnagel*/*Scholz*, MMR 2000, 721, 723; *Hornung*, DuD 2004, 218; *Gola*/*Klug/Schomerus*, BDSG, 2010, § 3 Rn. 10.

kommen sollte, letztlich kaum mehr ein Datum nicht personenbezogen wäre.[485] Auch wenn weitgehend Einigkeit besteht, dass der Personenbezug relativ zu bestimmen ist, wird darüber gestritten, welches Wissen der verarbeitenden Stille zugerechnet werden muss. Kommt es nur auf das Wissen an über das die jeweilige Stelle rechtmäßig verfügt, oder kann ihr etwa auch möglicherweise rechtswidrig zu erlangendes Wissen zugerechnet werden?[486]

Dieser Streit spiegelt sich im Diskurs um die Frage, ob es sich bei dynamischen IP-Adressen um ein personenbezogenes Datum handelt. Statische IP-Adressen werden stets als personenbezogenes Datum betrachtet, da grundsätzlich die Zuordnung der statischen IP-Adresse zum Inhaber möglich ist.[487] Dies ist für dynamische IP-Adressen allerdings nicht möglich, da diese durch den Internet-Zugangsanbieter jeweils nur temporär dem Nutzer zugeordnet werden.[488]

Unstrittig ist, dass dynamische IP-Adressen für den Internet-Provider personenbezogene Daten sind. Umstritten ist hingegen, ob es sich bei dynamischen IP-Adressen generell um personenbezogene Daten handelt.[489] Hier ist entscheidend, welches Wissen man der verantwortlichen Stelle zurechnet.

Die Ansicht, dass auch Wissen, das möglicherweise rechtswidrig erlangt werden könnte, der verarbeitenden Stelle zugerechnet werden muss, kann nicht überzeugen. Denn ihre Prämisse ist, dass die verarbeitende Stelle rechtswidrig handelt. Diese widerspricht der Rechtsstaatlichkeit und der im Grundgesetz normierten Bindung der Exekutive an Gesetz und Recht. Und auch Private sind grundsätzlich zur Beachtung der Gesetze verpflichtet. Zwar wird immer wieder gegen Gesetze verstoßen, dafür gibt es Sanktionen und Rechtsmittel. Der Rechtsstaat hebt sich aber selbst auf, wenn er grundsätzlich rechtswidriges Handeln seiner Akteure sowie von Privaten unterstellt.

Damit sollen Gesetzesverstöße und die Möglichkeit, dass sie begangen werden, nicht grundsätzlich ausgeschlossen werden. Sie können aber nicht ohne weitere Anhaltspunkte jedwedem Akteur unterstellt werden. Gerade im Bereich der Datenverarbeitung wurde das Vertrauen in verschiedene Unternehmen wiederholt durch Skandale über

---

485 *Eckhardt*, CR 2011, 339, 342.

486 *Weichert*, in: *Däubler/Klebe/Wedde/Weichert* BDSG 2010, § 3 Rn. 13; *Karg*, MMR-Aktuell, 315811.

487 *Eckhardt*, CR 2011, 339, 340; *Dammann,* in: *Simitis,* BDSG Komm 2011, § 3 Rn. 63; a.A. *Heidrich/Wegener,* DUD 2010, 172, 174; Dabei ist zu beachten, dass eine IP-Adresse nur dann personenbezogenes Datum ist, wenn der Inhaber eine natürliche Person ist.

488 *Eckhardt*, CR 2011, 339, 340.

489 Für eine objektive Einordnung stets als personenbezogenes Datum: *Karg*, MMR-Aktuell, 315811 a.A.: *Meyerdierks*, MMR 2009, 8, 13; *Eckhardt*, CR 2011, 339; *Spindler/,* in: *Spindler/Schuster,* 2011, § 11 TMG, Rn. 5b; *Krüger/Maucher*, MMR 2011, 433. Im Sinne der objektiven Betrachtung stellte etwa 2007 das *AG Berlin Mitte* fest, dass alle IP-Adressen personenbezogene Daten seien; a.A.: *AG Münch*en, Urt. 30.09.2008 - 133 C 5677/08, abgedr. in MMR 2008, 860. Ein Personenbezug sei nur dann gegeben, wenn die Herstellung der Beziehung zwischen Datum und Person nicht mit einem unverhältnismäßigen Aufwand verbunden sei. In diesem Sinne auch: *OLG Hamburg*, Urt. v. 3.11.2010 - 5 W 126/10, CR 2011, 126, Ermittlung von IP-Adressen in „File-Sharing-Fällen".

die missbräuchliche Nutzung personenbezogener Daten erschüttert. In konkreten Fällen muss, wenn Tatsachen einen Missbrauch belegen, dies in die Bewertung einfließen. Beispielsweise wenn bekannt wird, dass ein Unternehmen rechtswidrig den Personenbezug herstellt. Dann muss für dieses Unternehmen, da es über das erforderliche Wissen verfügt auch rechtswidrig erlangbares Zusatzwissen bei der Bestimmung des Personenbezugs miteinbezogen werden.

Es ist insofern nicht erforderlich und erst recht nicht geboten, generell rechtswidriges Verhalten zu unterstellen. Es genügt eine relative Betrachtung nach welcher, der verantwortlichen Stelle das ihr zur Verfügung stehende Wissen zugerechnet wird. Sobald ein Zusammenhang herstellbar ist, ist das Datenschutzrecht anwendbar.[490]

2.1.3.1.2 Eingriff und Eingriffsgewicht

Jeder Eingriff in die informationelle Selbstbestimmung, also jede Erhebung, Verarbeitung und Nutzung eines personenbezogenen Datums, muss gerechtfertigt werden. Der Grundrechtseingriff verlange, so wird vertreten, eine „Entprivatisierung personenbezogener Informationen", die erst bei einer Kenntnisnahme gegeben sei.[491] Andere stellen allein darauf ab, ob ein personenbezogenes Datum verarbeitet wird und nicht ob eine Person oder Institution aktiv Kenntnis von dem Datum erlangt.[492] Diese Ansicht überzeugt. Denn es kann gerade bei Eingriffen in die informationelle Selbstbestimmung nicht darauf ankommt, ob eine Kenntnisnahme vorliegt. Der Eingriff liegt in der Erhebung, Speicherung oder Verarbeitung. Ob die Daten später zur Kenntnis genommen werden, hat Einfluss auf das Eingriffsgesicht, nicht aber auf die Frage, ob überhaupt ein Eingriff vorliegt.

Wichtig für die Rechtfertigungsfähigkeit und damit für die Anforderungen an die Zulässigkeit eines Eingriffs, ist die Bestimmung des Eingriffsgewichts.[493] Das Übermaßverbot[494] verlangt, dass je schwerer ein Eingriff wiegt, umso schwerer müssen auch die Belange wiegen, die den Eingriff rechtfertigen. Zudem ist in der Verfassungsrechtsprechung anerkannt, dass die Anforderungen an die Bestimmtheit desto höher sind, je schwerer der Grundrechtseingriff wiegt.[495] Auch der Richtervorbehalt als verfahrens-

---

[490] *Eckhardt*, CR 2011, 339, 343 f.; Verweist hier auch darauf, dass dies sich auch für IPv6-Adressen nicht grundsätzlich ändern würde. Er empfiehlt zudem in einer mehrstufigen Prüfung zu ermitteln, ob ein Personenbezug vorliegt: 1. Bestimmung des datenschutzrechtlich verantwortlichen Unternehmens; 2. Bestimmung der (legalen soweit nicht tatsächlich illegales Verhalten gegeben ist) Möglichkeiten zur Herstellung des Personenbezugs; 3. Prüfung der Bestimmtheit oder Bestimmbarkeit der Information für die verantwortliche Stelle im Zeitpunkt der Bewertung; 4: Wird das Datum durch eine Selbstidentifikation des Nutzers zu einem personenbezogenen Datum?; a.A. *Freund/Schnabel*, MMR 2011, 495, 497.ff., die davon ausgehen, dass es sich wegen der vorwiegend statischen Vergabe bei IPv6 Adressen nach beiden Ansichten um personenbezogene Daten handle.

[491] *Gusy* 2011, 406; unter Hinweis auf BVerfGE 120, 378 (399) - *Kfz-Kennzeichenscanning.*

[492] *Dammann,* in: *Simitis,* BDSG Komm 2011, § 3 Rn. 106.

[493] *Gusy* 2011, 397.

[494] Zum Ursprung des Übermaßverbots und seinem Prüfungsumfang noch ausführlich unten, Kap. 2.1.4.2.2.

[495] BVerfGE 113, 348 (377 f.); 115, 320 (365); 120, 378 (408).

rechtliche Sicherung wird allein bei besonders schwerwiegenden Eingriffen gefordert.[496]

Für die Bestimmung des Eingriffsgewichts spielen in der Rechtsprechung des *Bundesverfassungsgerichts* verschiedene Faktoren eine Rolle.[497] Wesentlich sei die Anzahl der betroffenen Grundrechtsträger und ob diese einen Anlass für den Eingriff gegeben haben.[498] Denn je höher die Streubreite sei, desto stärkere Einschüchterungseffekte gingen von einem Eingriff aus. Die Anlasslosigkeit verursache ein Gefühl ständiger Kontrolle.[499] Auch komme es auf die „Intensität der individuellen Beeinträchtigung§ an.[500] Darüber hinaus kommt es nach Ansicht des Verfassungsgerichts darauf an, welche Inhalte von dem Eingriff erfasst werden und dabei darauf „welchen Grad an Persönlichkeitsrelevanz die betroffenen Informationen je für sich und in ihrer Verknüpfung mit anderen aufweisen".[501] Von Bedeutung für das Eingriffsgewicht ist nicht die Art des Datums, sondern vor allem, welche Verwendungsmöglichkeiten es gibt. Grundsätzlich gebe es kein belangloses Datum.[502] Auch spielt es eine Rolle, welche belastenden Auswirkungen mit dem Eingriff verknüpft sind. Weiter ist für die Eingriffsintensität entscheidend, ob dieser heimlich erfolgt. Da in einem Rechtsstaat die „Heimlichkeit staatlicher Eingriffsmaßnahmen die Ausnahme" bildet und daher einer besonderen Rechtfertigung bedürfe.[503] Schließlich verliert der Einzelne aufgrund der Heimlichkeit sowohl die Möglichkeit Rechtsschutz zu suchen, als auch faktisch durch sein Verhalten auf den Gang des Verfahrens einzuwirken. Aufgrund dessen wird das Gewicht des Grundrechtseingriffs verstärkt.[504] Eine Rolle spielt darüber hinaus auch, ob der Eingriff alternativlos ist – oder ob dem Einzelnen die Möglichkeit verbleibt dem Eingriff auszuweichen.[505]

---

496 *Gusy* 2011, 398; Dazu auch ausführlich unten 9.1.2.1.3.3, S. 278 f.

497 Die eingriffssteigernde Wirkung einzelner Faktoren ist zum Teil umstritten. Dies soll aber nicht hier vorab abstrakt diskutiert werden, sondern im Folgenden soweit dies relevant wird, dazu unten Kap. 9.1.2.1.3.1.

498 BVerfGE 115, 320 (357); unter Verweis auf 107, 299 (328); im Folgenden auch BVerfGE 120, 378 (396); 125, 260 (305).

499 BVerfGE 120, 378 (430); in diesem Sinne auch BVerfGE 125, 260 (335); kritisch dazu hinterfragt *Gusy* „Geht es beim Datenschutz um Rechtsschutz oder um Gefühlsschutz? Können Einschüchterungseffekte bei heimlichen Informationseingriffen überhaupt entstehen? Und wie sollen diese Gefühle ermittelt und gewichtet werden?" in: 2011, 402. Die Kritik an der Einbeziehung überindividueller (potentieller) Wirkungen in die Bewertung des Eingriffs fußt auf der Annahme, dass die Informationelle Selbstbestimmung allein Individualgrundrecht sei, so etwa 16 f.; 62 f. bzw. dass Gefühle nicht rechtlich geschützt seien. *Gusy* zeigt jedoch überzeugend auf, dass durchaus der Grundgedanke einer freien Gesellschaft und ihres Schutzes auch durch die Grundrechte anerkennenswert sei. Die Schwierigkeit bestünde zwar darin, dass ein Einschüchterungsverbot nur schwer in allgemein gültige Handlungs- und Entscheidungsnormen umgesetzt werden könne, dies mindere aber nicht ihre rechtliche Relevanz, erschwere allerdings die Rationalisierung von Ableitungen und die Legitimation von Entscheidungen; *Gusy* 2011, 412.

500 BVerfGE 115, 320 (347); in diesem Sinne auch 100, 313 (376); 107, 299 (318 ff.); 109, 279 (353).

501 Vgl. Fn. 500.

502 BVerfGE 65, 1 (45).

503 BVerfGE 120, 274 (325); mit Verweis auf BVerfGE 118, 168 (197).

504 BVerfGE 113, 348 (383 f.); 115, 320 (353); 120, 274 (325).

505 BVerfGE 125, 260 (319).

Eine Analyse der Verfassungsrechtsprechung führt zu der Feststellung, dass das Gericht zwar immer wieder besonders schwerwiegende Eingriffe festgestellt hat, aber es bislang keinen Eingriff als grundsätzlich unzulässig erklärt hat. Es hat daraus jeweils nur erhöhte Zulässigkeitsvoraussetzungen abgeleitet.[506]

2.1.3.1.3 Datenschutzrechtliche Grundprinzipien

Soweit ein personenbezogenes Datum erhoben, verarbeitet oder genutzt wird, ist der Schutzbereich des Rechts auf informationelle Selbstbestimmung betroffen. Damit findet das Datenschutzrecht Anwendung. Das Datenschutzrecht ist geprägt durch verschiedene Prinzipien, die im Folgenden überblicksartig skizziert werden, um zu verdeutlichen unter welchen Bedingungen eine Erhebung und Verarbeitung personenbezogener Daten zulässig ist. Die Prinzipien wurzeln sämtlich im Volkszählungsurteil, wurden seitdem aber durch Literatur und Rechtsprechung weiter geformt und konkretisiert. Da die Verarbeitung personenbezogener Daten in einer digitalisierten Welt schon heute allgegenwärtig ist, sind die Datenschutzgrundsätze für die Rechtswirklichkeit und Gewährleistungsfähigkeit der informationellen Selbstbestimmung und damit zur freien Entfaltung der Persönlichkeit unter den Bedingungen moderner Datenverarbeitung von herausragender Bedeutung.[507]

2.1.3.1.3.1 Zweckbindungsgrundsatz

Der Zweckbindungsgrundsatz soll sicherstellen, dass die von einer Datenverarbeitung betroffene Person in die Lage versetzt wird, die sie betreffenden Daten entsprechend ihrer sozialen Rolle im jeweiligen sozialen Kontext selbst zu steuern.[508] Er sieht vor, dass personenbezogene Daten für festgelegte eindeutige und rechtmäßige Zwecke erhoben und nicht in einer, mit diesen Zweckbestimmungen nicht zu vereinbarenden, Weise weiter verarbeitet werden dürfen.[509]

Ausgeschlossen wird damit auch eine Speicherung von Daten auf Vorrat im Sinne einer Speicherung für nicht bekannte Zwecke. Um dem Zweckbindungsgrundsatz zu entsprechen muss das Ziel der Erhebung und Benutzung der Daten so genau wie möglich definiert sein. Dem genügen bloß vage Beschreibungen des Gegenstands der Verarbeitung (etwa für Strafverfolgungszwecke) nicht. Grundsätzlich muss die Zweckbestimmung bereits im Zeitpunkt der Datenerhebung feststehen. Eine spätere Zweckänderung ist nur dann zulässig, wenn sie mit der ursprünglichen Zweckbestimmung in Einklang steht.[510] Der Zweckbindungsgrundsatz findet sich auch in Art. 6 Abs. 1 b) der DSRL und auch das BDSG verlangt die rechtzeitige und eindeutige Festlegung der Zweckbestimmung.[511]

---

[506] *Gusy* 2011, 398.

[507] Zu den Grundsätzen und dem Erfordernis einer Modernisierung des Datenschutzrechts *Roßnagel/Pfitzmann/Garstka* 2011; *Roßnagel,* Hb. DSR 2003.

[508] *Roßnagel* 2007, 116.

[509] Das *BVerfG* verlangt eine bereichsspezifische und präzise Zweckfestlegung; BVerfGE 65, 1 (46).

[510] *Gola/Klug* 2003, 48.

[511] z. B. Im Zusammenhang mit dem Direkterhebungsgrundsatz in § 4 Abs. 3; § 28 Abs. 1 S. 2 BDSG; im öffentlichen Bereich muss die Verarbeitung für die jeweilige Aufgabenerfüllung

2.1.3.1.3.2 Grundsatz der Erforderlichkeit

Die Verarbeitung personenbezogener Daten ist nur soweit zulässig, als sie erforderlich ist, um den zulässigen Zweck zu erreichen. Was so viel bedeutet wie, dass Daten nur, soweit sie für das Erreichen des Zwecks unbedingt benötigt werden, verarbeitet werden dürfen.[512] Die Erforderlichkeit beschränkt jeweils im konkreten Einzelfall als materiell-rechtliche Anforderung den Umfang der Datenverarbeitung.[513] Der Grundsatz der Erforderlichkeit findet seinen Niederschlag in zahlreichen Bestimmungen des BDSG.[514] Grundsätzlich ist danach die Speicherung und nachfolgende Verwendung personenbezogener Daten nur legitimiert, wenn und soweit sie zur Erfüllung von Pflichten oder zur Wahrnehmung von Rechten gespeichert werden müssen oder für diese Zwecke benötigt werden.[515]

2.1.3.1.3.3 Grundsatz der Datensparsamkeit und Datenvermeidung

Der Grundsatz der Datenvermeidung und Datensparsamkeit wird als Konkretisierung des Grundsatzes der Vorsorge für die technische Gestaltung der Datenverarbeitung verstanden.[516] Die Gefahren für das informationelle Selbstbestimmungsrecht des Betroffenen sollen soweit wie möglich minimiert werden, indem die Erhebung, Verarbeitung und Nutzung personenbezogener Daten möglichst reduziert wird. Der im Grundsatz der Datensparsamkeit und Datenvermeidung enthaltene Auftrag verlangt, dass die Erhebung von personenbezogenen Daten wenn möglich verhindert wird. Stattdessen sollen Systeme mit anonymisierten oder pseudonymisierten Daten arbeiten.[517]

2.1.3.1.3.4 Transparenz

Da das Recht auf informationelle Selbstbestimmung nur wirkungsvoll ist, wenn der Betroffene überprüfen kann, ob datenverarbeitende Maßnahmen rechtmäßig ablaufen, ist eine transparente Datenerhebung und -verarbeitung geboten. Daher wird grundsätzlich eine gegenüber dem Bürger offene und direkte Erhebung verlangt.[518] Darüber hinaus ist der Betroffene ordnungsgemäß und umfassend über die Bedingungen der ihn betreffenden Datenverarbeitungsmaßnahmen zu informieren.[519] Neben dem Grundsatz der Direkterhebung und den damit verbundenen Unterrichtungspflichten sind ergänzend Benachrichtigungs- und Auskunftspflichten anerkannt, um dem Transparenzgebot zu entsprechen.

---

der öffentlichen Stelle erforderlich sein; §§ 13 Abs. 1, 14 Abs. 1, 15 Abs. 1 Nr.1, 16 Abs. 1 Nr. 1 BDSG.

512 *Roßnagel* 2007, 117.

513 *Gola/Klug* 2003, 47.

514 § 13 Abs. 1, Abs. 2 Nr. 1, 3, 5 -9; Abs. 5 Nr. 2; § 14 Abs. 1, Abs. 2 Nr. 6-9; § 28 Abs. 1 Nr. 2, Abs. 2 Nr: 2 u. 4, Abs. 5 NR. 1, 3 u. 4, Abs. 7-9 BDSG. Verankert ist er auch in Art. 6 Abs. 1 c), e) DSRL.

515 Dazu *Gola/Klug/Schomerus*, BDSG, 2010, § 28 Rn. 15; *Simitis* in *Simitis,* BDSG Komm 2011, § 28 Rn. 52 ff.

516 § 3a BDSG; siehe dazu *Roßnagel* 2011a.

517 *Roßnagel* 2011a; *Roßnagel*/*Scholz* MMR 2000, 721.

518 *Roßnagel* 2007, 116; das Transparenzgebot verlangt eine möglichst offene Verwendung von Daten, vgl. *Britz*, JA 2011, 81, 84.

519 *Gola/Klug* 2003, 49.

2.1.3.1.4 Schutz informationeller Selbstbestimmung durch europäisches Recht

Ein Recht auf informationelle Selbstbestimmung wird nicht allein durch das Grundgesetz gewährt. Auch auf Europäischer Ebene wird dieses durch Art. 8 EMRK und Art. 8 EU-GRCh. geschützt.[520] Art. 8 EU-GRCh. normiert ausdrücklich ein Grundrecht auf Datenschutz. Dessen Konzeption stützt sich primär auf Art. 286 EG, die Datenschutzrichtlinie 95/46/EG (DSRL) und schließlich auf Art. 8 EMRK sowie das Übereinkommen des Europarats zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten.[521] Wesentlich für die Auslegung des Datenschutzgrundrechts ist die Datenschutzrichtlinie.

In Art. 16 AEUV wurde zudem mit dem Lissabon-Vertrag eine einheitliche Rechtsgrundlage für die europäische Regelung des Datenschutzes und -verkehrs im Unionsraum geschaffen. Im Januar 2012 wurde ein seit langem erwarteter Entwurf für eine Novelle der Datenschutzrichtlinie, nunmehr als Datenschutz-Grundverordnung, vorgestellt.[522]

Nach einer Darstellung der datenschutzrechtlichen Garantien in Grundrechtecharta und Europäischer soll dieser Entwurf kurz dargestellt werden, bei dem jedoch aktuell nicht absehbar ist, ob, bis wann und in welcher Form er in Kraft treten wird.

2.1.3.1.4.1 Datenschutz durch EU-Grundrechtecharta und EMRK

Art. 8 EU-GRCh. kommt die Funktion eines Individualrechts zu, welches zwar durch Sekundärrecht konkretisiert und verstärkt wird, dadurch aber nicht abgeschwächt werden darf.[523]

Geschützt durch das Europäische Datenschutzgrundrecht werden nur Daten, die die Person selbst betreffen. Hier genügt, um den Schutzbereich zu öffnen, bereits ein potentieller Personenbezug, also wenn die Person zwar noch nicht bestimmt ist, aber dieser, etwa durch weitere Datenverarbeitungen, bestimmt werden kann.[524] Dabei ist jedoch umstritten wann im Einzelnen Personenbezug vorliegt.

Zum Personenbezug von IP-Adressen hat der *Europäische Gerichtshof* in einem Urteil 2011 festgestellt, dass es sich bei diesen um personenbezogene Daten handle, da sie „die genaue Identifizierung der Nutzer ermöglichen".[525] Man könnte meinen, dass der *Europäische Gerichtshof* sich damit für eine objektive Bestimmung des Personenbezugs ausgesprochen habe.[526] Allerdings ging es im Streitfall um die Verarbeitung der

---

[520] Umfassend zum europäischen Datenschutz und den Veränderungen durch den Lissabon Vertrag, *Spiecker gen. Döhmann/Eisenbarth,* JZ 2011, 169 ff.

[521] Übereinkommen v. 28.1.1981 (in Kraft getreten am 1.10.1985); hierzu auch *Frenz* 2009, Rn. 1360.

[522] Kom 2012 (11) v. 25.1.2012 „Vorschlag für Verordnung des *Europäischen Parlament*s und des Rats zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (Datenschutz-Grundverordnung)".

[523] *Frenz* 2009, Rn. 1364; ausführlich zum Schutz personenbezogener Daten, vgl. auch *Schorkopf,* in: *Ehlers/Becker* § 16.1 Rn. 39 ff.

[524] *Frenz* 2009, Rn. 1370 f.

[525] *EuGH*, Urt. v. 24.11.2011, Az. C-70/10, Rn. 51; zum Urteil Rössel, jurisPR-ITR 25/2011, Anm. 2.

[526] So wird argumentiert, dass auf europäischer Ebene überwiegend eine objektive Betrachtung des Personenbezugs erfolge, dazu generell *Eckhardt*, CR 2011, 339, 342 ff.;

Daten durch einen Access-Provider, so dass durchaus hinterfragt werden kann, ob der *Europäische Gerichtshof* mit dem Urteil generell den Personenbezug von IP-Daten feststellen wollte, geschweige denn anerkennen wollte, dass der Personenbezug von Daten immer dann anzunehmen ist, wenn irgendjemand den Personenbezug herstellen kann.

Der *Europäische Gerichtshof für Menschenrechte* nimmt einen Eingriff in Art. 8 EMRK an, wenn der Staat Daten erhebt, sie aber später nicht verwendet.[527] Der Gerichtshof hat zudem in ständiger Rechtsprechung dargelegt, dass mit Art. 8 EMRK „eine sogenannte 'erkundende' oder allgemeine Überwachung“ unvereinbar sei.[528]

Wie auch im deutschen Datenschutzrecht lassen sich aus dem Datenschutzgrundrecht sowohl Abwehransprüche als auch Schutzpflichten ableiten. Der Zweckbindungsgrundsatz hat so auch im europäischen Recht Geltung.[529] Anerkannt sind darüber hinaus Auskunfts- und Berichtigungsansprüche.[530]

Das Recht auf Schutz personenbezogener Daten ist einschränkbar nach der allgemeinen Grundrechtsschranke des Art. 52 Abs. 1 EU-GRCh. Dabei sind die Schranken, die sich aus der Datenschutzrichtlinie ergeben, als „sachgebietsspezifische Ausformungen des Verhältnismäßigkeitsgrundsatzes“ zu berücksichtigen.[531]

Gemäß Art. 8 Abs. 2 EMRK sind Einschränkungen des Datenschutzgrundrechts zulässig, wenn sie „gesetzlich vorgesehen und in einer demokratischen Gesellschaft notwendig“ sind und auch dann nur für bestimmte Zwecke. Zu diesen zählen etwa die nationale oder öffentliche Sicherheit, die Aufrechterhaltung der Ordnung, sowie die Verhütung von Straftaten. In seiner Rechtsprechung berücksichtigt der *Europäische Gerichtshof für Menschenrechte* in welchem Zusammenhang die Daten erhoben wurden um welche Art an Information es sich handelt, wie sie verwendet und verarbeitet werden oder könnten.[532]

---

527 *EGMR*, Urt. v. 16.2.2000, *Amann ./. Schweiz*, Az. 27798/95, Rn. 45; *EGMR*, Urt. v. 4.12.2008, *S. und Marper ./. Vereinigtes Königreich*, Az. 30562/04 und 30566/04, Rn. 67.

528 Siehe Nr. 17 sowie Nr. 5 des vorletzten Absatzes des Gutachtens des Juristischen Dienstes in Dokument 10146/06, zitiert nach Dok. 8850/11 (Gutachten des Juristischen Dienstes, Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates über die Verwendung von Fluggastdatensätzen zu Zwecken der Verhütung, Aufdeckung, Aufklärung und strafrechtlichen Verfolgung von terroristischen Straftaten und schwerer Kriminalität (Dok. 6007/11) - Vereinbarkeit mit dem Recht auf Achtung des Privatlebens und dem Recht auf Schutz personenbezogener Daten, Interinsitutionelles Dossier 2011/0023 (COD)), S. 14 Absatz-Nr. 22.

529 Eine Datenverarbeitung bedarf sowohl nach Art. 8 Abs. 2 EMRK i.V.m. Art. 52 Abs. 3 EU-GRCh. als auch nach Art. 8 EU-GRCh. einer gesetzlichen Grundlage, die eine feste Zweckbindung – den datenschutzrechtlichen Grundsätzen folgend – verlangt. Gem. Art. 6 lit. B) RL 95/46/EG muss der Zweck eindeutig angegeben und an sich rechtmäßig sein. Es ist insofern auch europarechtlich anerkannt, dass das Erfordernis der eindeutigen Zweckbindung Ausdruck der erforderlichen Vorhersehbarkeit (damit die Adressaten ihr Verhalten daran ausrichten können) ist; so *Frenz* 2009, Rn. 1433 mit zahlreichen w. Nachw.

530 *Frenz* 2009, Rn. 1392 ff.; 1398 f.

531 *Bernsdorff,* in: *Meyer*, EU-GRCh. 2003, Art. 8 Rn. 17.

532 *Meyer-Ladewig,* EMRK HdK 2011, Art. 8 Rn. 40.

In Bezug auf Überwachungsinstrumente sind insbesondere die Entscheidungen *Klass* und *Marper* des *Europäischen Gerichtshofs für Menschenrechte* maßgeblich.[533] In der Rechtssache *Klass* hat der Gerichtshof festgestellt, dass heimliche Überwachungsmaßnahmen die Gefahr bergen, die Demokratie auszuhöhlen oder zu zerstören.[534] Die Speicherung von Fingerabdrücken, Zellproben und DNA-Profilen Verdächtiger (aber nicht Verurteilter) in einer Gendatenbank hat der Gerichtshof im Fall *Marper* als unverhältnismäßigen Eingriff in Art. 8 Abs. 1 EMRK bewertet.[535]

Art. 8 Abs. 2 S. 2 EU-GRCh. sieht schließlich ein Auskunfts- und Berichtigungsrecht des Betroffenen vor und verlangt damit nach verfahrensrechtlichen Vorkehrungen zur Gewährleistung des Datenschutzrechts. Eine verfahrensrechtliche Flankierung stellt auch der Art. 8 Abs. 3 GRCh. dar, der ein Recht darauf einräumt, dass Beschwerden durch die zuständige Stelle behandelt werden.[536]

2.1.3.1.4.2 Datenschutz-Grundverordnung

Die Datenschutz-Grundverordnung liegt bislang nur als Entwurf vor, der zudem in der Öffentlichkeit vielfach auf Kritik gestoßen ist.[537] Es ist bis dato nicht absehbar, ob, bis wann und in welcher Form die Datenschutz-Grundverordnung verabschiedet werden wird. Es ist jedoch zu erwarten, dass die neue Regelung an den Vorschlägen der Datenschutz-Grundverordnung anknüpft. Daher sollen die wesentlichen Änderungen, die die Datenschutz-Grundverordnung beinhaltet, überblicksartig dargestellt werden.[538]

Von Bedeutung ist zunächst, dass sich die Datenschutz-Grundverordnung nicht allein auf eine Modernisierung der Datenschutzrichtlinie beschränkt. Sie erfasst mit dem Vorschlag für eine „Richtlinie zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Aufdeckung, Untersuchung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr“[539] auch den Bereich der Datenverarbeitung im Bereich der polizeilichen und justiziellen Zusammenarbeit.[540] In diesem Bereich aber eben nur als Regelung in Gestalt einer Richtlinie und nicht wie für den Bereich des allgemeinen Datenschutzrechts als Verordnung.

Der Wechsel von einer Richtlinie auf eine Verordnung bedeutet in rechtlicher Hinsicht eine Entmachtung der Mitgliedstaaten in Bezug auf die originäre Regelung des Datenschutzrechts.[541] Für die Rechtslage in Deutschland heißt dies: zukünftig wäre nicht mehr nationales Datenschutzrecht Prüfungsmaßstab, sondern allein die Datenschutz-

---

533 *EGMR,* Urt. v. 4.12.2008, *Marper ./. Vereinigtes Königreich*, Nr. 30.562/04, 30.566/04; *EGMR,* Urt. 6.9.1978, *Klass u. a. ./. Deutschland,* Nr. 5029/71.

534 *EGMR, Klass u. a. ./. Deutschland,* Az. 5029/71, Rn. 49.

535 *EGMR*, *Marper ./. Vereinigtes Königreich,* Nr. 30.562/04, 30.566/04, §§ 119, 125.

536 Dazu: *Welsing* 2009, 74.

537 *Ermert,* heise online v. 7.3.2012, abrufbar unter: http://heise.de/-1465832; *Krempl,* heise online v. 20.3.2012, abrufbar unter: http://www.heise.de/-1475681.html.

538 Ausführlich zum Entwurf der Datenschutzgrundverordnung *Hornung* ZD 2012, 99 ff.; *Nebel/Richter,* ZD 2012, 407; *Richter,* DuD 2012, 576; *von Lewinski,* DuD 2012, 564 ff.

539 KOM (2012) 10; vgl. zur Gesamtstrategie auch KOM (2012) 9.

540 Dieser ist bislang allein mit RB 2008/977/JI v. 27.12.2008) harmonisiert.

541 *Richter,* DuD 2012, 576.

Grundverordnung.[542] Das informationelle Selbstbestimmungsrecht wäre auf Grund des Vorrangs des Gemeinschaftsrechts nicht mehr anwendbar.[543] Auch das *Bundesverfassungsgericht* wäre nicht mehr zuständig, sondern grundsätzlich müsste der *Europäische Gerichtshof* im Rahmen eines Vorabentscheidungsverfahrens angerufen werden.[544] Ein mit der Verfassungsbeschwerde vergleichbares Verfahren gibt es hier jedoch nicht. Zudem fehlt es in der Rechtsprechung des *Europäischen Gerichtshofs* an einem mit der Judikatur des *Bundesverfassungsgerichts* vergleichbaren Grundrechtsschutz.[545] Aus deutscher, datenschutzrechtlicher Perspektive, kann der Entwurf insofern bereits nur einen Verlust bedeuten, obgleich er im europäischen Vergleich voraussichtlich zu einer Steigerung des Datenschutzes führen würde.

Die einzelnen Elemente der Datenschutz-Grundverordnung beinhalten letztlich keine wesentlichen Änderungen an der generellen Konzeption des Datenschutzrechts. Auch wenn sie einige Neuerungen enthält.[546]

Nicht verändert hat sich die Definition einer bestimmten oder bestimmbaren Person, die im Entwurf zwar formal geändert wurde, aber inhaltlich deckungsgleich bleibt.[547] Die Datenschutzprinzipien lehnen sich an Art. 6 DSRL an. In Bezug auf die Grundsätze der Transparenz, der Datensparsamkeit und der Verantwortlichkeit für die Datenverarbeitung geht der Entwurf über die DSRL hinaus. Auch die Einwilligung muss nach dem Entwurf explizit erfolgen. Ebenfalls enthält der Entwurf Anforderungen an die Einwilligung von Kindern und an die Verarbeitung besonderer Datenkategorien, der die Regelungen der DSRL erweitert.[548] Auch die Rechte der Betroffenen sind im Entwurf erweitert.[549] Neu eingefügt wurde ein Recht auf Datenübertragbarkeit (Art. 18). Die Pflichten des für die Datenverarbeitung Verantwortlichen sind ausführlich in Art. 22 ff. geregelt. Statt der allgemeinen Meldepflicht aus Art. 18 DSRL sieht der Verordnungsentwurf umfassende Dokumentationspflichten (Art. 28) vor. Zudem wurde der Grundsatz „Datenschutz durch Technik und datenschutzfreundliche Voreinstellungen" in Art. 23 angedeutet. Art. 35 des Entwurfs verlangt nunmehr auch die Bestellung eines internen Datenschutzbeauftragten ab einer Unternehmensgröße von 250 Mitarbeitern oder bei der Verarbeitung durch eine öffentliche Stelle.[550] Geregelt ist schließlich die Übermittlung in Drittstaaten und an internationale Organisationen (Kap. 5). Das darauffolgende Kapitel enthält ausführlich Bestimmungen für die Einrichtung vollständig unabhängiger Aufsichtsbehörden. Dabei wird in Art. 51 Abs. 2 des Entwurfs auch vorgeschrieben, dass es eine federführende Aufsichtsbehörde am Ort der Hauptniederlassung geben müsse (Prinzip einer zentralen Anlaufstelle für den

---

542 *Hornung,* ZD 2012, 99, 100.

543 Vgl. zum Europäischen Recht als supranationales Recht, oben S. 48 f.; ausführlich zum Verhältnis zwischen Grundgesetz und europäischem Sekundärrecht auch oben, S. 175 f.

544 Dazu auch *v. Lewinski* DuD 2012, 564 ff.

545 *Hornung,* ZD 2012, 99, 100.

546 Der Entwurf sieht eine Datenschutz-Grundverordnung mit 11 Kapiteln und 91 Artikeln vor; Eine umfassende Darstellung der Regelungen findet sich bei *Hornung,* ZD 2012, 99 ff.

547 Vgl. Erwägungsgrund 23; Art. 4 DSVO-E dazu *Hornung,* ZD 2012, 99, 101.

548 Vgl. Art. 9 DS-GVO-E.

549 Kap. III DS-GVO-E.

550 Anstelle des fakultativen Datenschutzbeauftragten gem. Art. 18 Abs. 2 DSRL.

Datenschutz).[551] In Kap. VIII wurden umfassende Regelungen zu Rechtsbehelfen, Haftung und Sanktionen normiert. Neu ist hier der in Art. 74 vorgesehene Rechtsbehelf, um das Tätigwerden von Aufsichtsbehörden zu erzwingen.[552] Es finden sich sodann Bestimmungen über besondere Datenverarbeitungssituationen (etwa Ausnahmen für journalistische, künstlerische oder literarische Verarbeitung) in Kap. IX.

Der Entwurf ist in Teilen durchaus zu begrüßen. So stärkt er die Betroffenenrechte unter anderem durch umfassende Transparenzregelungen, aber auch durch neu eingeführte Klagemöglichkeiten. Auch ist die Forderung nach einer datenschutzfreundlichen Technikgestaltung zu begrüßen. Allerdings bleiben gerade die Anforderungen an die technische Ausgestaltung sehr vage, was unbefriedigend ist.[553] Fragwürdig ist darüber hinaus die starke Stellung, die im Entwurf der Kommission zugestanden wird: so billigt der Entwurf der Kommission an mehreren Stellen die Kompetenz zum Erlass von delegierten Rechtsakten zu (Art. 86, Art. 87 Abs. 2, 3) oder zur Konkretisierung der Vorgaben der RL etwa in Bezug auf den Datenschutz durch Technik (gem. Art. 86 i.V.m. Art. 23 Abs. 3), oder für Zertifizierungsverfahren und Datenschutzsiegel (Art. 39 Abs. 2).[554]

Insbesondere aber der Ansatz einer Vollharmonisierung bedeutet für das deutsche Datenschutzrecht eine Abkehr von bislang gültigen Konzepten und würde zu einer Verringerung des hohen Schutzstandards im Bereich des Datenschutzrechts in Deutschland führen.

2.1.3.1.5 Datenschutzrecht als Voraussetzung von Freiheit im digitalen Zeitalter

1983 wurde nicht nur das informationelle Selbstbestimmungsrecht anerkannt, sondern auch das WWW freigegeben.[555] Das eine wie das andere hat in den vergangenen Jahrzehnten eine rasante Entwicklung durchlebt. Die Anerkennung des informationellen Selbstbestimmungsrechts ist für die Freiheit im digitalen Zeitalter von herausragender Bedeutung: „Freiheit in der "Informationsgesellschaft" setzt informationelle Selbstbestimmung voraus.“[556] Die Entwicklungen wie das WWW und andere datenverarbeitende Instrumente eröffnen zwar zahlreiche neue Möglichkeiten zur Freiheitsausübung, sie wecken aber zugleich für die freie Entfaltung der Persönlichkeit neue Risiken.[557] Dies führt ein Blick auf die informatisierte Polizeiarbeit zu Tage: Nicht nur sind im digitalen Zeitalter neue Gefährdungen für die Freiheit des Individuums wie der

---

[551] Auf diese Weise soll eine einheitliche Rechtsanwendung gesichert werden.
[552] In Art. 73 ist darüber hinaus ein Verbandsklagerecht eingeführt worden.
[553] Auch an anderen Stellen des Entwurfs finden sich sowohl verschlechternde und verkomplizierende Neuerungen als auch Verbesserungen, vgl. *Hornung,* ZD 2012, 99, 103; *Richter,* DuD 2012, 576, 579.
[554] *Hornung,* ZD 2012, 99, 105.
[555] Ausführlich zur gemeinsamen Geschichte von WWW und dem Recht auf informationelle Selbstbestimmung *Hornung*, MMR 2004, 3.
[556] *Roßnagel* 2009, 99.
[557] Vgl. zu den neuen Risiken im digitalen Zeitalter ausführlich oben Kap. 1.5.

Gesellschaft insgesamt entstanden, sondern auch Polizei und Geheimdienste nutzen zur Gewährleistung der Sicherheit die neuen Techniken.[558]

Insofern prägen das WWW wie das informationelle Selbstbestimmungsrecht das Spannungsverhältnis von Freiheit und Sicherheit zu Beginn des 21. Jahrhunderts entscheidend: Das WWW erhöht den Bedarf an Sicherheit und verbessert zugleich die Möglichkeiten zur Herstellung von Sicherheit. Es schafft für die Gewährleistung von Freiheit einerseits neue Gefährdungen, andererseits werden durch das WWW neue Freiheitsräume geschaffen. Das Informationelle Selbstbestimmungsrecht ist Voraussetzung für die Freiheit unter den Bedingungen digitaler Datenverarbeiten. Es ist Anknüpfungspunkt für den Ausgleich zwischen Freiheits- und Sicherheitsinteressen unter den Bedingungen digitaler Datenverarbeitung.

2.1.3.2 IT-Grundrecht

Das *Bundesverfassungsgericht* hat im Urteil über die Ermächtigung zur Online-Durchsuchung im Verfassungsschutzgesetz Nordrhein-Westphalen aus dem allgemeinen Persönlichkeitsrecht das Grundrecht auf Vertraulichkeit und Integrität informationstechnischer System hergeleitet.[559] Im Hinblick auf die Gefährdungen für die Persönlichkeit durch die Nutzung informationstechnischer Systeme, „die sämtlich mit der Erzeugung, Verarbeitung und Speicherung von Daten verbunden sind", bestünde eine Schutzlücke.[560] Weder das Telekommunikationsgeheimnis, die Unverletzlichkeit der Wohnung noch das Recht auf informationelle Selbstbestimmung böten hier einen ausreichenden Schutz.[561] Diese würden nun durch das sogenannte Computer- oder IT-Grundrecht ergänzt.[562]

Die Anerkennung des Grundrechts auf Vertraulichkeit und Integrität informationstechnischer Systeme ist zum Teil auf scharfe Kritik gestoßen.[563] Das *Bundesverfassungsgericht* habe in „freier Rechtsschöpfung" das neue Grundrecht „erfunden".[564] Kritisiert wird, dass das Gericht den Schutzbereich von Art. 10 GG darauf reduziert habe, dass er nur das Vertrauen darauf schütze, dass ein Telekommunikationsvorgang nicht von dritter Seite wahrgenommen wird. Dies widerspreche aber der bisherigen Rechtsprechung zu Art. 10 GG, die gerade einen Eingriff ablehnt, wenn ein Gesprächsteilnehmer einen Dritten ein anderes Telefonat an seinem Endgerät mithören lässt.[565] Das Gericht habe mittels einer nicht gebotenen einschränkenden Auslegung des Rechts auf informationelle Selbstbestimmung die Schutzlücke konstruiert.[566] Bis

---

[558] Zu den Anforderungen eines modernen Datenschutzes, *Hirsch,* KritV 2011, 139 ff.
[559] BVerfGE 120, 274 (LS 1, 303 ff., 313).
[560] BVerfGE 120, 274 (305).
[561] BVerfGE 120, 273 (306).
[562] *Hopfauf*, in: *Schmidt-Bleibtreu/Klein*, GG 2011, Art. 2 Rn. 30d.
[563] *Pagenkopf*, in: *Sachs,* GG 2011, Art. 10, Rn. 10a; zahlreiche Nachw. finden sich bei *Gudermann* 2010, 161 (Fn. 533); auf den S. 162 ff. wird der Schutzgehalt grundrechtsdogmatisch eingeordnet.
[564] *Pagenkopf,* in: *Sachs,* GG 2011, Art. 10, Rn. 10a.
[565] *Pagenkopf,* in: *Sachs,* GG 2011, Art. 10, Rn. 10a.
[566] *Volkmann,* DVBl. 2008, 590, 592.

heute wird immer wieder betont wird, dass eine weitere dogmatische Durchdringung erforderlich sei.[567]

Von seiner Konzeption her schützt das Grundrecht in Abgrenzung zum informationellen Selbstbestimmungsrecht nicht primär die Selbstbestimmung des Bürgers über Erhebung, Verarbeitung und Nutzung seiner Daten, sondern verbietet das Eindringen und Verändern in die persönlichen informationstechnischen Systeme.[568] Es ergänzt insoweit das Grundrecht auf informationelle Selbstbestimmung, um den Schutz informationstechnischer Systeme.

Ein Eingriff in dieses Grundrecht ist dann anzunehmen, „wenn die Integrität des geschützten informationstechnischen Systems angetastet wird, indem auf das System so zugegriffen wird, dass dessen Leistungen, Funktionen und Speicherinhalte durch Dritte genutzt werden können;“ da dann „die entscheidende technische Hürde für eine Ausspähung, Überwachung oder Manipulation des Systems genommen“ wurde.[569] Das Grundrecht ist jedoch nicht schrankenlos: „Eingriffe können sowohl zu präventiven Zwecken als auch zur Strafverfolgung gerechtfertigt sein.“[570]

Die bestehenden Regelungen zur Onlinedurchsuchung waren jedoch, so das *Bundesverfassungsgericht,* sowohl zu unbestimmt als auch unverhältnismäßig im engeren Sinne. In Bezug auf die Anforderungen an die Angemessenheit betont das Gericht zum einen, dass eine angemessene Zuordnung des Individualinteresses, das durch einen Grundrechtseingriff beschnitten wird, zu den Allgemeininteressen erforderlich sei.[571] Dem hätten die bestehenden Regelungen nicht entsprochen. Zudem bedürfe es „ergänzender verfahrensrechtlicher Vorgaben, um den grundrechtlich geschützten Interessen des Betroffenen Rechnung zu tragen“.[572]

Auf europäischer Ebene wird weder ausdrücklich in der Europäischen Menschenrechtskonvention oder der Europäischen Grundrechtecharta noch durch die Rechtsprechung von *Europäischem Gerichtshof* oder *Europäischem Gerichtshofs für Menschenrechte* ein mit dem IT-Grundrecht vergleichbares Grundrecht gewährt. Ein Schutz bei der Infiltration von informationstechnischen Systemen wird aber durch das Recht auf Achtung des Privatlebens (Art. 8 EMRK; Art. 7 EU-GRCh.) garantiert.

2.1.3.3 Telekommunikationsfreiheit

Nicht nur Datenverarbeitung prägt die Gesellschaft im digitalen Zeitalter. Sie ist sowohl Informations- als auch Kommunikationsgesellschaft.

---

567 *Gudermann* 2010, 164.

568 *Gudermann* 2010, 131 ff; zu den Systemen werden PC, informationstechnische Komponenten in TK-Geräten u. andere elektronische Geräte sowie die Vernetzung der Systeme, genannt, so *Jarass,* in: *Jarass/Pieroth,* GG 2011, Art. 2 Rn. 45.

569 BVerfGE 120, 274 (314).

570 BVerfGE 120, 274 (315).

571 BVerfGE 120, 274 (322).

572 BVerfGE 120. 274 (322).

Die Vertraulichkeit des Fernmeldeverkehrs wird in Art. 10 GG garantiert. Auch auf europäischer Rechtsebene wird ein Schutz gewährleistet und zwar durch den Anspruch des Einzelnen auf Privatheit aus Art. 8 EMRK und Art. 7 und 8 EU-GRCh.[573]

2.1.3.3.1 Funktion und Bedeutung von Art. 10 GG

Art. 10 GG sichert die Vertraulichkeit des durch Kommunikationsmittel ermöglichten individuellen Informationsaustauschs.[574] Das Grundrecht erfasst unterschiedslos Kommunikation privaten, geschäftlichen oder politischen Inhalts. Abgegrenzt wird allein zwischen verschiedenen Medien. Es handelt sich also um keinen inhaltsbezogenen Schutz, sondern der Schutz wird durch das benutzte Medium konstituiert.[575]

Schutzziel der Telekommunikationsfreiheit in Art. 10 GG ist die Unbefangenheit der Kommunikation. Das heißt die Beteiligten sollen nicht damit rechnen müssen, dass staatliche Stellen sich in die Kommunikation einschalten und Kenntnisse über Kommunikationsbeziehungen oder Inhalte gewinnen.[576] Insoweit schützt Art. 10 GG sowohl den Inhalt als auch die Umstände der Telekommunikation.[577] Zeitlich endet der Schutz durch Art. 10 Abs. 1 GG nach Beendigung des Kommunikationsvorgangs.[578] In sachlicher Hinsicht schützt Art. 10 Abs. 1 GG, das Brief-, Post- und Fernmeldegeheimnis – wobei es sich um ein einheitliches Grundrecht und nicht etwa um drei verschiedene Grundrechte handelt.[579]

Die Bedeutung des Post- und Briefgeheimnisses hat durch die Digitalisierung des Fernmeldeverkehrs an praktisch relevanter Bedeutung verloren. Heute wird überwiegend auf die schnelleren und kostengünstigen Kommunikationsmittel Internet und Telefonie zurückgegriffen. Daher ist heute das Fernmeldegeheimnis, das zunehmend als Telekommunikationsgeheimnis[580] oder auch als Telekommunikationsfreiheit[581] be-

---

573 *Petri*, RDV 2003, 16, 18.

574 *Durner,* in: *Maunz/Dürig*, GG 2011, Art. 10, Rn. 41, 50; *Gusy,* in: v. *Mangoldt/Klein*, 2005, Art. 10, Rn. 10; *Schoch*, Jura 2011, 194.

575 *Durner,* in: *Maunz/Dürig*, GG 2011, Art. 10, Rn. 49 f.; *Hermes,* in: *Dreier*, GG 2004, Art. 10 Rn. 36 f.

576 *Zöller* 2003, 291, 307; „Art. 10 Abs. 1 GG begegnet Gefahren für die Vertraulichkeit von Mitteilungen, die aus dem Übermittlungsvorgang einschließlich der Einschaltung fremder Übermittler entstehen". Schutzziel von Art. 10 GG sei es zu verhindern „dass der Meinungs- und Informationsaustausch mittels Telekommunikationsanlagen deswegen unterbleibt oder nach Form und Inhalt verändert verläuft, weil die Beteiligten damit rechnen müssen, dass staatliche Stellen sich in die Kommunikation einschalten und Kenntnisse über die Kommunikationsbeziehungen der Kommunikationsinhalte gewinnen." BVerfGE 107, 299 (313).

577 BVerfGE 125, 260 (304); *Sodan,* in: *Sodan,* GG, 2011, Art.10, Rn. 7 – Diesen Schutzgehalt des Kommunikationsvorgangs als solchen, haben Brief-, Post und Fernmeldegeheimnis gemein, *Sodan,* in: *Sodan,* GG, 2011, Art.10, Rn. 8.

578 S. z.B. *Schoch*, Jura 2011, 194, 197. Zum Teil wurde für den Bereich der E-Mail-Kommunikation eine andere Auslegung gefordert, da es hier am Element der Dauer fehle. Schließlich ende die Kommunikation ohne dass dies unmittelbar bemerkt werde. So hat auch das *BVerfG* im Auslesen einer SIM-Karte einen Eingriff in Art. 10 Abs. 1 GG angenommen (*BVerfG*, NJW 2005, 1637, 1639) – später hat das Gericht diese Entscheidung jedoch (stillschweigend) korrigiert, BVerfGE 115, 166 (183f.) – dazu auch ausführlich *Schoch*, Jura 2011, 194, 198 ff.

579 *Schoch*, Jura 2011, 194, 195.

580 *Sodan,* in: *Sodan,* GG, 2011, Art.10, Rn. 5.

zeichnet wird, in den Mittelpunkt der Art. 10 GG betreffenden rechtlichen Auseinandersetzungen gerückt.[582]

In Anbetracht der rasanten technischen Entwicklungen gestaltet sich die Bestimmung des (grundsätzlich entwicklungsoffenen)[583] Schutzbereichs von Art. 10 GG als besonders schwierig: Denn im Gegensatz zur analogen Kommunikation hinterlässt die digitale Kommunikation immer technisch ablesbare Datenspuren. Dies verursacht eine im Gegensatz zu den früheren Übermittlungsformen extensive Verletzlichkeit.[584]

In Bezug auf die neuen Gefährdungslagen aufgrund der fortschreitenden technologischen Entwicklung betont das *Bundesverfassungsgericht*, dass das Fernmeldegeheimnis „einen Ausgleich für den technisch bedingten Verlust an Beherrschbarkeit der Privatsphäre, der durch die Nutzung von Anlagen Dritter zwangsläufig entsteht“[585] gewährleisten müsse.[586] Daran wird deutlich, dass das *Bundesverfassungsgericht* der Telekommunikationsfreiheit eine hohe Bedeutung zuerkennt. Das Gericht hat darüber hinaus immer wieder die Nähe zur Menschenwürdegarantie hervorgehoben. Durch das Grundrecht des Art. 10 Abs. 1 GG werde „die freie Entfaltung der Persönlichkeit durch einen privaten, vor den Augen der Öffentlichkeit verborgenen Austausch von Nachrichten, Gedanken und Meinungen (Informationen)“ geschützt und „die Würde des denkenden und freiheitlich handelnden Menschen“ gewahrt.[587]

Neben dieser individualrechtlichen Bedeutung beinhaltet der Schutz von Kommunikation auch eine objektive Wertentscheidung des Grundgesetzes.[588] Durch den Entzug der individuellen Kommunikation vor staatlichem Zugriff soll die Freiheit des Gedankenaustauschs sichergestellt werden, die wesentliche Grundvoraussetzung eines demokratischen und rechtsstaatlichen Gemeinwesens ist.[589]

---

581 Etwa BVerfGE 125, 260 (338).

582 *Pagenkopf*, in: *Sachs,* GG 2011, Art. 10, Rn. 14.

583 Dass das Grundgesetz grundsätzlich entwicklungsoffen konzipiert ist, hat das *BVerfG* deutlich gemacht BVerfGE 115, 166 (182). Das Verfassungsrecht wird nicht nur durch ausdrückliche Textänderungen verändert, sondern es wandelt sich auch „durch eine allmähliche und permanente Bedeutungsänderung“, *Roßnagel* 1984, 19.

584 *Pagenkopf*, in: *Sachs,* GG 2011, Art. 10, Rn. 6; *Schoch*, Jura 2011, 194, 195 stellt fest, dass die technologischen Entwicklungen zu neuen Gefährdungslagen geführt haben; vgl. zu den digitalen Spuren, oben S. 34 f.

585 BVerfGE 115, 166 (186).

586 Dazu mit Beispielsfällen, *Schoch*, Jura 2011, 194, 195 ff.

587 BVerfGE 67, 157 (171); 106, 28 (35); 110, 33 (53); ähnlich BVerfGE 115, 166 (182 f.) siehe dazu auch *Durner,* in: *Maunz/Dürig*, GG 2011, Art. 10, Rn. 1; *Petri*, RDV 2003, 16, 18 zum engen Bezug zur Menschenwürdegarantie, vgl. auch *Pagenkopf*, in: *Sachs,* GG 2011, Art. 10, Rn. 6

588 *Durner,* in: *Maunz/Dürig*, GG 2011, Art. 10, Rn. 2; So führt das *BVerfG* aus, dass die zum Schutze der Kommunikation geschaffenen gesetzlichen Vorkehrungen „in seinem objektivrechtlichen Gehalt die Vertraulichkeit der Telekommunikation auch in ihrer gesamtgesellschaftlichen Bedeutung“ erfassten und so „auch dem Vertrauen der Allgemeinheit zugute“ kämen, BVerfGE 107, 299 (328); vgl. dazu auch *Hermes,* in: *Dreier,* GG 2004, Art. 10 Rn. 81 ff.

589 *Kindt*, MMR 2009, 661, 666; vgl. dazu auch schon oben, S. 74 f.

2.1.3.3.2 Eingriff und Rechtfertigung

Jede Kenntnisnahme, Aufzeichnung oder Verwertung von Telekommunikationsdaten durch den Staat, ist ein Eingriff in die durch Art. 10 Abs. 1 GG geschützte Vertraulichkeit der individuellen Kommunikation.[590] Auf die Form der Kenntnisnahme kommt es dabei nicht an.[591]

Zum Teil wird vertreten, dass ein Grundrechtseingriff zu verneinen sei, wenn es in Bezug auf die Kommunikationsinhalte oder Telekommunikationsverkehrsdaten nicht zur Kenntnisnahme durch staatliche Stellen komme.[592] Begründet wird dies mit einem Verweis auf die Entscheidung des *Bundesverfassungsgerichts* zum Kfz-Kennzeichenscanning. Hier hat das Gericht keinen Eingriff in das Recht auf informationelle Selbstbestimmung angenommen, wenn Daten unmittelbar nach ihrer Erhebung wieder spurenlos gelöscht werden.[593] Gegen diese Auslegung spricht jedoch, dass dies die klare Bestimmbarkeit, wann ein Eingriff vorliegt verwischt: Maßnahmen, die zeitlich gesehen dem Eingriff durch die Speicherung nachgelagert sind, dienen dazu, den in der Speicherung liegenden Eingriff zu relativieren. Dies ist schon in sich widersprüchlich. Darüber hinaus ist diese Konstruktion dogmatisch unsauber. Denn die Frage, ob die Daten unmittelbar gelöscht werden, ist relevant für die Beurteilung der Schwere des Eingriffs; nicht aber für die Frage, ob überhaupt ein Eingriff vorliegt. Dass auch das *Bundesverfassungsgericht* sich von der Bestimmung des Eingriffs wie sie im Kfz-Kennzeichen-Urteil erfolgt ist, verabschiedet hat, zeigt das Urteil zur Vorratsdatenspeicherung. Hier hat das Gericht, ohne überhaupt darauf einzugehen, ob eine Kenntnisnahme stattfindet, schon die Speicherungsverpflichtung als (schwerwiegenden) Eingriff in Art. 10 Abs. 1 GG bewertet.[594]

Art. 10 Abs. 2 S. 1 GG enthält einen unlimitierten Gesetzesvorbehalt. Eingriffe können demnach gerechtfertigt werden, wenn sie auf einem förmlichen Gesetz beruhen und materiell den verfassungsrechtlichen Anforderungen entsprechen, insbesondere dem Verhältnismäßigkeitsprinzip. Auch muss nach Art. 19 Abs. 2 GG der Wesensgehalt gewahrt werden.

Daneben enthält Art. 10 Abs. 2 S. 2 GG eine Sonderregelung für Eingriffe durch die Nachrichtendienste. Zum Schutz der freiheitlich demokratischen Grundordnung oder des Bestandes oder der Sicherung des Bundes oder eines Landes, kann in das Fernmeldegeheimnis eingegriffen werden, ohne dass dies dem Betroffenen mitgeteilt wird und damit auch faktisch der Rechtsweg ausgeschlossen wird.[595]

---

[590] „Ein Grundrechtseingriff ist jede Kenntnisnahme, Aufzeichnung und Verwertung von Kommunikationsdaten sowie jede Auswertung ihres Inhalts oder sonstige Verwendung durch die öffentliche Gewalt, BVerfGE 85, 386 (398); 100, 313 (366); 110, 33 (52); 125, 260 (310).

[591] *Schoch*, Jura 2011, 194, 200.

[592] *Schoch*, Jura 2011, 194, 200.

[593] BVerfGE120, 378; vgl. dazu auch schon oben Kap. 2.1.3.1.2, S. 85.

[594] BVerfGE 125, 260 (310).

[595] Mit dem G10-Gesetz ist von dieser sog. „Staatsschutzklausel“ Gebrauch gemacht worden, dazu *Schoch*, Jura 2011, 194, 203 f.

2.1.3.3.3 Richtervorbehalt

In langer, bereits vorkonstitutioneller gesetzgeberischer Tradition werden Eingriffe in Art. 10 GG grundsätzlich unter einen präventiven Richtervorbehalt gestellt, obwohl der Verfassungstext dies nicht ausdrücklich verlangt (wie es hingegen bei Eingriffen in den Wohnraum nach Art. 13 Abs. 2 GG der Fall ist).[596]

Im Urteil zur Online-Durchsuchung verlangt das *Bundesverfassungsgericht* auch zur Rechtfertigung von Eingriffen in das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme „eine vorbeugende Kontrolle durch eine unabhängige Instanz". Die Gesetzgebungsprärogative „bei der Entscheidung über die kontrollierende Stelle und das anzuwendende Verfahren" reduziere sich bei einem „Grundrechtseingriff von besonders hohem Gewicht" dahingehend, dass die Maßnahme „grundsätzlich unter den Vorbehalt richterlicher Anordnung zu stellen" ist.[597]

Fraglich ist inwiefern diese Erwägungen grundsätzlich auf Eingriffe in das Telekommunikationsgeheimnis übertragen werden können.[598] Letztlich verlangt der Verhältnismäßigkeitsgrundsatz bei besonders schwer wiegenden Grundrechtseingriffen einen Ausgleich. Dazu dient auch die Anordnung präventiver Richtervorbehalte als Instrument der vorbeugenden Kontrolle.[599] Gerade auch bei der vielfach heimlichen Überwachung der Telekommunikation ist die vorbeugende richterliche Kontrolle anerkannt. Jedenfalls in Fällen in denen das Gewicht des Eingriffs wie bei einer Online-Durchsuchung besonders schwer wiegt, ist eine präventive richterliche Prüfung zu verlangen.

Dem wird entgegengebracht, dass der Richtervorbehalt systemfremd sei, da sich in Art. 10 GG nicht wie in Art. 13 Abs. 2 GG ausdrücklich die richterliche Prüfung normiert findet. Damit würde, mittels des Verhältnismäßigkeitsgrundsatzes, ungeschriebenes Verfassungsrecht über geschriebenes Verfassungsrecht gesetzt werden.[600] Diese Kritik trifft aber nicht zu. Denn der Richtervorbehalt erwächst aus den verfassungsrechtlichen Anforderungen – auch wenn er in der Verfassung nicht ausdrücklich normiert ist. Ungeschriebenes Verfassungsrecht wird jedenfalls nicht über geschriebenes Verfassungsrecht gestellt. Vielmehr hat das *Bundesverfassungsgericht* über den Richtervorbehalt in Art. 13 Abs. 2 GG hinaus systemkonform für andere vergleichbar schwerwiegende Grundrechtseingriffe eine richterliche Kontrolle gefordert.[601] Dabei ist die Bedeutung richterlicher Kontrolle bei heimlichen Sicherheitsmaßnahmen besonders groß, da so die an sich gebotene Transparenz bei Eingriffen in die Freiheitsrechte der Bürger durch eine richterliche Kontrolle ersetzt wird. Polizeiliche Willkür soll so verhindert werden und das Vertrauen der Bürger in die Sicherheitsbehörden gestärkt werden. Wichtig ist insofern gerade bei heimlichen Eingriffen in die Telekom-

---

596 *Durner,* in: *Maunz/Dürig*, GG 2011, Art. 10, Rn. 152; siehe auch *Schoch*, Jura 2011, 194, 203.
597 BVerfGE 120, 274 (331).
598 Damit befasst sich: *Durner,* in: *Maunz/Dürig*, GG 2011, Art. 10, Rn. 154.
599 *Durner,* in: *Maunz/Dürig*, GG 2011, Art. 10, Rn. 154.
600 *Wolff*, NVwZ 2010, 751, 752
601 Etwa BVerfGE 120, 274 (331).

munikationsfreiheit diese durch das Instrument der präventiven richterlichen Prüfung der Anordnung der Überwachungsmaßnahme zu beschränken.

2.1.3.3.4 Datenschutzrechtlicher Kern des TK-Geheimnisses

Art. 10 Abs. 1 GG gewährleistet die Verfügungsbefugnis über Informationen, die übermittelte Kommunikationsvorgänge betreffen, und weist insofern auch einen Schutz der Selbstbestimmung über Informationen auf, die es mit dem Grundrecht auf informationelle Selbstbestimmung teilt. Die Schutzwirkung der Telekommunikationsfreiheit umfasst also auch den Informations- und Datenverarbeitungsprozess. Dem Grundrecht kommt so eine datenschutzrechtliche Dimension zu.[602] Art. 10 GG geht dabei sogar über das allgemeine Datenschutzrecht hinaus, indem es verlangt, dass jede Zweckänderung von Daten, die von Adressaten des Art. 10 GG zulässigerweise zur Kenntnis genommen oder gespeichert wurden, einer eigenen Rechtsgrundlage bedarf.[603] Da Art. 10 Abs. 1 GG, soweit etwa Telekommunikationsverkehrsdaten betroffen sind, lex specialis zur allgemeinen Garantie informationeller Selbstbestimmung ist, treten Art. 2 Abs. 1 GG i.V.m. Art. 1 Abs. 1 GG zurück. Soweit es sich aber im Kern um Datenschutzfragen handelt, werden bei der Beurteilung, die im Rahmen des Rechts auf informationelle Selbstbestimmung entwickelten Wertungen berücksichtigt.[604]

2.1.3.3.5 Schutz der (Tele-)Kommunikation durch Europäische Grundrechte

Art. 8 EMRK enthält mit dem Recht auf Achtung des Briefverkehrs ausdrücklich einen Anspruch auf den Schutz der Korrespondenz. Der Begriff „Briefverkehr" wird dabei weit ausgelegt. Er erfasst so auch Telefongespräche, E-Mails oder Kurznachrichten.[605] Dies erklärt sich aus dem Schutzzweck der Norm. Geschützt wird nämlich der Austausch nicht-öffentlicher Mitteilungen vor staatlichen Eingriffen. Vergleichbar mit dem Schutzziel der Telekommunikationsfreiheit aus Art. 10 Abs. 1 GG soll das Vertrauen des Bürgers bei der Kommunikation über Distanz geschützt werden. Der Bürger soll auch bei der Kommunikation über Distanz, auf den Schutz vor dem Zugriff Dritter auf den Übertragungsweg vertrauen können.[606] Es ist anerkannt, dass nicht nur die inhaltliche Überwachung, sondern bereits die Erfassung der Umstände der Telekommunikation in Art. 8 EMRK eingreift. Wobei anerkannt ist, dass das Eingriffsgewicht durch die Erfassung der Umstände geringer wiegt.[607]

---

[602] *Hermes,* in: *Dreier*, 2004, Art. 10, Rn. 16; *Gusy,* in: v. *Mangoldt/Klein/Starck*, 2005, Art. 10, Rn. 60; *Gurlit*, NJW 2010, 1035, 1036.

[603] *Gusy,* in: v. *Mangoldt/Klein*, 2005, Art. 10, Rn. 60.

[604] „Insoweit lassen sich allerdings die Maßgaben, die das *Bundesverfassungsgericht* aus Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 GG entwickelt hat, weitgehend auf die speziellere Garantie des Art. 10 GG übertragen" BVerfGE 125, 260 (310) mit Verweis auf BVerfGE 100, 313 (358 f.).

[605] *Grabenwarter/Pabel* 2011, § 22 Rn. 24 f.; so der *EGMR* mit Urt. v. 29. 6. 2007 „Weber u. Saravia", NJW 2007, 1433 Rn. 77.

[606] *Hermes,* in: *Dreier,* GG 2004, Art. 10 Rn. 15; *Jarass,* in: *Jarass/Pieroth,* GG 2011, Art. 10 Rn. 3 ff.; *Schädler,* in: KarlsruherKomm StPO, Art. 8 EMRK Rn. 1; *EGMR,* NJW 2007, 1433 Rn. 77.

[607] *EGMR*, Urt. v. 2.8.1984, *Malone./.Vereinigtes Königreich*, Nr. 8691/79; *EGMR* Urt. v. 25.9.2001, *P.G u. J.H. ./. Vereinigtes Königreich*, Nr. 44787/98, Z. 42; vgl. auch *Grabenwarter/Pabel* 2011, §§ 22 Rn. 31.

Wie Art. 8 EMRK schützt auch Art. 7 EU-GRCh. die Kommunikation. Art. 7 EU-GRCh. gewährt wie das Recht auf Achtung des Privat- und Familienlebens. Der Begriff ist nach der Rechtsprechung des *Europäischen Gerichtshofs für Menschenrechte* umfassend zu verstehen[608] und wird nicht abschließend definiert. Unter den Schutzbereich fällt auch die Kommunikation[609] sowie der Schutz der Privatsphäre, soziale Beziehungen oder auch das Recht, sich ohne Aufzeichnung in der Öffentlichkeit zu bewegen.[610]

In Bezug auf die Überwachung der Telekommunikation hat der *Europäische Gerichtshof für Menschenrechte* wegen der schwerwiegenden Beeinträchtigung besonders hohe Anforderungen an die Klarheit der gesetzlichen Regelung gefordert.[611] In Bezug auf die Verhältnismäßigkeit von Eingriffen in die Kommunikationsfreiheit, spielt es, so der Gerichtshof, eine bedeutende Rolle, ob innerstaatlich ein ausreichender Schutz vor Missbrauch vorhanden ist.[612]

In Bezug auf die geheime Telefonüberwachung im Rahmen des G 10-Gesetzes stellte der *Europäische Gerichtshof für Menschenrechte* fest, dass eine Gesetzgebung, die die heimliche Überwachung der Telekommunikation ermögliche, in Anbetracht des technischen Fortschritts und der Entwicklung des Terrorismus, notwendig für die nationale Sicherheit sein können. Darüber hinaus könne sie auch unter Berücksichtigung eines weiten Ermessensspielraums der Mitgliedstaaten verhältnismäßig sein.[613]

2.1.3.4 Kommunikationsfreiheit als Grundlage der Freiheit

Digitale Kommunikation prägt unsere Lebenswelt. In vielen Lebensbereichen ist heute Telekommunikation erforderlich, um überhaupt am gesellschaftlichen Leben teilnehmen zu können. Ob als Kommunikationsplattform oder Informationsquelle, als Raum zur beruflichen wie privaten Betätigung − das Internet prägt heute unsere Lebenswirklichkeit. Vielfach ist so, aufgrund der Abhängigkeit von Kommunikationsmitteln, Telekommunikation quasi zu einer Grundvoraussetzung für die Wahrnehmung von Grundrechten geworden.[614] Aus diesen Gründen wird das Telekommunikationsgeheimnis auch als zentrales Menschenrecht der Informationsgesellschaft bezeichnet.[615] Denn in vielen Bereichen ist das Telekommunikationsgeheimnis Garant der Freiheit.

Plakativ zeigen dies die Protestbewegungen in Nordafrika, die zwar nicht allein wegen der technischen Möglichkeiten erfolgreich waren, jedoch für die die Technik (zumindest zunächst) ein zentrales Vehikel für die unentdeckte und anonyme Organisation

---

608 *Uerpmann-Wittzack/Jankowska-Gilberg,* MMR 2008, 83, § 3 Rn. 3 m.w.Nachw.
609 *Schorkopf,* in: *Ehlers/Becker* § 16.1 Rn. 25.
610 *Schorkopf,* in: *Ehlers/Becker* § 16.1 Rn. 17.
611 *Grabenwarter/Pabel* 2011, § 22 Rn. 34 (Fn. 194 m. zahlreichen Nachw. aus der Rspr.).
612 Und zwar insbesondere im Hinblick darauf, ob den Betroffenen wirksame Kontrollmöglichkeiten zu Verfügung stehen, dazu *Grabenwarter/Pabel* 2011, § 22 Rn. 46.
613 *EGMR* Urt. v. 6.9.1978, *Klaas ./.Deutschland*, Nr. 5029/71 (NJW 1979, 278); *EGMR* Urt. v. 29.6.2006, *Weber u. Saravia*, Nr. 4378/02 (NJW 2006, 1433); dazu auch *Grabenwarter/Pabel* 2011, § 22 Rn. 40.
614 *Hammer*/*Pordesch*/*Roßnagel* 1993, 43 f.; *Hoffmann-Riem*, JZ 2008, 1009.
615 *Dix* 2004, 117.

des Protests war.[616] Telekommunikation ist aber nicht nur für derart massiven Protest gegen ein ganzes System von zentraler Bedeutung, sondern für jegliche Freiheitswahrnehmung und damit auch für alle durch das Grundgesetz garantierten partiellen Individualfreiheiten: denn jede äußere Freiheit manifestiert sich gerade in und durch Kommunikation.

Kommunikation kann insoweit als Grundlage der Ausübung der durch das Grundgesetz garantierten Freiheiten gesehen werden. So formuliert *Denninger* treffend: „Die Freiheit aller öffentlichen und erst recht aller privaten Kommunikationen von staatlicher Überwachung, von Zensur und jeder Art von Gängelei ist eine elementare Voraussetzung für das Gedeihen eines freiheitlichen Meinungsklimas, für die Entfaltung individueller künstlerischer wie technisch-innovativer Phantasie oder wissenschaftlicher oder friedlicher politischer Auseinandersetzungen."[617] Damit bringt er zum Ausdruck, was auch eine Analyse der Grundrechte im Hinblick auf die Frage, inwiefern durch die Freiheitsgrundrechte auch Kommunikation geschützt wird, zu Tage führt: Die Grundrechte formen eine objektive Werteordnung der Gesellschaft. Dabei wird die Kommunikationsfreiheit letztlich auch partiell durch sämtliche (anderen) Freiheitsrechte geschützt:

Art. 4 GG schützt die Religions- und Gewissensfreiheit und damit auch die religiöse Kommunikation.[618] Der kommunikative Aspekt der Meinungsfreiheit kommt schon in der Formulierung des Grundrechts zum Ausdruck: „Jeder hat das Recht, seine Meinung in Wort, Schrift und Bild frei zu äußern und zu verbreiten".[619] Die von Art. 6 GG geschützte Ehe und Familie basiert auch auf dem sozialen Miteinander und damit der Kommunikation zweier Menschen. Geschützt durch dieses Grundrecht ist insoweit unter anderem die Kommunikation in der Ehe.[620] Ebenfalls beinhaltet die Versammlungsfreiheit mit der Garantie, sich „zu versammeln" einen kommunikativen Aspekt: Schon die Versammlung an sich dient der Kommunikation einer Meinung nach Außen (so jedenfalls bei Demonstrationen) − ebenso geschützt ist ihre innere Organisation, für die Kommunikation zwischen den Organisationsmitgliedern erforderlich ist.

---

616 *Mattcke/Pollock,* Die Technik des Aufstand, Technology Review v. 28.10.2011, abrufbar unter: http://www.heise.de/-1364854.html; dazu auch oben, Kap. 1.1.3.2.

617 *Denninger*, ZRP 2004, 101 ff., 103.

618 *Herzog,* in: *Maunz/Dürig*, GG 2011, Art. 4 Rn. 7; Art. 4 gewähre die „Freiheit des Redens".

619 Art. 5 Abs. 1 GG.

620 Art. 6 Abs. 1 GG umfasst das Recht auf eheliches und familiäres Zusammenleben, *OVG Berlin-Brandenburg* v. 28.4.2009, OVG 2 B 6.08; in der Entscheidung zum Großen Lauschangriff betont das *BVerfG* „Ehe und Familie haben (…) für die Kommunikation im höchstpersönlichen Bereich, gerade auch im Intimbereich, eine besondere Bedeutung. So fußt eine in der ehelichen Vertrautheit besonders leicht mögliche thematisch unbegrenzte Kommunikation mit dem Ehepartner auf der Erwartung, dass der Vorgang nicht von Außenstehenden zur Kenntnis genommen werden kann. Nichts anderes gilt für Gespräche mit anderen engsten Familienangehörigen, etwa Geschwistern und Verwandten in gerader Linie, insbesondere wenn sie im selben Haushalt leben", BVerfGE 109, 279, 331 f.

Schließlich sind auch Vorbereitungshandlungen[621] und damit auch die einer Versammlung vorgelagerte Kommunikation durch die Versammlungsfreiheit geschützt.

Für alle weiteren Freiheitsrechte könnte diese Auflistung fortgeführt werden, ob Berufsfreiheit, Recht auf informationelle Selbstbestimmung oder Eigentumsfreiheit. Jedes durch das Grundgesetz garantierte Freiheitsrecht erfasst auch einen kommunikativen Aspekt. Eben weil Kommunikation wesentlicher Bestandteil oder gar die Grundlage von Freiheit ist.[622]

Freiheit entsteht vielleicht im Geiste, erforderlich ist aber zur Gewährleistung von Freiheit, wie sie das Grundgesetz durch die Grundrechte zu garantieren sucht, Freiheitsräume zu schaffen und zwar zur Ausübung der Freiheitsrechte, die sämtlich einen kommunikativen Aspekt beinhalten.[623] Freiheitsräume können dabei auch als Kommunikationsräume beschrieben werden (wobei sie nicht darauf beschränkt werden dürfen).

Da heute Telekommunikationstechnologien die Grundrechtsausübung prägen, kommt der Gewährleistung der Telekommunikationsfreiheit besondere Bedeutung zu. Denn wie gezeigt wurde, beinhaltet jede grundrechtlich gewährleistete Freiheit einen Kommunikationsaspekt. Die Gewährleistung der Telekommunikationsfreiheit ist insoweit zentral für die Ausübung anderer Freiheitsrechte[624] und kann auch als Grundlage der Freiheit im digitalen Zeitalter bezeichnet werden.

2.1.4 Staatsorganisationsrechtliches Bekenntnis zur Freiheit

Nicht nur durch die Freiheitsrechte sondern auch durch die staatsorganisationsrechtlichen Bestimmungen wird Freiheit gesichert. Zwar wird der Begriff Freiheit nicht explizit in den Staatsfundamentalnormen (Art. 20 Abs. 1 und 28 Abs. 1 GG) angeführt, dennoch zielen gerade die tragenden Staatsstrukturprinzipien auf den Schutz der Freiheit.

2.1.4.1 Demokratieprinzip

Das Demokratieprinzip ist in Art. 20 Abs. 1 GG und Art. 2 GG normiert. Maßgeblich für die Demokratie in diesem Sinne ist, dass das Volk Träger der Staatsgewalt ist und sie selbst ausübt. Das Staatsvolk muss Entscheidungen durch seine Mehrheit und auf der Grundlage freier und gleicher Entscheidungen treffen.[625] Entsprechend müssen Wahlen frei sein.[626] Schon darin kommt die Bedeutung von Freiheit für das Demokratieprinzip zum Ausdruck. Entsprechend wird die Garantie von Freiheit und Gleichheit

---

621 *Schulze-Fielitz,* in: *Dreier,* GG 2004, Art. 8 Rn. 15; *Depenheuer,* in: *Maunz/Dürig*, GG 2011, Art. 8 Rn. 75.

622 Ganz in diesem Sinne geht *Luhmann* davon aus, dass der Mensch erst durch die Kommunikation mit anderen zum Menschen wird. Zur Leistungs- und Kommunikationstheorie zur Bestimmung der Menschenwürdegarantie, vgl. oben Kap. 2.1.1; insbes. Fn. 438.

623 In ähnliche Richtung formuliert *Hoffmann-Riem*: „Freiheit als selbstbestimme Verwirklichung und Interessenverfolgung soll es in der Kommunikation und durch Kommunikation geben." *Hoffmann-Riem* 2003, 59.

624 *Hoffmann-Riem*, JZ 2008, 1009.

625 *Sachs*, in: *Sachs,* GG 2011, Art. 20, Rn. 12.

626 *Robbers*, in: BK-GG 2011, Art. 20, Rn. 865.

des politischen Prozesses als Einzelausprägung des Demokratieprinzips verstanden.[627] Denn Wahlen können letztlich nur dann demokratische Legitimation vermitteln, wenn sie frei sind. Verlangt wird daher, dass zum einen die Stimmabgabe an sich frei von Zwang und unzulässigem Druck erfolgt (und zwar das Wie und das Ob), und zum anderen, dass auch die Wahlentscheidung in einem freien und offenen Prozess der Meinungsbildung gefällt werden kann.[628] Die „geistige Freiheit", wie sie die Menschenwürdegarantie voraussetzt,[629] wird somit auch durch das Demokratieprinzip geschützt.

2.1.4.2 Rechtsstaatsprinzip

Eines der tragenden Verfassungsprinzipien der Bundesrepublik Deutschland ist das Rechtsstaatsprinzip. Dieses ist in Art. 20 Abs. 2 S. 2 und Abs. 3 GG normiert. Mit der Betonung der Rechtsstaatlichkeit wurde die Abkehr vom Unrechtsstaat im Dritten Reich vollzogen.[630] Geprägt ist das Rechtsstaatsprinzip dabei durch die Erkenntnis, dass ein nachhaltiger, freiheitsverbürgender Rechtsstaat sowohl formeller als auch materieller Rechtsstaat sein muss.[631] Das heißt, es muss nicht nur formelle Rechtmäßigkeit gewahrt werden, sondern auch in materieller Hinsicht, nämlich indem Freiheit von jedweder staatlichen Willkür garantiert wird. Dieser Auftrag kann dem Rechtsstaatsprinzip entnommen werden. Konkretisiert wird dieses generelle Bekenntnis zu einem willkürfreien Staat durch zahlreiche Elemente, die das Rechtsstaatsprinzip prägen und die, soweit sie ihren Niederschlag auch noch in anderen Regelungen im Grundgesetz gefunden haben, dem Rechtsstaatsprinzip vorgehen. In Bezug auf den Schutz der Freiheit des Einzelnen, sind insbesondere zu nennen:[632] die Menschenwürdegarantie, die Grundrechtsbindung aller staatlichen Gewalt (Art. 1 Abs. 3 GG), die Rechtsweggarantie (Art. 19 Abs. 4 GG), die Gewaltenteilung (Art. 20 Abs. 2 GG), die Bindung an Verfassung, Gesetz und Recht (Art. 20 Abs. 3 Hs. 1 und Hs. 2 GG), die Ewigkeitsgarantie (Art. 79 Abs. 3 GG), das Rechtsprechungsmonopol der Gerichte (Art. 92 GG), die Unabhängigkeit der Richter (Art. 97 GG) und schließlich Verfahrensrechte bei Freiheitsentzug (Art. 104 GG). Darüber hinaus hat das *Bundesverfassungsgericht* als Bestandteile des Rechtsstaatsprinzips die Verpflichtung zur Gerechtigkeit, den Bestimmtheitsgrundsatz, das Rückwirkungsverbot, den Grundsatz der Verhältnismäßigkeit, die Justizgewährung und verschiedene Verfahrensanforderungen anerkannt.[633] Auch diesen Konkretisierungen des Rechtsstaatsprinzips kommt eine die Freiheit vor Willkür sichernde Funktion zu.

---

627 *Sachs*, in: *Sachs,* GG 2011, Art. 20, Rn. 13.

628 *Hofmann*, in: *Schmidt-Bleibtreu/Klein*, GG 2011, Art. 20, Rn. 48; *Kloepfer,* Verfassungsrecht I 2011, § 10 Rn. 133 ff.

629 Vgl. dazu schon oben S. 77, Fn. 447.

630 *Kloepfer,* Verfassungsrecht I 2011, § 10, Rn. 285; ähnlich auch *Sachs*, in: *Sachs,* GG 2011, Art. 20, Rn. 74.

631 *Kloepfer,* Verfassungsrecht I 2011, § 10 Rn. 12; Im Entwurf von Herrenchiemsee wurde der Rechtsstaat als Verwaltung auf Grund der Gesetze unter der Kontrolle unabhängiger, nur an das Gesetz gebundener Gerichte und ein gesicherter Schutz vor Missbrauch der Staatsgewalt beschrieben, *Sachs*, in: *Sachs*, GG 2011, Art. 20, Rn. 74; vgl. Art.2 Abs. 2 HChE.

632 Eine abschließende Aufzählung findet sich bei: *Sachs*, in: *Sachs,* GG 2011, Art. 20, Rn. 77.

633 *Sachs*, in: *Sachs,* GG 2011, Art. 20, Rn. 78 mit zahlreichen Nachweisen.

Mit dem Bestimmtheitsgrundsatz und dem Verhältnismäßigkeitsprinzip werden im Folgenden zwei zentrale Elemente des Rechtsstaatsprinzips erläutert, die materiell[634] die Einschränkbarkeit von Grundrechten begrenzen und damit für die Gewährleistung der Freiheit des Einzelnen besonders bedeutend sind.

2.1.4.2.1 Bestimmtheitsgrundsatz

Das Rechtsstaatsprinzip verlangt, dass staatliches Handeln auf hinreichend bestimmten Regelungen basiert.[635] „Das Bestimmtheitsgebot soll sicherstellen, dass der demokratisch legitimierte Parlamentsgesetzgeber die wesentlichen Entscheidungen über Grundrechtseingriffe und deren Reichweite selbst trifft, dass Regierung und Verwaltung im Gesetz steuernde und begrenzende Handlungsmaßstäbe vorfinden und dass die Gerichte eine wirksame Rechtskontrolle durchführen können. Ferner erlauben die Bestimmtheit und Klarheit der Norm, dass der betroffene Bürger sich auf mögliche belastende Maßnahmen einstellen kann".[636] Für den Bürger soll die Rechtsordnung eine sichere Grundlage für sein Verhalten bieten.[637] Schließlich handelt es sich bei der Verlässlichkeit der Rechtsordnung um eine Grundbedingung freiheitlicher Verfassungen.[638] Die Anforderungen an die Bestimmtheit eines Gesetzes sind dabei umso höher, je stärker bei Missachtung der Gesetze oder durch das Gesetz selbst in den Freiheitsbereich der Bürger eingegriffen wird.[639]

So führt das *Bundesverfassungsgericht* aus, dass das Bestimmtheitsgebot für Ermächtigungen zu Überwachungsmaßnahmen zwar nicht verlange, „dass die konkrete Maßnahme vorhersehbar ist, wohl aber, dass die betroffene Person grundsätzlich erkennen kann, bei welchen Anlässen und unter welchen Voraussetzungen ein Verhalten mit dem Risiko der Überwachung verbunden ist. Hinreichend bestimmte Voraussetzungen des staatlichen Eingriffs − und damit der ihn begrenzenden Maßstäbe − kommen auch Personen zugute, denen die konkreten Handlungsvoraussetzungen nicht bekannt sein können, weil sie den Anlass nicht geschaffen haben und eher zufällig betroffen sind."[640]

2.1.4.2.2 Verhältnismäßigkeitsprinzip

Von herausragender Bedeutung als „Schranken-Schranke" von Grundrechtseingriffen, ist der Grundsatz der Verhältnismäßigkeit. Dieser wird auch als Übermaßverbot bezeichnet und ist materielle Ausprägung des Rechtsstaatsprinzips. Er bindet den Staat

---

634 Sie sind insofern Ausdruck der materiellen Rechtsstaatlichkeit, die auch höchstrichterlich anerkannt ist: „Zur Rechtsstaatlichkeit gehört auch (…) die materielle Gerechtigkeit.", BVerfGE 20, 323 (331); dazu auch BVerfGE 21, 378 (388); 95, 96 (130); 52, 131 (144).

635 *Robbers,* in: BK-GG 2011, Art. 20 Rn. 2128.

636 BVerfGE 120, 378 (407); so oder ganz ähnlich auch: BVerfGE 8, 274 (325); 21, 73 (79); 108, 186 (235); 110, 33 (52 ff.); 113, 348 (375 f.); vgl. auch *Sachs*, in: *Sachs,* GG 2011, Art. 20, Rn. 126, 129; *Sodan*, in: *Sodan*, GG , Vorb. v. Art. 1, Rn. 59.

637 *Kloepfer,* Verfassungsrecht I 2011, § 10 Rn. 142.

638 *Robbers,* in: BK-GG 2011, Art. 20 Rn. 2133.

639 *Kloepfer,* Verfassungsrecht I 2011, § 143. Darum ist auch für Strafgesetze das Bestimmtheitsgebot ausdrücklich in Art. 103. Abs. 2 GG normiert. Dazu auch *Robbers,* in: BK-GG 2011, Art. 20 Rn. 2136.

640 BVerfGE 113, 348 (376) – leitet hier das Bestimmtheitsgebot unmittelbar aus Art. 10 GG ab.

bei Eingriffen in die Freiheitssphäre der Bürger.[641] Er ist in ständiger Rechtsprechung anerkannt und besitzt Verfassungsrang.[642]

Der Verhältnismäßigkeitsgrundsatz verbietet, dass der Einzelne unnötigen Eingriffen der öffentlichen Gewalt ausgesetzt wird. Sollte ein gesetzlicher Eingriff unerlässlich sein, müssen die Mittel, um dieses Ziel zu erreichen, geeignet sein und sie dürfen den Einzelnen nicht übermäßig belasten.[643] Es wird demnach durch den Verhältnismäßigkeitsgrundsatz gewährleistet, dass staatliche Eingriffsmaßnahmen prinzipiell zu begrenzen sind, damit der Bürger der staatlichen Gewalt nicht unbegrenzt und willkürlich ausgeliefert ist.[644]

Dahinter steht der Gedanke, dass staatliche Maßnahmen nicht prinzipiell unbegrenzt und unbegründet sein dürfen. Vielmehr muss jeder Eingriff gerechtfertigt werden. Und zwar dadurch, dass er einen benennbaren Zweck verfolgt und in seinem Umfang und Ausmaß gemessen an dem verfolgten Zweck, nicht außer Verhältnis steht. Das heißt, wenn in Freiheitsrechte des Bürgers eingegriffen wird, muss dies verhältnismäßig sein.

Dafür muss der Eingriff zunächst einem *legitimen Zweck* zu dienen bestimmt sein, sowie zur Erreichung dieses *geeignet, erforderlich* und *angemessen* sein.[645] Eine Maßnahme ist geeignet, wenn sie die Zweckerreichung fördert. Verlangt wird dafür nicht, dass das Regelungsziel in jedem Fall tatsächlich erreicht werden muss.[646] Die Erforderlichkeit ist gegeben, wenn kein gleich geeignetes, weniger einschneidendes Mittel ersichtlich ist.[647] Angemessen oder verhältnismäßig i.e.S. ist ein Instrument dann, wenn es in einem angemessenen Verhältnis zu dem Gewicht und der Bedeutung des Grundrechts steht.[648]

---

641 Hat sich insbesondere in der Rspr des *BVerfG* entwickelt, welches es aus dem Rechtsstaatsprinzip und dem Wesen der Grundrechte abgeleitet hat, BVerfGE 19, 342 (348); 61, 126 (134); 113, 154 (162); dazu auch *Voßkuhle*, JuS 2007, 429, 429; *Sodan*, in: *Sodan,* GG, 2011, Vorb. v. Art. 1, Rn. 60 ff. Der Grundsatz der Verhältnismäßigkeit hat seinen Ursprung in der Beschränkung polizeilicher Maßnahmen, hat sich aber in seiner Entwicklung vom Polizeibegriff gelöst, dazu von *Krauss* 1955, 5, 8ff.; Davon zu unterscheiden ist das Untermaßverbot, welches den staatlichen Zugriff auf geschützte Rechtspositionen nicht beschränkt, sondern im Gegenteil den Staat zu solchen Zugriffen legitimiert oder sogar verpflichtet, *Grzeszick,* in: *Maunz/Dürig,* GG 2011, Art. 20, Rn. 108; Auch das Übermaßverbot kann nicht einfach mit dem Verhältnismäßigkeitsgrundsatz gleichgesetzt werden, wie dies bisweilen indifferent erfolgt, da er eine speziellen Aspekt des Verhältnismäßigkeitsgrundsatzes beschreibt und sich allein auf die Erforderlichkeit und Angemessenheit einer Maßnahme bezieht, so *Robbers,* in: BK-GG 2011, Art. 20 Rn. 1906; Die Wurzeln des Verhältnismäßigkeitsgrundsatzes reichen historisch auf das Kreuzberg-Urteil zurück, *Pieroth/Schlink/Kniesel* 2012, § 1 Rn. 12, vgl. zu diesem auch oben S. 61.

642 *Robbers,* in: BK-GG 2011, Art. 20 Rn. 1876.

643 *Robbers,* in: BK-GG 2011, Art. 20 Rn. 1878; BVerfGE 17, 306 (313); 55, 159 (165).

644 *Grzeszick,* in: *Maunz/Dürig,* GG 2011, Art. 20, Rn. 107.

645 BVerfGE 109, 279 (335ff); 115, 320 (345); 118, 168 (193); 125, 260 (316).

646 BVerfGE 63, 88 (115); 67, 157 (175); 96, 10 (23); 103, 293 (307); 125, 260 (316).

647 BVerfGE 120, 274 (321).

648 *Hesse* 1995, Rn. 318; stRspr BVerfGE 107, 299 (322); 109, 279 (351).

Die Feststellung, dass Zweck und Mittel nicht außer Verhältnis zueinander stehen, besagt nichts darüber, ob das Verhältnis auch optimal ist.[649] Die Optimierung aller denkbaren Zweck-Mittel-Relationen ist nicht Inhalt der Verhältnismäßigkeitsprüfung, sondern obliegt grundsätzlich der Einschätzungsprärogative der Legislative.[650]

Bei der Verhältnismäßigkeit handelt es sich zwar um ein Gebot des Rechtsstaatsprinzips, im Vordergrund steht jedoch immer der Bezug zum konkreten Grundrecht.[651]

Auch in der Rechtsprechung von *Europäischem Gerichtshof* und *Europäischem Gerichtshof für Menschenrechte* ist der Grundsatz der Verhältnismäßigkeit anerkannt.[652] In Art. 52 Abs. 1 S. 2 EU-GRCh. ist er sogar ausdrücklich normiert. Auch ist er als allgemeiner Rechtsgrundsatz im Gemeinschaftsrecht verankert.

2.1.4.3 Gewaltenteilung

Als weiteres, das Grundgesetz tragendes Organisations- und Funktionsprinzip[653] dient die Gewaltenteilung der Sicherung einer freiheitlichen Gesellschaftsordnung und damit auch der Freiheit des Einzelnen. Die Gewaltenteilung ist im Grundgesetz ausdrücklich normiert durch die Garantien in Art. 1 Abs. 3 GG als auch durch Art. 20 Abs. 2 S. 2 GG. Sie ist darüber hinaus auch ein Element des Rechtsstaatsprinzips.[654]

Der Grundgedanke der Gewaltenteilung reicht zurück in die griechische Antike. In der griechischen Staatsphilosophie *Platons* und *Aristoteles* stand allerdings der „Ordnungsgedanke" im Mittelpunkt.[655] Erst *Locke* und *Montesquieu* entwickelten den Gedanken, dass durch Gewaltenteilung Machtbeschränkung erfolgen könne.[656] Das Ziel der Mäßigung der Staatsherrschaft wird heute als zentrale Funktion der Gewaltenteilung betrachtet. Sie dient damit auch dem Schutz der Freiheit des Einzelnen.[657] Daneben hat sie auch die Funktionen, die Staatsaufgaben sinnvoll aufzuteilen sowie schließlich eine demokratiesichernde Funktion.[658] Durch die Aufteilung der Gewalten können staatliche Machtkonzentrationen und die damit verbundene Gefahr des Machtmiss-

---

649 *Grabitz*, AöR1973 (Bd. 98), 568, 576.

650 *Michael*, JuS 2001, 148, 149.

651 *Sommermann*, in: *Mangoldt/ Klein/ Starck*, GG 2010, Art. 20 Abs. 3, Rn. 313; Denn Voraussetzung der Anwendung des Verhältnismäßigkeitsgrundsatzes ist, dass eine Rechtsposition konkret betroffen wird, *Jarass,* in: *Jarass/Pieroth,* GG Komm 2011, Art. 20, Rn. 81; *Kloepfer* betont, dass der Anwendungsschwerpunkt des Übermaßverbots im Bereich der Grundrechte liege, *Kloepfer,* Verfassungsrecht I 2011, § 10 Rn. 197.

652 *Robbers,* in: BK-GG 2011, Art. 20 Rn. 1886 ff.; zur Verhältnismäßigkeitsprüfung durch den *EGMR Frenz* 2009, Rn. 602.

653 *Sachs,* in: *Sachs,* GG 2011, Art. 20, Rn. 81.

654 Zum Rechtsstaatsprinzip oben Kap. 2.1.4.2.

655 *Kloepfer,* Verfassungsrecht I 2011, § 10 Rn. 46.

656 Wobei *Locke* lediglich eine Zweiteilung der Gewalten vorsieht. Erst *Montesquieu* differenziert zwischen den drei Gewalten: Exekutive, Legislative und Judikative; dazu ausführlich *Kloepfer,* Verfassungsrecht I 2011, § 10 Rn. 46.

657 *Kloepfer,* Verfassungsrecht I 2011, § 10 Rn. 49; *Sachs*, in: *Sachs,* GG 2011, Art. 20, Rn. 81; vgl. auch BVerfGE 9, 268 (279); 95, 1 (17).

658 Und zwar indem sie sicherstellt, dass durch die wechselseitigen Einflussmöglichkeiten gewährleistet wird, dass verschiedene Interessengruppen am staatlichen Willensbildungsprozess beteiligt werden, *Kloepfer,* Verfassungsrecht I 2011, § 10 Rn. 49.

brauchs wirksam begrenzt werden. Die gegenseitige Kontrolle der Gewalten ist durch die Staatsorganisation garantiert. Zudem besteht durch die Organisation Deutschlands als Bundesrepublik auch eine horizontale Gewaltenteilung, die den Effekt der Machtbegrenzung und der Aufgabenverteilung noch verstärkt.

2.1.4.4 „Freiheitlich, demokratische Grundordnung"

Neben der Zielsetzung eine freie Gesellschaftsordnung zu schaffen, wie sie etwa in Demokratie- und Rechtsstaatsprinzip und der Aufteilung der Gewalten seinen Ausdruck findet, gibt es noch andere Anknüpfungspunkte, um die Annahme zu begründen, dass mit den staatsorganisationsrechtlichen Regelungen die Bundesrepublik als eine freie Gesellschaft freier Individuen konstituiert wurde.

Der Begriff Freiheit im abstrakten Sinn findet sich im Grundgesetz (nur) in der Formel „freiheitlich demokratischen Grundordnung".[659] Diese wird in zahlreichen Artikeln verwendet.[660] Allerdings ist zu beachten, dass dieses Verfassungskürzel nicht unmittelbar Freiheiten gewährt, sondern es sich vielmehr um ein Tatbestandsmerkmal verfassungsunmittelbarer Grundrechtsschranken handelt.[661] Das heißt, die Formel dient im Ergebnis der Legitimation von Grundrechtseingriffen. Dies zeigt aber, dass die Ordnung des Grundgesetzes einen Eingriff in die Freiheit des Einzelnen allein zu Gunsten der Freiheit aller/ der anderen als legitim erachtet.[662]

Zudem verdeutlicht die vielfache Nennung dieser Formel, dass es sich um ein zentrales Strukturprinzip in der Verfassung handelt. Zu beachten ist, dies zeigt der Konstitutionsprozess, dass „freiheitlich" nicht zwingend vor demokratisch steht. Es geht insofern nicht allein um die Beschreibung einer „freiheitlichen Demokratie", sondern auch um eine freiheitliche Grundordnung.[663]

Das *Bundesverfassungsgericht* definiert die freiheitlich demokratische Grundordnung als Ordnung, „die unter Ausschluss jeglicher Gewalt- und Willkürherrschaft eine rechtsstaatliche Herrschaftsordnung auf der Grundlage der Selbstbestimmung des Volkes nach dem Willen der jeweiligen Mehrheit und der Freiheit und Gleichheit darstellt".[664] Dazu gehört unter anderem „die Achtung vor den im Grundgesetz konkretisierten Menschenrechten, vor allem vor dem Recht der Persönlichkeit auf Leben und freie Entfaltung".[665] Mittelbar wird durch die Formel der freiheitlich demokratischen Grundordnung als Tatbestandsmerkmal von Grundrechtsschranken die verfassungs-

---

659 *Merten,* in: HGR I, 2006, § 27 Rn.2, Rn. 32; zur Substanz des Begriffs und ihrer Begründung, *Streinz,* in: *Mangoldt/Klein/Starck,* GG 2010, Art. 21 Rn. 224 ff.

660 Art. 10 Abs. 2 S. 2; 11 Abs. 2; 18; 21 Abs. 2; 73 Nr. 10b; 87a Abs. 4 S. 1; 91 Abs. 1 GG; wobei der Begriff selbst in allen Vorschriften einheitlich ausgelegt wird. Viele dieser Normen haben zudem erst im Rahmen von Verfassungsänderungen Eingang in das GG gefunden, dazu ausführlich *Merten,* in: HGR I, 2006, § 27 Rn. 32.

661 So auch *Merten,* in: HGR I, 2006, § 27 Rn. 32.

662 *Roßnagel*, Informatik-Spektrum 2002, 33, 35.

663 *Merten,* in*:* HGR I, 2006, § 27 Rn. 33 legt hier ausführlich dar, welche historischen Gründe dazu führten, dass die Bezeichnung so wie sie heute ist, gewählt wurde.

664 BVerfGE 2, 1 (12 f.); Jedoch ohne Angabe konkreter Verfassungsbestimmungen.

665 BVerfGE 2, 1 (12 f.).

rechtliche Ordnung als Raum beschrieben, in welchem dem Bürger die freie Entfaltung seiner Persönlichkeit zugestanden wird.

2.1.5 „Der Staat als Diener der Freiheit"

Die Staatsorganisation, geprägt durch Rechtsstaatlichkeit und Demokratie, bringt zum Ausdruck, dass mit dem Grundgesetz ein Staat konstituiert wurde, um die Freiheiten des Einzelnen zu sichern.[666] Die umfassende Analyse der Verfassungsnormen zeigt, dass diese im Kern alle auf den Schutz von Freiheit zielen.[667] Dabei wird primär die Freiheit des Individuums durch die Grundrechte geschützt. Daneben dient aber auch die Staatsorganisation der Gewährleistung von Freiheit. Ziel ist dabei nicht nur die Freiheit des Einzelnen zu schützen, sondern auch die Freiheit aller.

Zulässig ist es so, dem Grundgesetz im Wege der Systembildung ein Prinzip[668] „Freiheit" zu entnehmen, auch wenn es eben nicht ausdrücklich in der Verfassung genannt ist.[669] Richtigerweise betont *Merten*, dass auch wenn ein Prinzip Freiheit dem Grundgesetz zu entnehmen ist, man im Umgang mit diesem Vorsicht walten lassen müsse. Die Feststellung, dass es ein Prinzip Freiheit gibt, macht die Prüfung von Einzelfragen nicht obsolet.[670] Dennoch ist die Feststellung, dass ein Prinzip Freiheit im Grundgesetz verankert ist, nicht zu missachten, so kann es als „Widerlager wirken, um ein exzessives Vordringen gegenläufiger Prinzipien (…) zu hindern."[671]

Fest steht jedenfalls, dass mit der umfassenden Gewährleistung von Freiheit durch die Verfassung, der Staat quasi als Diener der Freiheit konzipiert wurde.[672] Es ist seine vorrangige Aufgabe, ein möglichst hohes Maß an Freiheit zu realisieren.[673] Die Freiheit des Einzelnen wird im Interesse aller Bürger und „einer freiheitsorientierten Gesellschaftsordnung" durch das Grundgesetz geschützt.[674]

2.2 Sicherheit

Es wird vom Staat erwartet, dass dieser für Sicherheit[675] sorgt. Die Gewährleistung von (innerer und äußerer) Sicherheit ist ureigenste Aufgabe des Staates.[676] Gemeinsam

---

666 Die Überschrift entspricht einer Überschrift aus: *Roßnagel*, Informatik-Spektrum 2002, 33, 34.

667 Diese Auffassung findet sich schon bei *Locke* „Man being born … with a Title to perfect Freedom…", zitiert nach *Merten,* in*:* HGR I, 2006, § 27 Rn.12

668 „Der Gewinnung von Verfassungsprinzipien liegt die Erkenntnis zugrunde, daß sich die les legum nicht in einzelnen Verfassungsvorschriften erschöpft, sondern daß dahinter allgemeine Leitvorstellungen oder Grundsätze stehen können, die sich zu einer Ganzheit zusammensetzen lassen", *Merten,* in: HGR I, 2006, § 27 Rn. 40; unterscheidet im Folgenden zwischen expliziten Prinzipien, die als solche Rechtswirkungen entfalten und impliziten, die nur soweit wirken wie die ihnen zu Grunde liegenden Einzelaussagen in ihrer Gesamtheit, (Rn. 41).

669 *Merten,* in: HGR I, 2006, § 27 Rn. 39.

670 *Merten,* in*:* HGR I, 2006, § 27 Rn. 42.

671 *Merten,* in: HGR I, 2006, § 27 Rn. 42.

672 Den Staat bezeichnet auch *Roßnagel*, Informatik-Spektrum 2002, 33, 34 als „Diener der Freiheit".

673 *Roßnagel* 2003, 18.

674 *Roßnagel*, Informatik-Spektrum 2002, 33, 35.

675 Im Zentrum steht, auch wenn hier der allgemeine Begriff Sicherheit verwendet wird, die „innere Sicherheit". Im Polizeirecht wird das Begriffspaar „öffentlich Sicherheit und Ordnung verwendet", zu den Begriffen, *Götz,* in: *Isensee*/*Kirchof*, HStR IV 2006, § 85 Rn. 4. Im einfachen Recht, etwa

mit der Gewährleistung von Frieden bildet sie seit jeher die Legitimationsgrundlagen der Staatlichkeit.[677] So auch das *Bundesverfassungsgericht*: „Die Sicherheit des Staates als verfaßter Friedens- und Ordnungsmacht und die von ihm zu gewährleistende Sicherheit seiner Bevölkerung sind Verfassungswerte, die mit anderen im gleichen Rang stehen und unverzichtbar sind, weil die Institution Staat von ihnen die eigentliche und letzte Rechtfertigung herleitet".[678] So wird die Gewährleistung innerer Sicherheit auch als Kernaufgabe des Staates bezeichnet[679] oder als Merkmal zur Beschreibung des modernen Staats genutzt.[680]

Dabei kann vorab festgestellt werden, dass das Grundgesetz insgesamt die Pflicht zur Gewährleistung von (innerer) Sicherheit nicht ausdrücklich normiert. Dass es daran fehlt, wird damit begründet, dass es sich schließlich bei der Gewährleistung von Sicherheit um eine Selbstverständlichkeit handle und daher eine positivierte materiellrechtliche Grundlage entbehrlich sei.[681] Allein in Art. 13 Abs. 4 und 7 GG, Art. 24 Abs. 2 GG, Art. 35 Abs. 2 S. 1 GG und Art. 73 Abs. 1 Nr. 10 b) GG wird der Begriff „Sicherheit" verwendet.

In Art. 35 Abs. 2 S. 1 GG ist die Möglichkeit der Länder normiert, in besonders bedeutenden Fällen „zur Aufrechterhaltung der Wiederherstellung der öffentlichen Sicherheit und Ordnung" Unterstützung des Bundesgrenzschutzes anzufordern.[682] Zur Begründung der Staatsaufgabe Sicherheit wird diese Kompetenzzuweisung ebenso wenig wie Art. 13 Abs. 4, 7 und Art. 24 Abs. 2 GG soweit ersichtlich nicht herangezogen.

Jedoch wird vereinzelt Art. 73 Abs. 1 Nr. 10 b) GG als materielle Grundlage der Staatsaufgabe (innere) Sicherheit interpretiert.[683] Dieser weist dem Bundesgesetzeber die Kompetenz für die Regelung der Kooperation von Bund und Ländern „zum Schutze der freiheitlichen demokratischen Grundordnung, des Bestandes und der Sicherheit des Bundes oder eines Landes (Verfassungsschutz)" zu. Gegen diese Ansicht spricht vor allem, dass hier ein Teilbereich der inneren Sicherheit – nämlich die Kompetenz zur Zusammenarbeit von Bund und Ländern geregelt ist – und nicht generell die Auf-

---

in § 120 Abs. 1 G*VG*, wird der Begriff der inneren Sicherheit mit einem besonderen, eingeschränkten Bedeutungsgehalt verwendet, dazu *Götz,* in: *Isensee*/*Kirchof*, HStR IV 2006, § 85 Rn. 8. Hinzuweisen ist darauf, dass heute innere und äußere Sicherheit als „eng und geradezu untrennbar" angesehen werden, *Götz,* in: *Isensee*/*Kirchof*, HStR IV 2006, § 85 Rn. 17.

676 *Roßnagel* 2003, 18; als älteste Konkretion des Gemeinwohls bezeichnet sie *Link*, VVDStRL 1990, 7; Zum historischen Hintergrund und dem rechtsphilosophischen Fundament, schon oben Kap. 1.1.

677 *Horn* 2003, 440.

678 BVerfGE 49, 24, (56 f.); zuvor bereits BVerwGE 49, 202 (209).

679 *Papier*, DVBl. 2010, 801, 803.

680 *Kloepfer* 2011, § 1 Rn. 44.

681 *Werthebach/Droste*, in: BK-GG 1998, Art. 73 Nr. 10, Rn. 52.

682 Die Definition von öffentlicher Sicherheit und Ordnung in Art. 35 Abs. 2, S. 1 GG entspricht der des Polizeirechts. *Erbguth*, in: *Sachs,* GG 2011, Art. 35, Rn. 35.

683 So etwa *Götz,* in: *Isensee*/*Kirchof*, HStR IV 2006, § 85 Rn. 17, 23; *Werthebach/Droste*, in: BK-GG, 1998, Art. 73 Nr. 10, Rn. 48 ff., 52; Mit Art. 73 Nr.10 würde „Sicherheit als vornehmstem aller Staatszwecke" zur Staatsaufgabe erhoben werden, vgl. *Degenhardt*, in: *Sachs,* GG 2011, GG, Art. 73, Rn. 49.

gabe Sicherheit im Inneren zu gewährleisten formuliert ist. Auch Art. 73 Abs. 1 Nr. 10 b) GG setzt so das Bestehen der Staatsaufgabe Sicherheit voraus. Er kann diese daher nicht begründen.[684]

Dass der Staat Sicherheit im Inneren zu gewährleisten hat, ist dennoch allgemein anerkannt.[685] Die Ansätze zur Begründung der Staatsaufgabe und des Staatsziels[686] (innerer) Sicherheit unterscheiden sich jedoch. Es soll im Folgenden erörtert werden, wie die Pflicht zur Gewährleistung von Sicherheit verfassungsrechtlich begründet werden kann und in welchem Umfang das Grundgesetz den Staat verpflichtet Sicherheit im Inneren zu garantieren.

2.2.1 Gewaltmonopol und Rechtsstaatsprinzip

Vielfach wird die Staatsaufgabe Sicherheit mit dem staatlichen Gewaltmonopol begründet: „Erst die Monopolisierung der Gewalt macht den Staat zum Friedensverband."[687] Da der Staat das Gewaltmonopol[688] innehabe, müsse er für die Sicherheit sorgen, da ansonsten seine Staatsgewalt in Frage gestellt würde.[689] Das Gewaltmonopol selbst ist nicht ausdrücklich im Grundgesetz normiert, es ergibt sich normativ aus Art 20 Abs. 1 GG.

Hier ist die Staatlichkeit der Bundesrepublik normiert.[690] Ein „Staat" wird im Sinne der allgemein anerkannten *Jellinek'schen* Drei-Elemente-Lehre durch Staatsvolk, Staatsgebiet und Staatsgewalt konstituiert.[691] Staatlichkeit setzt also voraus, dass es eine Staatsgewalt gibt und zwar eine, die das Gewaltmonopol innehat.[692]

Von anderen wird ohne Bezug auf Art. 20 Abs. 1 GG das Gewaltmonopol anerkannt und zwar mit der Begründung, dass das neuzeitliche Staatsverständnis das staatliche Gewaltmonopol voraussetzt.[693]

---

684 *Degenhardt,* in: *Sachs,* GG 2011, Art. 73, Rn. 49.

685 *Isensee* 2003, 25, Fn. 36 mit zahlreichen Nachw.

686 Es ist zwischen Staatsaufgaben und Staatszeilen zu unterscheiden. Während Staatsaufgaben sich auf einen bestimmten abgegrenzten Sektor beziehen, strahlen Staatsziele auf die gesamte Staatstätigkeit aus, dazu *Isensee,* in: *Isensee/Kirchof* HStR IV, § 73 Rn. 16.

687 *Roßnagel* 1984, 59; *Isensee* formuliert „Am Anfang des modernen Staates steht seine Aufgabe, das Leben und die aber der Bürger vor dem Übergriff anderer zu schützen, die physische Gewalt Privater zu bannen und eine Ordnung des inneren Friedens sicherzustellen. Um dieses Zieles willen beansprucht die Staatsorganisation das Gewaltmonopol." *Isensee,* in: *Isensee/Kirchof* HStR IV, § 71 Rn.76.

688 Das staatliche Gewaltmonopol wird verstanden als Möglichkeit der physischen Gewaltanwendung des Staates und ist ein unverzichtbarer Bestandteil staatlicher Daseinssicherung und Zukunftsvorsorge, *Stober*, NJW 1997, 889, 890.

689 *Bull* 1977, 349; in diesem Sinne auch *Scholz*, NJW 1983, 705, 707.

690 *Robbers,* in: BK-GG 2011, Art. 20 Rn. 177; andere gehen davon aus, dass e seiner Erwähnung des Gewaltmonopols im Grundgesetz gar nicht bedarf, *Bull* 1977, 349.

691 *Jellinek,* Allgemeine Staatslehre 1959, 183, 394 ff; ausführlich zu dieser und auch der Kritik an ihr *Kettler* 1995, 21 ff.; vgl. auch *Schliesky* 2004, 25.

692 *Robbers,* in: BK-GG 2011, Art. 20 Rn. 182.

693 *Link*, VVDStRL 1990, 7, 28; vgl. auch Fn. 687.

Das Gewaltmonopol des Staates ist eng mit dem Rechtsstaatsprinzip verknüpft. Denn die dem Rechtsstaatsprinzip zu Grunde liegende Vorstellung, dem Menschen vor Willkür zu schützen und ihm also Freiheit (vor Willkür) zu gewähren, ist erst möglich, wenn die Befugnis, Gewalt auszuüben, nicht ein Jedermanns-Recht ist, sondern vielmehr der Einzelne dieses Recht abgegeben hat:[694] „Im Rechtsstaat sollen Gewalt und Zwang nur noch nach Maßgabe des Rechts und nicht nach Willkür und Belieben angewendet werden dürfen. Nicht Menschen, sondern das Recht soll herrschen."[695] So wird Sicherheit auch als Bestandteil der zentralen Verfassungsidee der Rechtsstaatlichkeit ausgemacht.[696] „Der Rechtsstaat gibt sich nicht nur Preis, wenn er die Freiheit seiner Bürger unterdrückt, sondern auch, wenn er ihnen die Sicherheit vorenthält."[697]

Letztlich unterscheiden sich die verschiedenen Ansätze zur Begründung des Gewaltmonopols nicht nachhaltig. Jedenfalls besteht Einigkeit dahingehend, dass das Grundgesetz dem Staat das Gewaltmonopol zuerkennt.

Nicht zu bestreiten ist, dass dieses seinen Sinn verliert, wenn der Staat der, der Legitimation dieses Monopols dienenden, Aufgabe nämlich der Gewährleistung von Sicherheit und Ordnung nicht mehr nachkommt. Es ist die älteste aller Aufgabe, die dem Gemeinwesen zukommt und seit Jahrhunderten gilt.[698] Insofern kann festgehalten werden, da die Bundesrepublik in der Verfassung als Staat konstituiert ist, eine ihrer Aufgaben die Gewährleistung von (innerer) Sicherheit ist.

Der Staatszweck Sicherheit wird, da Voraussetzung der Staatlichkeit, als in seiner „Kernsubstanz" unantastbar bezeichnet.[699] Entsprechend setzt das Gewaltmonopol auch Tendenzen zur Privatisierung der Staatsaufgabe Sicherheit, wie sie beobachtet werden können,[700] Grenzen. Der Staat muss selbst über die erforderlichen Instrumente und das notwendige Personal verfügen, um grundsätzlich Sicherheit zu gewähren und vor allem auch soweit er das Gewaltmonopol durchsetzt.[701]

Die Verpflichtung auf den Rechtsstaat und die Begründung der Staatlichkeit bilden das materielle Fundament der Verpflichtung des Staates, Sicherheit im Inneren zu gewähren.

Die Pflicht Sicherheit zu erzeugen, zeigt sich heute jedoch überwiegend im „modernen Gewande der Ableitung von Schutzpflichten aus den Grundrechten". [702]

---

694 Zur Entwicklung des modernen Rechtsstaats, vgl. Kap. 1.1.
695 *Roßnagel* 1984, 59.
696 *Götz,* in: *Isensee*/*Kirchof*, HStR IV 2006, § 85 Rn. 20.
697 *Isensee* 1983, 60; ähnlich auch *Isensee* 2003, 31.
698 *Bull* 1977, 347. Dazu auch schon oben S. 10 ff.
699 *Stober*, NJW 1997, 889, 890
700 Dazu oben Kap. 1.4.2.3; Dennoch besteht kein grundsätzliches Privatisierungsverbot. Der Frage, wo die Grenze genau zu ziehen ist, wird in Kap. 9.2.1.1 nachgegangen.
701 Vgl. dazu auch unten S. 297 f.
702 *Götz,* in: *Isensee*/*Kirchof*, HStR IV 2006, § 85 Rn. 21.

2.2.2 Schutzpflichten zu Gunsten der Grundrechte

Schutzpflichten des Staates werden als „rechtsstaatlicher Ausgleich für das staatliche Gewaltmonopol und das Gewaltverbot für Private“ betrachtet, da für den Einzelnen der Verzicht auf das Recht zur Verteidigung seiner Rechtsgüter nur in Betracht kommt, wenn er sie durch den Staat gesichert sieht.[703] Logisch kann das Bestehen von Schutzpflichten so als Kehrseite des staatlichen Gewaltmonopols begriffen werden.

Entsprechend hat sich auch die Auffassung durchgesetzt, dass die Grundrechte als Sitz von Schutzpflichten des Staates die Grundlage des Staatsziels der inneren Sicherheit bilden.[704] Nicht zuletzt, weil das *Bundesverfassungsgericht* in ständiger Rechtsprechung[705] die schutzrechtliche Seite der Grundrechte immer wieder betont hat.[706] Art. 2 Abs. 1 GG verpflichte i.V.m. Art. 1 Abs. 2 GG „den Staat dazu, das Leben und die körperliche Unversehrtheit des Einzelnen zu schützen, das heißt vor allem, auch vor rechtswidrigen Eingriffen von Seiten anderer zu bewahren“. Es hebt hervor, dass der Schutzpflicht des Staates ein hohes verfassungsrechtliches Gewicht zukommt. Gleiches gilt für das Rechtsgut der Freiheit einer Person i.S.v. Art. 2 Abs. 2 S. 2 GG, auch hier treffen den Staat umfassende Schutzpflichten.[707] Da das menschliche Leben die vitale Basis der Menschwürde und die Voraussetzung aller anderen Grundrechte ist, kommt ihr innerhalb der grundgesetzlichen Ordnung ein Höchstwert zu.[708]

Kloepfer hält das Lebensgrundrecht sogar für das „höchstrangige Verfassungsgut“, für den „höchsten Wert“ schlechthin.[709] In ständiger Rechtsprechung wird aus der hervorgehobenen Stellung in der Verfassungsordnung unmittelbar die Pflicht des Staates abgeleitet, „jedes menschliche Leben zu schützen, es vor allem vor rechtswidrigen Eingriffen von Seiten anderer zu bewahren.“[710] Auch wenn die Rechtsprechung des *Bundesverfassungsgerichts* zur Schutzpflichtendimension der Grundrechte häufiger technische Gefährdungen betraf als die Verbrechensbekämpfung, ist anerkannt, dass die grundrechtlich hergeleiteten Schutzpflichten auch den Schutz vor Verbrechen erfassen.[711]

Bei der Erfüllung von Schutzpflichten kommt dem Staat ein weiter Einschätzungs- und Gestaltungspielraum zu. Gefordert ist insofern nicht, dass mit absoluter Sicherheit Grundrechtsgefährdungen ausgeschlossen werden.[712] Grundsätzlich ist die Frage, wie staatliche Organe ihren Schutzplichten nachkommen, in eigener Verantwortung zu entscheiden.[713] Das *Bundesverfassungsgericht* hat insofern nur eine eingeschränkte

---

703 *Hopfauf*, in: *Schmidt-Bleibtreu/Klein*, GG 2011, Einl., Rn. 130; vgl. auch Fn. 702.
704 *Götz,* in: *Isensee*/*Kirchof*, HStR IV 2006, § 85 Rn. 24.
705 BVerfGE 39, 1 (419); 46, 160 (164); 49, 89 (141f.); 53, 30 (57); 56, 54 (73); 77, 170 (214); 88, 203 (251ff.); 92, 26 (46); 93, 1 (16); 115, 118 (152ff.).
706 *Hopfauf*, in: *Schmidt-Bleibtreu/Klein*, GG 2011, Einl. Rn. 142.
707 BVerfGE 115, 320 (346).
708 *Roßnagel* 1984, 53 mit Verweis auf: BVerfGE 39, 1 (42); 46, 160 (164); 49, 24 (53).
709 *Roßnagel* 1984, 53.
710 *Roßnagel* 1984, 53 mit Verweis auf BVerfGE 49, 24 (53); 39, 1 (42); 46, 160 (164); 53, 30 (57)
711 *Götz,* in: *Isensee*/*Kirchof*, HStR IV 2006, § 85 Rn. 24.
712 Vgl. Fn. 709.
713 *Hopfauf*, in: *Schmidt-Bleibtreu/Klein*, GG 2011, Einl., Rn. 142.

Kontrollbefugnis im Hinblick auf das Untermaßverbot.[714] Dieses wird als „schutzpflichtspezifische Ausprägung des Verhältnismäßigkeitsprinzips" verstanden.[715] Der Staat ist insofern nicht verpflichtet, das optimale oder höchst mögliche Maß an Sicherheit zu gewähren, sondern grundsätzlich nur das, was er für angemessen erachtet.

Doch auch aus dem Schutzpflichtengedanken lässt sich eine subjektive Komponente der Staatsaufgabe Sicherheit herleiten.[716] Allerdings besteht hier ein Anspruch erst dann, wenn der Staat das Untermaßverbot verletzen sollte.[717] Darin liegt der wesentliche Unterschied zwischen der primären abwehrrechtlichen Dimension der Grundrechte und ihrer Schutzpflichten-Dimension. Während Grundrechte als subjektive Rechte voll gerichtlich nachprüfbar sind, ist das Einschreiten des Staates bis zur Grenze des Untermaßverbots nicht einklagbar.[718]

Die Grundrechte verlangen also auch nach Schutz durch den Staat und verpflichten so den Staat zur Gewährleistung von Sicherheit, wobei Exekutive wie Legislative bei der Wahrnehmung dieser Aufgabe einen weiten Gestaltungsspielraum innehaben.

In Bezug auf die Lebens- und Gesundheitsgefahren der Kernenergie stellt das *Bundesverfassungsgericht* zutreffend fest, angesichts der Art und Schwere der Gefahr müsse bereits die entfernte Wahrscheinlichkeit des Eintritts genügen, um die Schutzpflicht des Staates konkret auszulösen. Es müsse „praktisch" ausgeschlossen sein, dass sich die Risiken der Kernenergie verwirklichen.[719]

Fraglich ist, ob dies entsprechend für die Bedrohung durch den internationalen Terrorismus gilt, denn auch hier drohen besonders schwere Unglücksfälle und eine Gefährdung für das Leben zahlreicher Menschen. Anders als bei den Risiken der Kernenergie handelt es sich bei der Bedrohung durch den internationalen Terrorismus nicht um ein technisches, naturwissenschaftlich beleg- und berechenbares Risiko, sondern um eine Bedrohung, die von Menschen ausgeht. Ob und wie hoch die Bedrohung ist, kann nicht naturwissenschaftlich überprüft werden, sondern obliegt im Ergebnis der Einschätzung von Nachrichtendiensten, Polizei und Innenministerien. Insofern unterscheidet sich die Tatsachen-Grundlage beider Gefährdungen bereits. Zwar haben beide Gefährdungen gemein, dass sie für eine Vielzahl von Menschen, für die Umwelt und für den Staat (lebens-)bedrohlich sein können. Der Unterschied zwischen den Risiken durch terroristische Anschläge und den Gefährdungen durch die Nutzung der Kernenergie besteht zunächst darin, dass die Entscheidung für die Atomenergie eine Entscheidung des Staates ist. Er provoziert also das Risiko und muss entsprechend dafür sorgen, dass dieses möglichst gering ist. Die Bedrohung durch den internationalen Terrorismus, kommt hingegen von außen. Seine Entstehung hat soziale, kulturelle und religiöse Ursachen und ist nicht ursächlich durch ein Verhalten/ eine Entscheidung des

---

[714] BVerfGE 77, 170 (214); 79, 174 (202); 88, 203 (251ff.); 92, 26 (46); 96, 56 (64); 115, 118 (159f.).
[715] *Götz,* in: *Isensee*/*Kirchof*, HStR IV 2006, § 85 Rn. 30; *Möstl* 2002, 103.
[716] *Thiel* 2011, 154.
[717] Zum Untermaßverbot vgl. die Ausführungen in Fn. 641; Nachweise aus der Rspr des *BVerfG* in Fn. 714
[718] *Hopfauf*, in: *Schmidt-Bleibtreu/Klein*, GG 2011, Einl., Rn. 142.
[719] *BVerfGE* 49, 89, 135 ff.; so auch *Roßnagel* 1984, 53.

Staates entstanden. So gibt es auch diverse Anknüpfungspunkte zur Verhinderung und Bekämpfung von Terrorismus. Allerdings besteht keine Einigkeit in der Frage wie Terrorismus effektiv bekämpft und seine Entstehung verhindert werden kann. Zudem macht die Entwicklung des internationalen Terrorismus gerade nicht an Landesgrenzen Halt. Dennoch ist Knackpunkt, dass die Verursachung der Gefährdung durch nukleare Katastrophen durch die Entscheidung für die friedliche Nutzung der Atomenergie in die Verantwortlichkeit des Staates fällt. Daher werden Schutzpflichten hier unmittelbar ausgelöst. Die Gefährdung durch den internationalen Terrorismus kommt hingegen von außen und ist auf Grund der Intensität der Gefährdung geeignet ebenfalls Schutzpflichten auszulösen. Allerdings kann hier keine entfernte Wahrscheinlichkeit genügen, um konkrete Eingriffe zu rechtfertigen. Auch wenn keine konkrete Gefahr in Anbetracht des hohen Gefährdungsrisikos verlangt werden kann, müssen sich doch zumindest die Anhaltspunkte für das Entstehen einer konkreten Gefahr verdichtet haben.

2.2.3 Grundrecht auf Sicherheit?

Maßgeblich von *Isensee* geprägt ist die Ansicht, dass, auch wenn nicht ausdrücklich normiert, die Verfassung ein Grundrecht auf Sicherheit gewähre.[720] Die negative und die positive Funktion der Grundrechte hätten den gleichen verfassungsrechtlichen Rang. Dogmatisch sei so aus der Gesamtheit der Schutzaspekte ein „Grundrecht auf Sicherheit" ableitbar − wobei dies mit der durch das *Bundesverfassungsgericht* anerkannten Kategorie der grundrechtlichen Schutzpflichten weitgehend übereinstimme.[721] Es gehe jedoch insoweit über diese hinaus, als es die Perspektive des Bürgers ins Zentrum stelle und aus dieser heraus unmittelbar ein Anspruch ableitet.[722]

Das Grundrecht sei zwar im Wesentlichen „gesetzesmediatisiert",[723] darüber hinaus bilde es aber „den verfassungsrechtlichen Magnet, der die über verschiedene Rechtsgebiete verstreuten Späne der sicherheitsrelevanten Regelungen in sein Feld zieht und ordnet".[724]

Die Ansicht *Isensee* hat sich nicht durchgesetzt.[725] Zu Recht wird betont, was er verkennt, nämlich dass die Grundrechte primär abwehrrechtliche Funktion haben. Durch

---

[720] Grundlegend *Isensee* 1983; so auch *Robbers* 1987, 28 f.; unklar *Aulehner* 1998, 442 ff.; 448, der zwar mit dem „Grundrecht auf Sicherheit" als Gegenpol zum Recht auf informationelle Selbstbestimmung argumentiert, sich aber nicht festlegen möchte ob es im rechtstechnischen Sinne ein Grundrecht auf Sicherheit gibt; umfassend zur Konzeption des Grundrechts auf Sicherheit *Thiel* 2011, 154 ff. in Fn. 105 mit zahlreichen Nachweisen über die Gefolgschaft dieser Lehre im Schrifttum.

[721] Zu unterscheiden sei dies vom status-negativus-Grundrecht der Freiheit der Person.

[722] *Isensee* 1983, 33 ff.

[723] Das heißt, es gelte vorwiegend nach Maßgabe der Gesetze.

[724] *Isensee* 1983, 44.

[725] Kritisch etwa *Denninger* 1990, 33, 47 f., 57, 377; *Hassemer*, vorgänge 2002(Nr. 159), 10 ff.; *Kniesel*, ZRP 1996, 482, 486; *Petri*, RDV 2003, 16, 17 meint die Anerkennung eines Grundrechts auf Sicherheit bedeuten würde, „Dass Sicherheit Freiheit bedeutet"; *Gusy* 2009, Rn. 74 meint, dass „Weder dem Grundgesetz noch dem Unionsrecht lässt sich „die" Staatsaufgabe Sicherheit entnehmen", wohl aber enthielten beide eine Vielzahl von Normen, welche die „Wahrnehmung zahlreicher staatlicher Sicherheitsaufgaben dirigieren, organisieren und limitieren können".

die Annahme eines Grundrechts auf Sicherheit wird das Verhältnis von Freiheitsgewähr und Einschränkung dieser zu Gunsten der Sicherheit verkehrt: Die Folge wäre, dass der Staat den Freiheitseingriff nicht mehr rechtfertigen muss, sondern der Bürger seine Freiheitsausübung rechtfertigen müsste.[726]

Zudem ist problematisch, dass schon Sicherheit ein vager und relativer Begriff ist. Absolute Sicherheit ist nicht realisierbar. Daher ist *Sicherheit* ein Hang zur Maßlosigkeit immanent – sie ist ein „nie erfüllbares Ideal".[727] Ein Grundrecht auf Sicherheit anzuerkennen, entspricht damit einem nicht erfüllbaren Versprechen.

Insofern ist es auch nicht richtig, dass das Grundrecht auf Sicherheit durch die Gesetze mediatisiert wird, sondern es gibt zahlreiche Gesetze, die der Umsetzung der Staatsaufgabe Sicherheit dienen.[728]

Schließlich sprechen auch historische Gesichtspunkte gegen die Annahme eines Grundrechts auf Sicherheit. Zwar sollte im Grundgesetz ursprünglich ein Recht auf Sicherheit niedergelegt werden, dies wurde aber vom Redaktionsausschuss des Parlamentarischen Rates abgelehnt mit der Begründung, dass ein Recht auf Sicherheit „doch nur Ausfluss der persönlichen Freiheit" sein könne.[729]

Art. 6 EU-GRCh. und Art. 5 EMRK gewähren ein Recht auf Freiheit und Sicherheit. Dabei schützt das garantierte Recht auf Sicherheit allein die Sicherheit vor (willkürlichem) Freiheitsentzug.[730] Der *Europäische Gerichtshof für Menschenrechte* hat in seiner Rechtsprechung darüber hinaus dem Recht auf Sicherheit keine eigenständige Bedeutung zuerkannt. Es gibt insofern auf europäischer Ebene trotz der scheinbar ausdrücklichen Nennung eines Rechts auf Sicherheit, kein mit der Konstruktion *Isensees* vergleichbares Grundrecht auf Sicherheit.

2.2.4 Sicherheit als legitimes Eingriffsziel

Das *Bundesverfassungsgericht* hat wiederholt festgestellt, dass die Sicherheit des Staates als verfasste Friedens- und Ordnungsmacht und die von ihm zu gewährleistende Sicherheit der Bevölkerung vor Gefahren für Leib, Leben und Freiheit Verfassungswerte sind, „die mit anderen hochwertigen Gütern im gleichen Rang stehen".[731] Sicherheit sei ein legitimer Zweck, um grundsätzlich einen Eingriff in Grundrechte zu rechtfertigen.[732] Die Schutzgüter der öffentlichen Sicherheit und Ordnung besäßen ein hohes verfassungsrechtliches Gewicht. „Das Gewicht des jeweils konkret verfolgten Einsatzzwecks hängt allerdings davon ab, auf welche beeinträchtigten Rechtsgüter er sich konkret bezieht und welche Intensität deren Gefährdung aufweist."[733] Die Siche-

---

[726] So *Brugger*/*Gusy*, VVDStRL 2004, 151, 168 ff.
[727] *Thiel* 2011, 157.
[728] Insofern kann ein „Grundrecht auf Sicherheit" maximal „als Sammelbezeichnung für die verschiedenen Ausprägungen eines subjektiven Rechts auf Schutz gebraucht werden", *Thiel* 2011, 158
[729] *Bull* 1977, 348, Fn. 9 ff.
[730] *Frenz* 2009, Rn. 1070; Allein Art. 9 IPvpR enthält ein Recht gegen den Staat auf Schutz vor Angriffen, BGBl. 1973 II, 1534.
[731] BVerfGE 120, 274 (319) mit Verweis auf BVerfGE 49, 24 (56 f.); 115, 320 (346).
[732] BVerfGE 100, 313 (373, 383f.); 107, 299 (316); 109, 279 (336); 115, 320 (345); 125, 260 (316f.).
[733] BVerfGE 120, 378 (427).

rung des Rechtsfriedens an sich, habe dabei „ein eigenständiges Gewicht“.[734] „Das *Bundesverfassungsgericht* hat wiederholt die unabweisbaren Bedürfnisse einer wirksamen Strafverfolgung und Verbrechensbekämpfung hervorgehoben, das öffentliche Interesse an einer möglichst vollständigen Wahrheitsermittlung im Strafverfahren − zur Überführung von Straftätern ebenso wie zur Entlastung Unschuldiger − betont und die wirksame Aufklärung gerade schwerer Straftaten als einen wesentlichen Auftrag eines rechtsstaatlichen Gemeinwesens bezeichnet:“[735] Mit dem Ziel Sicherheit zu erzeugen, können Grundrechtseingriffe also grundsätzlich gerechtfertigt werden. Dabei wird vom *Bundesverfassungsgericht* akzeptiert, dass der Gesetzgeber auf veränderte gesellschaftliche Bedingungen mit neuen Instrumenten reagiert.[736]

Die Gewährleistung der inneren Sicherheit zielt nach weitverbreiteter Ansicht auf den „Schutz der Unversehrtheit des jeweils vorhandenen Bestandes individueller und überindividueller Rechte und Güter, den Bestand, die Unversehrtheit und Funktionsfähigkeit der Organe und Einrichtungen des Staates eingeschlossen“.[737] Als Kernaufgabe der Gewährleistung innerer Sicherheit wird die Bekämpfung der Kriminalität gesehen.[738] Über die Verbrechensbekämpfung durch Polizei und Justiz hinaus werden zur inneren Sicherheit die sicherheitspolizeilich eingestuften Aufgaben des Melde-, Pass-, Ausländer, Vereins- und Versammlungswesens, alle vollzugspolizeilichen Aufgaben, die Aufgaben des Verfassungsschutzes und der Nachrichtendienste und die des Katastrophenschutzes gezählt.[739]

In Art. 74 Nr. 1 GG, mittelbar Art. 104 GG und angedeutet in Art. 73 Nr. 10 GG werden zumindest die Aufgaben Strafrecht und Strafvollzug erwähnt.[740]

Bei der Zielsetzung Sicherheit im Inneren zu erzeugen, kann unterschieden werden zwischen der Sicherheit von Personen und Sachen und der Sicherheit von Zuständen wie sie sich in den polizeirechtlichen Begriffen „öffentliche Sicherheit“ und „öffentliche Ordnung“ wiederspiegeln.[741] Der Staat schützt zum einen die persönliche Integri-

---

734 BVerfGE 113, 348 (385); 107, 104 (118).

735 BVerfGE 109, 279 (336) verweist auf BVerfGE 77, 65 (76); 80, 367 (375); 100, 313 (389); 107, 299 (316).

736 So etwa im Urteil zur Vorratsdatenspeicherung. Als Reaktion auf das spezifische Gefahrenpotenzial der Telekommunikation müsse auch eine Speicherung der Telekommunikationsverkehrsdaten auf Vorrat akzeptiert werden. Denn die Telekommunikation erleichtere eine verdeckte Kommunikation von Straftätern und ermögliche es so auch verstreuten Gruppen von wenigen Personen, sich zusammenzufinden und effektiv zusammenzuarbeiten. , BVerfGE 125, 260 (317). Neue Herausforderungen bestünden insbesondere aus dem Grund, dass „mangels öffentlicher Wahrnehmbarkeit“ es an einem „gesellschaftlichen Gedächtnis“ fehle, so dass es nicht möglich sei, wie in anderen Bereichen, „zurückliegende Vorgänge auf der Grundlage zufälliger Erinnerung zu rekonstruieren“, BVerfGE 125, 260 (323). Zur Bedeutung von Telekommunikationsverkehrsdaten für die Arbeit der Ermittlungsbehörden, ausführlich unten Kap. 4.4.2.

737 *Götz,* in: *Isensee*/*Kirchof*, HStR IV 2006, § 85 Rn. 1.

738 *Götz,* in: *Isensee*/*Kirchof*, HStR IV 2006, § 85 Rn. 5.

739 *Götz,* in: *Isensee*/*Kirchof*, HStR IV 2006, § 85 Rn. 6.

740 *Bull* 1977, 349.

741 *Bull* 1977, 348.

tät des Einzelnen, die Rechtsordnung im Übrigen als auch sich selbst – also den Staat und seine Einrichtungen.[742]

Es wird vertreten, dass das Staatsziel innere Sicherheit im wesentlichen Prävention sei.[743] Die Zuordnung der Präventivfunktion von Strafgesetz, Strafrechtspflege und Strafe zu dem Staatsziel der inneren Sicherheit sei unausweichlich, da das moderne Strafrecht vom den Ziel der Verbrechensvorbeugung beherrscht sei.[744] Dem Grunde nach ist dem zuzustimmen, denn schließlich prägt der Präventionsgedanke im Sinne einer Spezial- und Generalprävention auch das Strafrechtssystem. Allerdings ist zu betonen, dass zwar Prävention dem Schutzgedanken immanent ist, dieser aber keineswegs eine grenzenlose Prävention fordert. Die Verfassung verlangt nicht die Gewährleistung einer hundertprozentigen Sicherheit.

2.2.5 Sicherheitsarchitektur des Grundgesetzes

Dass das Grundgesetz eine Staatsaufgabe Sicherheit voraussetzt, belegt schließlich die im Grundgesetz staatsorganisationsrechtlich angelegte Sicherheitsarchitektur. Nachrichtendienste, Polizei und Streitkräfte werden insbesondere im Rahmen kompetenzrechtlicher Zuweisungen genannt. So hat der Bund gem. Art. 73 Abs. 1 Nr. 9a GG die ausschließliche Gesetzgebungskompetenz zur „Abwehr von Gefahren des internationalen Terrorismus durch das Bundeskriminalpolizeiamt in Fällen, in denen eine länderübergreifende Gefahr vorliegt, die Zuständigkeit einer Landespolizeibehörde nicht erkennbar ist oder die oberste Landesbehörde um eine Übernahme ersucht“ und gemäß Nr. 10 für die Zusammenarbeit von Bund und Ländern in der Kriminalpolizei, dem Verfassungsschutz und „zum Schutze gegen Bestrebungen im Bundesgebiet, die durch Anwendung von Gewalt oder darauf gerichtete Vorbereitungshandlungen auswärtige Belange der Bundesrepublik Deutschland gefährden“ sowie schließlich für die Einrichtung eines Bundeskriminalpolizeiamtes und für die internationale Verbrechensbekämpfung.

Weitere Regelungen in denen auf die Polizei Bezug genommen wird finden sich in Art. 91 Abs. 1 und 2 S 1 und Art. 104 Abs. 2 S. 2 GG. Da sich keine ausdrückliche Kompetenzregelung für das Polizeirecht im Grundgesetz findet, ist dies Ländersache (Art. 70 Abs. 1 GG). Die Polizeihoheit der Länder prägt ganz generell die Sicherheitsarchitektur der Bundesrepublik.[745] Trotz vorhandener Vielfalt der Polizeiorganisationen in den einzelnen Bundesländern hat sie eine gemeinsame Struktur: So gibt es in Deutschland, anders als in vielen anderen Staaten, eine Einheitspolizei und nicht mehrere verschiedene „Polizeien“.[746]

Aufgabe der allgemeinen Polizeibehörden ist zunächst die Abwehr von Gefahren für die öffentliche Sicherheit und Ordnung. Daneben wird sie repressiv zur Verfolgung von Straftaten und Ordnungswidrigkeiten tätig. Zwar ist die Strafverfolgung originäre Aufgabe der Staatsanwaltschaften, da diese aber über kein eigenes Ermittlungsperso-

[742] Zum Schutz des Staates und seiner Einrichtungen, ausführlich *Bull* 1977, 354f.
[743] *Götz,* in: *Isensee*/*Kirchof*, HStR IV 2006, § 85 Rn. 14.
[744] *Götz,* in: *Isensee*/*Kirchof*, HStR IV 2006, § 85 Rn. 14.
[745] *Götz,* in: *Isensee*/*Kirchof*, HStR IV 2006, § 85 Rn. 33.
[746] *Götz,* in: *Isensee*/*Kirchof*, HStR IV 2006, § 85 Rn. 33.

nal verfügen, wird die Polizei als „Hilfspersonal“ für die Staatsanwaltschaft tätig. Für strafrechtliche Ermittlungen gilt grundsätzlich das Legalitätsprinzip gemäß §§ 152 StPO und 386 AO. Das heißt wenn ein Verdacht einer Straftat besteht, muss, auch wenn weder Anzeige oder Antrag gestellt wurden, ermittelt werden. Damit soll sichergestellt werden, dass nicht willkürlich ermittelt wird, sondern Gleichheit vor dem Gesetz besteht.

Neben den Landespolizeibehörden gibt es auf Bundesebene die Bundespolizei.[747] Diese ist zuständig für den grenzpolizeilichen Schutz des Bundesgebietes, dabei auch für die Bekämpfung der grenzüberschreitenden Kriminalität, für die Gefahrenabwehr und Sicherheit im Bereich der Bahnanlagen des Bundes, für Luftsicherheitsaufgaben und schließlich für den Schutz von Bundesorganen. Daneben gibt es das Bundeskriminalamt,[748] welches die nationale Verbrechensbekämpfung in Zusammenarbeit mit den Landeskriminalämtern koordiniert und leitend in bestimmten Kriminalfeldern mit Auslandsbezug die Ermittlungen durchführt. Es hat darüber hinaus die Aufgabe die Mitglieder der Verfassungsorgane des Bundes zu schützen. Schließlich dient es bei Interpol als nationales Zentralbüro (NZB). Die Kompetenz des Bundes zur Errichtung von Bundespolizei und Bundesgrenzschutz findet sich in Art. 87 Abs. 1 GG, indem auch die Ermächtigung zur Einrichtung eines Verfassungsschutzes normiert ist.

Die Verfassungsschutzbehörden gehören zu den Nachrichtendiensten. Insgesamt verfügen über nachrichtendienstliche Befugnisse in Deutschland mehrere Behörden.[749] Zu nennen sind zunächst die drei Nachrichtendienste des Bundes, nämlich Bundesnachrichtendienst, der auch Auslandsnachrichtendienst genannt wird,[750] der Inlandsnachrichtendienst mit Namen Bundesamt für Verfassungsschutz[751] und der Militärische Abschirmdienst, der der Bundeswehr angehört.[752] Daneben gibt es in jedem Bundes-

[747] Früher Bundesgrenzschutz. Die Namensänderung erfolgte mit Gesetz zur Umbenennung des Bundesgrenzschutzes in Bundespolizei v. 21.6.2005 (BGBl I, 1818).

[748] Kompetenz zur Errichtung des BKA aus Art. 73 Nr. 10 GG.

[749] Zu nennen sind der BVerfSch und die jeweiligen Landesbehörden; BND; MAD; BSI; Zentrum für Nachrichtenwesen der Bundeswehr; Kommando Strategische Aufklärung; und das Das Gemeinsame Terrorismus Abwehrzentrum.

[750] Aufgabe ist die Informationssammlung und Auswertung zur Gewinnung von Erkenntnissen über das Ausland, die von außen- und sicherheitspolitischer Bedeutung sind, § 1 II S. 1 BNDG.

[751] Aufgabe ist im Wesentlichen die Sammlung und Auswertung von Informationen über Bestrebungen gegen die freiheitliche demokratische Grundordnung, den Bestand oder die Sicherheit des Bundes/ eines Landes oder Beeinträchtigung der Verfassungsorgane; sowie sicherheitsgefährdende oder geheimdienstliche Tätigkeiten im Geltungsbereich dieses Gesetzes für eine fremde Macht, § 3 Abs.1 BVerfSchG.

[752] § 1 Abs. 1 S. 1 MADG beschreibt als primäre Aufgabe die Sammlung und Auswertung von Informationen über Bestrebungen gegen die freiheitliche demokratische Grundordnung, den Bestand oder die Sicherheit des Bundes/ eines Landes, oder sicherheitsgefährdende oder geheimdienstliche Tätigkeiten im Geltungsbereich dieses Gesetzes für eine fremde Macht, wenn gegen Bundesministeriums der Verteidigung gerichtet und von ihm angehörigen Personen ausgehend. Nur ausnahmsweise besteht gemäß § 2 MADG eine Zuständigkeit für Personen außerhalb des Ministeriums, nämlich zum Schutz des Ministeriums.

land als lokale Inlandsnachrichtendienste Verfassungsschutzbehörden der Länder.[753] Den verschiedenen nachrichtendienstlichen Behörden sind jeweils spezifische Aufgaben zugewiesen.[754] Nachrichtendienste haben in der Bundesrepublik grundsätzlich keine polizeilichen Befugnisse, sondern müssen im gegebenen Fall eine andere Behörden um Amtshilfe ersuchen.[755]

Als drittes Element neben Polizei und Nachrichtendiensten in der Sicherheitsarchitektur ist die Bundeswehr zu nennen. Art. 87a GG, der den Bund ermächtigt Streitkräfte zur Verteidigung aufzustellen, wurde erst nachträglich mit der Wehrnovelle 1956 in das Grundgesetz eingeführt.[756] Ein Einsatz im Inneren ist gemäß Art. 87a Abs. 2 GG nur zulässig, soweit dies das Grundgesetz ausdrücklich vorsieht. Was allein in Art. 35 Abs. 2, 3 GG der Fall ist. Dieser ermächtigt dazu Streitkräfte zur Unterstützung der Polizeikräfte im Fall von Naturkatastrophen oder eines Unglücksfalles im Inneren einzusetzen. Das Militär darf dabei allerdings nur zur Unterstützung der Polizei und wie Polizeikräfte eingesetzt werden. Ein militärischer Waffeneinsatz ist daher im Fall eines Katastropheneinsatzes der Bundeswehr unzulässig.[757]

Polizei, Nachrichtendienste und Streitkräfte sind als Organisationseinheiten mit der Aufgabe Sicherheit und Ordnung herzustellen betraut. Sie bilden dabei „keine Funktionseinheit".[758] Vielmehr zeigen schon die kompetenzrechtlichen Bestimmungen und Nennungen der drei Sicherheitsbehörden, dass zwischen den Aufgaben und Kompetenzen von Militär, Polizei und Nachrichtendiensten strikt getrennt wird. Diese strikte Trennung zwischen den Aufgaben insbesondere von Polizei und Nachrichtendiensten ist schließlich historisch begründet und dient dazu die Macht der einzelnen Behörden zu begrenzen (sog. Trennungsgebot).[759]

---

[753] Daneben haben im zivilen Bereich auch das Bundesamt für Sicherheit in der Informationstechnik (BSI) sowie das Informations- und Kommunikationstechnikzentrum (IKTZ) der Bundespolizei nachrichtendienstliche Aufgaben.

[754] Diese sind jeweils überblicksartig dargestellt in Fn. 750, 751, 752.

[755] § 3 II S. 1 BNDG; § 8 Abs. 3 BVerfSchG; § 4 II MADG. Sie haben auch keine Weisungsbefugnisse. Amtshilfeersuchen sind nur zulässig, soweit sie selbst zu den Maßnahmen befugt sind. Ausführlich zum Trennungsgebot, unten S. 331; zur Aufweichung des Trennungsgebot im Rahmen der Sicherheitsstrategie, oben S. 68 ff.

[756] BGBl. 1956 I, 111. Er wurde mit der sog. Notstandsverfassung (17. Gesetz zur Ergänzung des GG v. 24.6.1968 (BGBl. 1968 I, 709)) neu gefasst.

[757] So BVerfGE 115, 118 (118, LS. 2); dazu kritisch *Götz,* in: *Isensee*/*Kirchof*, HStR IV 2006, § 85 Rn. 32.

[758] *Pieroth/Schlink/Kniesel* 2012, § 2, Rn. 2 Funktionseinheit meint, dass um der gemeinsamen Funktion willen Befugnisse, Daten und Informationen einer Behörde auch in den Dienst der Aufgabe einer anderen Behörde gestellt werden können. Dann könnten aus der Aufgabe auf Befugnisse geschlossen werden, die so nicht ausdrücklich normiert sind. Dieser Schluss ist aber eine Folgerungsweise des Polizeistaats, die mit dem Rechtsstaats nicht in Einklang steht. Daher ergibt sich die Antwort darauf, wie viel Kooperation zulässig ist, allein aus dem Gesetz und nicht aus einer angenommen Funktionseinheit. Dies gilt auch trotz der Erweiterung des Sicherheitsbegriffs.

[759] Die historische Begründung des Trennungsgebots stellt ausführlich *Klee* 2010, 21 ff. dar. Zum Trennungsgebot auch noch ausführlich unten Kap. 9.3.2.3.

2.2.6 Europarechtliche Begründung der staatlichen Pflicht zur Gewährleistung von Sicherheit

Das ausdrücklich formulierte Recht auf Sicherheit in Art. 5 EMRK und Art. 6 EU-GRCh., begründet keine Pflicht zur Gewährleistung von Sicherheit durch Strafverfolgung und Gefahrenabwehr. Es wurde bereits dargelegt, dass sich dieses Recht allein darauf beschränkt die Sicherheit zu gewähren, nicht willkürlich verhaftet zu werden. Es ist insofern ein unmittelbar freiheitsicherndes Recht.[760]

Doch auch die Europäischen Grundrechte verpflichten zur Gewährleistung von innerer (und äußerer) Sicherheit. So ist eine Schutzpflichtdimension für das Recht auf Leben aus Art. 2 Abs. 1 EMRK und Art. 2 Abs. 1 EU-GRCh. anerkannt.[761] Der Staat wird durch diese beispielsweise verpflichtet, effektive Verfahren zu schaffen, um die Durchsetzung der Sanktionen zu ermöglichen.[762] Zum anderen muss der Staat unter bestimmten Umständen auch vorbeugend tätig werden, um das Leben eines Menschen zu schützen. Dies ist allerdings nur der Fall, wenn konkrete Anhaltspunkte einer „wirklichen und unmittelbaren Gefahr" vorliegen, die von Behörden erkannt wurde oder erkannt hätte werden müssen.[763] Insgesamt belassen Art. 2 Abs. 1 EMRK und Art. 2 Abs. 1 EU-GRCh. dem Staat einen weiten Gestaltungsspielraum bei der Auswahl der Mittel zum Schutz des Lebens.

2.2.7 „Der Staat als Beschützer der Bürger"

Die Analyse der grundrechtlichen Vorgaben zeigt, dass es zwar kein Grundrecht auf Sicherheit gibt, das Grundgesetz den Staat aber nichtsdestotrotz zur Gewährleistung von Sicherheit verpflichtet.[764] Dies jedoch nicht zum bloßen Selbstzweck, sondern – und dies wird insbesondere deutlich, wenn man mit dem *Bundesverfassungsgericht* die Begründung der Staatsaufgabe Sicherheit aus der Schutzfunktion der Grundrechte herleitet[765] – um es dem Einzelnen zu ermöglichen seine Freiheitsrechte auszuüben. Die Feststellung, dass der Staat als Kehrseite der Grundrechte verpflichtet ist Sicherheit zu gewährleisten, ändert allerdings nichts an der Tatsache, dass den Grundrechten primär eine abwehrrechtliche Funktion im Sinne eines Schutzes vor dem Staat zukommt. Die Schutzpflichtendimension der Grundrechte ist der abwehrrechtlichen Funktion nachgeordnet. Auch enthält das Grundgesetz nicht nur den Sicherheitsauftrag, sondern auch „Organisationsnormen sowie inhaltliche Maßstäbe und Grenzen für dessen Wahrnehmung".[766]

Die Staatsaufgabe Sicherheit umfasst nicht die Pflicht eine maximale oder gar eine absolute[767] Sicherheit zu erstellen.[768] Vielmehr ist sie darauf beschränkt konkrete Gefah-

---

[760] Dazu oben Kap. 2.2.3.
[761] *Frenz* 2009, Rn. 1076.
[762] *Schädler,* in: KarlsruherKomm StPO, Art. 8 EMRK Rn. 10 ff.
[763] *EGMR* Urt. v. 24.10.2002 - 37703/97, NJW 2003, 3259, 3260.
[764] *Roßnagel*, Informatik-Spektrum 2002, 33, 34.
[765] Zahlreiche Nachweise in Fn. 751.
[766] *Gusy* 2009, Rn. 73.
[767] Selbst *Isensee* erkennt, dass es totale Sicherheit nie geben wird: „Totale Sicherheit wird allenfalls im totalen Staat angestrebt; aber noch nicht einmal er kann sie erreichen. Der freiheitliche Staat hat weder die Macht noch das Recht, in allen privaten und gesellschaftlichen erreichen präsent zu sein,

ren von Rechtsgütern abzuwehren und einen Schutz gegen abstrakte Gefahren, die von erheblichem Gewicht sind, zu gewähren. Die Sicherheitsgewährleistung ist dennoch nicht nur objektiv bestehende Staatsaufgabe, sondern beinhaltet auch einen subjektivrechtlichen Kern.[769]

Der Staat ist Beschützer der Bürger.[770]

2.3 Freiheit und Sicherheit in einem natürlichen Spannungsverhältnis

Die verfassungsrechtliche Analyse hat gezeigt, dass das Grundgesetz sowohl Freiheit als auch Sicherheit gewährt. Es handelt sich dabei um keine Antinomie.[771] Vielmehr stehen Freiheit und Sicherheit in einem Komplementärverhältnis zueinander:[772] Es gibt keine Freiheit ohne Sicherheit, aber auch Sicherheit ohne Freiheit wäre unerträglich.[773] „Freiheit braucht Sicherheit und Sicherheit braucht Freiheit".[774] Freiheit und Sicherheit sind im Grundgesetz nicht als Gegensätze konzipiert, sondern eng miteinander verquickt: sowohl die Pflicht zur Gewährleistung von Freiheit als auch die zur Sicherheit wurzeln beide in den Grundrechten und im Rechtsstaatsprinzip. Sie haben jedoch nicht nur die gleichen Wurzeln, sondern sie beschränken sich auch gegenseitig. In Grundrechte darf und muss unter bestimmten Voraussetzungen, eingegriffen werden, um Sicherheit und Ordnung zu erzielen. Grenzen werden diesem Eingriff jedoch wiederum durch das Bestimmtheitsgebot, den Verhältnismäßigkeitsgrundsatz und schließlich die Menschenwürdegarantie und den Wesensgehalt der Grundrechte gesetzt – also um der Freiheit des Einzelnen oder der Gesellschaft willen. Durch das Verbot unverhältnismäßiger Grundrechtseingriffe werden die staatlichen Schutzpflichten begrenzt.[775] Die Zielsetzung, absolute Sicherheit zu erzeugen, ist damit ausgeschlossen.[776]

Der Spielraum bei der Erfüllung des Sicherheitsaufgabe wird durch zwei Grenzen markiert: auf der einen Seite „dem Staat schlechthin verschlossenen Mittel" auf der

---

um bei jeder möglichen Gefahr bereitzustehen." *Isensee* 1983, 41. Führt im Folgenden aus, dass es Aufgabe des Gesetzgebers sei die widerstreitenden Prinzipien zum Ausgleich zu bringen und sich keines von ihnen kompromisslos und vollkommen zu Eigen zu machen.

768 *Hopfauf*, in: *Schmidt-Bleibtreu/Klein*, GG 2011, Rn. 145.

769 *Thiel* 2011, 158; dazu ausführlich oben Kap. 2.2.3.

770 Vgl. Fn. 764.

771 „Sicherheit und Freiheit (…) hängen untrennbar zusammen. Sie sind zwei Seiten einer Medaille, verschiedene staatsrechtliche Aspekte derselben Sache: des Lebens, der Freiheit der Person, des Eigentums wie der sonstigen Rechtsgüter. (…) Der Schutz des Staates konstituiert den status positivus des Bürgers, die Rechtswahrung den status negativus. Beide status bilden ein integrales Ganzes. ES gibt daher keine Antinomie zwischen den beiden Rechtswerten. Allenfalls ergibt sich eine Spannung im konkreten Fall, die der Gesetzgeber oder der Gesetzesanwender auszugleichen hat", *Isensee* 1983, 21.

772 *Di Fabio*, NJW 2008, 421, 422; Dass Freiheit und Sicherheit keinen kategorischen Gegensatz aufweisen betont auch *Thiel* 2011, 180 ff.; in diesem Sinne auch *Bull* 2011, 20.

773 *Hopfauf,* in: *Schmidt-Bleibtreu/Klein*, GG 2011, Einl., Rn. 145.

774 *Gusy*, VerwArch 2010, 309, 331.

775 *Hopfauf*, in: *Schmidt-Bleibtreu/Klein*, GG 2011, Rn. 145.

776 *Hopfauf*, in: *Schmidt-Bleibtreu/Klein*, GG 2011, Rn. 145.

anderen „die unabweisbare, zwingende Notwendigkeit des Einschreitens zum Schutz bedrohter Individualrechte und -güter“ („Untermaßverbot“).[777]

Auch wenn Freiheit und Sicherheit als „miteinander verquickt“, als „komplementär“ oder als „zwei Seiten einer Medaille“ beschrieben werden können, ändert dies nichts an der Tatsache, dass im Rahmen von sicherheitspolitischen Entscheidungen, Freiheits- und Sicherheitsinteressen miteinander kollidieren. Freiheit und Sicherheit ergänzen und bedingen sich nicht nur gegenseitig, sondern stehen auch in einem natürlichen Spannungsverhältnis zueinander.[778]

Dieses Spannungsverhältnis tritt aktuell besonders deutlich zu Tage, wie die Ausweitung und Digitalisierung der staatlichen Sicherheitsvorsorge zeigen, wie sie oben beschrieben wurden.[779] Denn durch die zunehmende Betonung des Schutzpflichtencharakters der Grundrechte wird der abwehrrechtliche Charakter vernachlässigt.[780] Dies ist der Hintergrund der Frage, ob die zu beobachtenden Entwicklungen hin zu mehr Sicherheit noch mit der verfassungsrechtlichen Ordnung konform gehen. Bevor jedoch diese Frage beantwortet werden kann, ist zu untersuchen, ob und wenn ja welche Regeln dem Grundgesetz zur Auflösung von Kollisionsfällen von Freiheits- und Sicherheitsinteressen entnommen werden können.

---

[777] *Götz,* in: *Isensee*/*Kirchof*, HStR IV 2006, § 85 Rn. 28.

[778] *Hassemer*, vorgänge 2002, (Nr. 159), 10; „Die Zielwerte stehen in einem prekären Verhältnis zueinander. Wird einer absolut gesetzt, verkümmern die anderen. Nicht Maximierung des einen auf Kosten des anderen ist der Königsweg, sondern wechselseitige Optimierung durch Balancierung.“ So *Hoffmann-Riem* 2009, 57.

[779] Kap. 1.4.2; *Hassemer*, vorgänge 2002, (Nr. 159), 10, 11: “Im Spannungsverhältnis von Freiheit und Sicherheit bewegen wir uns seit geraumer Zeit hin zum Pol der Sicherheit. Das geht zu Lasten der Freiheit.“

[780] So etwa *Denninger,* in: *Huster/Rudolph* 2008, 85, 95 ff.

3 Auflösung des Kollisionsverhältnisses von Freiheits- und Sicherheitsinteressen

Letztlich ist, um das Spannungsverhältnis von Freiheit und Sicherheit aufzulösen, eine Güterabwägung vorzunehmen. Wie dabei die Gewichte zu bestimmen sind, ist umstritten. Es werden im Folgenden die unterschiedlichen Kollisionsregeln, wie sie in der Wissenschaft diskutiert werden, sowie die Argumentation des *Bundesverfassungsgerichts* analysiert. Es soll eine Antwort auf die Frage gefunden werden, wie ein im Sinne der Verfassung bestmöglicher Interessenausgleich aussähe.

3.1 Konzepte zur Auflösung von Kollisionsfällen in der Literatur

Zum Teil wird im rechtswissenschaftlichen Schrifttum betont, dass Sicherheit stets der Möglichkeit der Freiheitsausübung vorgelagert sei, im Sinne eines „ohne Sicherheit keine Freiheit".[781] So betrachtet etwa *Isensee* Freiheit und Sicherheit als zwei Werte, die auf verschiedenen Ebenen lägen. Dabei sei Sicherheit Voraussetzung von Freiheit.[782] Sie sei daher auch Schranke der Freiheit. Die rechtsstaatliche Balance zwischen Freiheit und Sicherheit würde durch Übermaß- und Untermaßverbot erzielt.[783] Soweit ein echtes Kollisionsverhältnis bestünde, gebe ein weiteres Rechtsgut, nämlich „der Geltungsanspruch der Gesamtrechtsordnung" und damit die Sicherheit der Friedensordnung den Ausschlag.[784] Diese Ansicht verkehrt jedoch das Verhältnis von Freiheit und Sicherheit, wie es in der Konzeption der Grundrechte primär als Abwehrrechte (und nicht primär als Schutzpflichten)[785] konstituiert ist in ihr Gegenteil.

Entsprechend wird in der Literatur auch die umgekehrte Vorrangregel vertreten: Freiheit sei tendenziell Vorrang vor Sicherheit einzuräumen – in dubio pro libertate.[786] Diese Maxime hat ihre Wurzeln im Römischen Recht.[787] Als Ausprägung dieser Zweifelsregelung ist im Strafrecht der Grundsatz „im Zweifel für den Angeklagten" anerkannt – und auch in Art. 6 Abs. 2 EMRK normiert. Darüber hinaus ist die These von einem allgemeinen und grundsätzlichen Vorrang der Freiheit vor Sicherheit jedoch abzulehnen. Zwar ist, wie *Merten* aufzeigt, auf Grund des prinzipiellen oder grundsätzlichen Charakters die verfassungsrechtliche Freiheit im Einzelfall wahrscheinlicher als

---

781 In diesem Sinne etwa *Calliess*, ZRP 2002, 1, 7.

782 *Isensee* 2003, 28; Ähnlich auch *Götz,* in: *Isensee*/*Kirchof*, HStR IV 2006, § 85 Rn. 2:„Innerer Sicherheit ist die Voraussetzung für die Ausübung individueller Freiheiten und Rechte". *Di Fabio*, NJW 2008, 421, 422 führt aus, dass erst mit Sicherheit die Freiheit beginne.

783 *Isensee* 2003, 31.

784 *Isensee* 2003, 31 f.

785 Die Schutzpflichten haben ihre Wurzel in dieser primären Funktion, so *Hopfauf,* in: *Schmidt-Bleibtreu/Klein*, GG 2011,Einl., Rn. 145; dazu schon oben Kap. 2.2.2.

786 *Stegner* 2008*,* 151ff.; dazu auch *Thiel* 2011, 180 mit weiteren Nachweisen aus der Literatur, Fn. 247.

787 *Schneider* erläutert, dass in einem Verfahren, das die freie Geburt der schönen Vergenia zum Gegenstand hatte, festgelegt wurde, dass für die Dauer des Freiheitsprozesses der Status libertatis solange beibehalten wurde bis ein Beweis der Unfreiheit erbracht wurde. Dieser Grundsatz gilt im Grunde auch heute entsprechend etwa in Bezug auf die Unterbringung in einer psychiatrischen Klinik, *Schneider*, KritV 1988, 294, 296.

A. Moser-Knierim, *Vorratsdatenspeicherung,* DuD-Fachbeiträge,
DOI 10.1007/978-3-658-04156-4_3, © Springer Fachmedien Wiesbaden 2014

die Unfreiheit. Allerdings könne noch müsse sie deshalb vermutet werden.[788] Er verdeutlicht dies an Hand von Beispielen: Weder sei die Freiheit des Drogenkonsums noch des Kannibalismus im Rahmen der allgemeinen Handlungsfreiheit zu vermuten. Auch bestehe keine uneingeschränkte Freiheitsvermutung des Kernkraftwerksbetreibers. Besonders deutlich werde, dass eine Vermutung für die Freiheit versagt bei Grundrechtskollisionen, etwa wenn die Baufreiheit des einen mit der Eigentumsfreiheit des gestörten Nachbarn kollidiert. Hier hilft eine Vermutung für die Freiheit nicht weiter – denn wessen Freiheit gebührt nun der Vorrang? Zudem spricht gegen eine Regel in dubio pro libertate zur Auflösung von Kollisionsfällen von Freiheits- und Sicherheitsinteressen, dass sich Vermutungen schwerpunktmäßig im Verfahrensrecht zur Regelung von Beweislastfragen finden. Im Bereich der Rechtsfindung besteht hingegen kein Raum für Vermutungen.[789]

Schneider wendet daher in *dubio pro libertate* nur auf Fälle von Tatsachenzweifeln an. Hier greife sie als Abwägungsregel in Fällen des non liquet. Gebunden würden Verwaltung und Gesetzgebung, da Grundrechtseinschränkungen nur zulässig sind, wenn entsprechende tatsächliche Voraussetzungen zweifelsfrei erwiesen sind.[790] Soweit die Maxime allein im abwehrrechtlichen Bereich als Garantieprinzip positioniert würde, erzwinge sie einen Argumentationsprozess, in dem für Eingriff und Einschränkung stärkere Argumente dargelegt werden müssen als für die Nicht-Intervention.[791] Dagegen wird insbesondere angeführt, dass diese Kollisionsregel bei mehrpoligen Rechtsverhältnissen versagt.[792] Die Frage wurde schon aufgeworfen, bei der Kollision der Freiheit des einen mit der Freiheit des anderen (was gerade auch im Bereich des Sicherheitsrechts überwiegend der Fall ist, da Sicherheitsmaßnahmen stets der Freiheitssicherung dienen) bietet die Regel *in dubio pro libertate* keine Antwort wie das Kollisionsverhältnis aufzulösen ist. Grundsätzlich spricht, noch über die dargelegten Argumente hinaus, gegen die Fassung einer Regel eines *in dubio pro libertate*, dass sie dazu verleitet Freiheit und Sicherheit als Gegensätze zu begreifen, anstatt ihre Komplementarität in den Mittelpunkt zu stellen.[793] Daher ist sie jedenfalls als abstrakte Kollisionsregel ebenso wie ein *in dubio pro securitate* abzulehnen.

Zielführender für die Frage wie Kollisionsverhältnisse aufzulösen sind, ist eine Betrachtung der Gemeinsamkeiten von Freiheit und Sicherheit. Es ist der Doppelauftrag, den der Rechtsstaat zu erfüllen hat:[794] „Der rechtsstaatlichen Ordnung ist beides aufgegeben, die Sicherheit und die Freiheit.“[795] *Calliess* sieht daher die Rechtsstaatlichkeit als „staatstheoretischen Kompass“ für die Auflösung von Kollisionsfällen von Freiheits- und Sicherheitsinteressen. Die herausgearbeitete Schnittmenge könne dogmatisch eine Maßstabswirkung dergestalt entfalten, „dass der verfassungsrechtlich ge-

[788] *Merten,* in*:* HGR I, 2006, § 27 Rn. 44.
[789] *Merten,* in: HGR I, 2006, § 27 Rn. 45.
[790] *Schneider* 1960, 291.
[791] *Schneider*, KritV 1988, 294, 304.
[792] *Bethge,* in: *Merten/Papier,* GR II, 2009, § 72, Rn. 83.
[793] *Thiel* 2011, 180 f.
[794] Inwiefern das Rechtsstaatsprinzip Freiheit sichert, Kap. 2.1.4.2; zur rechtsstaatlichen Begründung der Staatsaufgabe Sicherheit, Kap. 2.2.1.
[795] *Horn* 2003, 447.

forderten Abwägung mittels jener aus der Schnittmenge fließenden Vorgaben der Weg gewiesen wird. In einer Situation, in der von Terror und Gewalt erzeugte Angst die Bereitschaft erhöht, Freiheitsrechte gegen − eine tatsächlich ja nicht umfassend zu gewährleistende − Sicherheit einzutauschen, ist verstärkt die (verfassungs-) rechtliche Rationalisierungsfunktion gefordert. Nur mit ihrer Hilfe können jene, im Interesse einer vermeintlichen Sicherheit ergriffenen staatlichen Maßnahmen herausgefiltert werden, die effektiv nicht dem physischen Schutz der Bürger dienen, sondern bestenfalls eine rechtsstaatlich teuer erkaufte Beschwichtigungsfunktion übernehmen".[796] *Calliess* sucht so den Ausgleich mit der Vorstellung zweier sich teilweise überschneidender Kreise zu illustrieren. „Die Staatsaufgabe Sicherheit steht einerseits in einem Spannungsverhältnis zum Rechtsstaatsprinzip, insbesondere zu dessen in den Grundrechten (in ihrer klassischen Abwehrdimension) verkörperten materiellen Gehalt. Andererseits besteht mit Blick auf die Sicherheits- und Schutzdimension des Rechtsstaats eine gemeinsame Schnittmenge, in der Sicherheit und freiheitlicher Rechtsstaat deckungsgleich sind. So gesehen korrespondiert also die Staatsaufgabe Sicherheit in der gemeinsamen Schnittmenge der Schutzfunktion des Rechtsstaats, kollidiert aber gleichzeitig (außerhalb der Schnittmenge) mit der liberalen Abwehrfunktion des Rechtsstaats."[797] Ausgehend von dieser Schnittmenge ließe sich, so *Calliess,* die Abwägung steuern: Die Schnittmenge würde einen Anhaltspunkt dafür liefern, ob im konkreten Fall ein Abwägungsspielraum besteht. Zudem sei sie Maßstab für die Freiheitsverträglichkeit von Sicherheit. Für die Abwägung selbst seien Skalierungen erforderlich, um Bemessen zu können, ob ein Eingriff in die Freiheit von Bürgern leicht, mittel oder schwer wiegt." Dabei gilt − auf einer gleitend gedachten Skala, die sich horizontal durch die beiden Kreise „Sicherheit" und „Rechtsstaat/Freiheit" samt ihrer Schnittmenge zieht − die Regel: Je größer die Nähe des jeweiligen Sicherheitsaspekts zur Schnittmenge ist, desto eher lässt er sich unter rechtsstaatlichen Gesichtspunkten rechtfertigen. Denn je geringer sein Abstand im Kreis „Sicherheit" zur Schnittmenge ist, desto geringer ist auch sein Abstand zur Schnittmenge im Kreis „Rechtsstaat/Freiheit". Wenn sich also ein Sicherheitsaspekt von der Schnittmenge entfernt, dann bedeutet dies auf Grund des in der Schnittmenge zum Ausdruck gekommenen Zusammenhangs auch, dass sich parallel hierzu − freilich in entgegengesetzter Richtung − der Abstand des rechtsstaatlichen Aspekts zur Schnittmenge vergrößert".[798]

Die Betrachtungsweise Calliess überzeugt im Ergebnis, da er keine absolute Vorrangregel konstatiert, wie sie auch dem Grundgesetz nicht entnommen werden kann, sondern die Komplementarität von Freiheit und Sicherheit betont.

[796] *Calliess*, ZRP 2002, 1, 7.
[797] *Calliess*, ZRP 2002, 1, 5 f.
[798] *Calliess*, ZRP 2002, 1, 6; zustimmend: *Thiel* 2011, 182.

3.2 Auflösung des Kollisionsverhältnisses in der Rechtsprechung des BVerfG

Mit dem Verhältnis von Freiheit und Sicherheit befasst sich das *Bundesverfassungsgericht*, wenn es die Verfassungsmäßigkeit von Eingriffen zu Sicherheitszwecken in grundgesetzlich verbürgte Freiheiten prüft.[799] Die Verfolgung von Sicherheitsinteressen (im Wesentlichen zur Strafverfolgung und Gefahrenabwehr) stellt grundsätzlich legitime Ziele dar, die Eingriffe rechtfertigen können.[800] Die Abwägung und insofern die Auflösung des Kollisionsverhältnisses prüft das *Bundesverfassungsgericht* im Rahmen der Prüfung der Verhältnismäßigkeit.

An die Geeignetheit stellt das Gericht keine hohen Anforderungen. Auch bei sicherheitsrechtlichen Instrumenten genügt es nach Ansicht des Verfassungsgerichts, wenn sie abstrakt und auf Grund einer ex ante Betrachtung geeignet sind, die Zweckerreichung zu fördern. Das Regelungsziel muss also nicht tatsächlich erreicht werden.[801] Auch für die Erforderlichkeit genügt es, wenn kein gleich geeignetes, weniger einschneidendes Mittel ersichtlich ist. Soweit nur eine geringfügig geringere Erfolgsaussicht gegeben ist, ist ein Instrument bereits nicht gleich geeignet. Da gerade Instrumente der Sicherheitsvorsorge nach den Maßstäben des *Bundesverfassungsgerichts* wohl nie gänzlich ungeeignet sein werden. Sie zudem je umfassender sie sind auch überwiegend keine gleichermaßen geeigneten Mittel vorstellbar sind, konzentriert sich faktisch die Argumentation, ob ein Sicherheitsinstrument verhältnismäßig ist, auf die Prüfung der Angemessenheit (Verhältnismäßigkeit i.e.S.).[802]

Hier betont das Gericht zunächst, dass bei der Prüfung der Angemessenheit Zurückhaltung geboten ist. Denn so stellt das *Bundesverfassungsgericht* fest, ist es primär die Aufgabe des Gesetzgebers, das „Spannungsverhältnis zwischen der Pflicht des Staates zum Rechtsgüterschutz und dem Interesse des Einzelnen an der Wahrung seiner von der Verfassung verbürgten Rechte“ in „abstrakter Weise einen Ausgleich der widerstreitenden Interessen zu erreichen“.[803] Dabei dürften die Gewichte jedoch „nicht grundlegend verschoben werden.“[804]

Die Auflösung des Kollisionsverhältnisses von Sicherheits- und Freiheitsinteressen obliegt damit in der Regel der Entscheidungsprärogative des Gesetzgebers.

Der Gesetzgeber habe, so das *Bundesverfassungsgericht*, den Auftrag eine „angemessene Balance zwischen Freiheit und Sicherheit herzustellen“. Das schließe „nicht nur die Verfolgung des Ziels absoluter Sicherheit aus, welche ohnehin faktisch kaum, jedenfalls aber nur um den Preis einer Aufhebung der Freiheit zu erreichen wäre“. Sondern auch die „Verfolgung des Ziels, die nach den tatsächlichen Umständen größtmögliche Sicherheit herzustellen“, sei „rechtsstaatlichen Bindungen, zu denen insbesondere das Verbot unangemessener Eingriffe in die Grundrechte als Rechte staatlicher Ein-

[799] BVerfGE 109, 279; 113, 348; 120, 274; 118, 186; 120, 378; 125, 260.
[800] Zahlreiche Nachweise vgl. oben Fn. 732.
[801] Erforderlich ist nach stRspr des *BVerfG* nicht dass das Regelungsziel tatsächlich erreicht wird, BVerfGE 63, 88 (115); 67, 157 (175); 96, 10 (23); 103, 293 (307); 125, 260 (317f.).
[802] Dazu ausführlich noch unten S. 208 ff.
[803] BVerfGE 120, 428 mit Verweis auf BVerfGE 109, 279 (350).
[804] BVerfGE 115, 320 (358).

griffsabwehr zählt“ unterworfen. Dieses Verbot sei es, durch welches den Schutzpflichten des Staates Grenzen gesetzt seien.[805] Denn „die Grundrechte seien primär dazu bestimmt, die Freiheitssphäre des Einzelnen vor Eingriffen der öffentlichen Gewalt zu sichern; sie sind Abwehrrechte des Bürgers gegen den Staat“.[806]

Der Gesetzgeber ist also durch die rechtsstaatlichen Bindungen,[807] absolute Grenzen – wie die Menschenwürdegarantie – sowie Übermaß- und Untermaßverbot in seiner Entscheidungsfreiheit eingeschränkt. Für die Prüfung der Angemessenheit betont das Gericht, dass staatliche Schutzpflichten nicht dazu führen dürften, „dass das Verbot unangemessener Grundrechtseingriffe unter Berufung auf grundrechtliche Schutzpflichten leer läuft, so dass in der Folge allenfalls ungeeignete oder unnötige Eingriffe abgewehrt werden könnten.“[808]

Im Rahmen der Angemessenheit bewertet nun das *Bundesverfassungsgericht* jeweils die Bedeutung der sicherheitspolitischen Maßnahmen und der kollidierenden Freiheitseinschränkung. Es fragt so, welcher Rang den zu schützenden Rechtsgütern beizumessen ist, und setzt dem eine Bewertung des Eingriffsgewichts entgegen.

In der seiner Rechtsprechung hat das *Bundesverfassungsgericht* verschiedene Kriterien für das Eingriffsgewicht in das Telekommunikationsgeheimnis wie auch in das Recht auf informationelle Selbstbestimmung anerkannt. Entscheidend dafür sei die Anzahl der betroffenen Grundrechtsträger (Streubreite der Maßnahme) und ob diese einen Anlass für den Eingriff gegeben haben sowie die Intensität der individuellen Beeinträchtigung.[809] Darüber hinaus kommt es darauf an, welche Inhalte von dem Eingriff erfasst werden und dafür „welchen Grad an Persönlichkeitsrelevanz die betroffenen Informationen je für sich und in ihrer Verknüpfung mit anderen aufweisen“.[810] Auch spiele es eine Rolle, welche belastenden Auswirkungen mit dem Eingriff verknüpft sind. Weiter ist für die Intensität des Eingriffs entscheidend, ob dieser heimlich erfolgt.[811]

Je schwerer der Grundrechtseingriff wiegt, desto höheren Rechtsgütern muss die Maßnahme dienen. Zudem steigen die Anforderungen an die Ausgestaltung der Maßnahme mit dem Eingriffsgewicht.

---

805 BVerfGE 115, 320 (358).

806 BVerfGE 115, 320 (358) „Die Funktion der Grundrechte als objektive Prinzipien und der sich daraus ergebenden Schutzpflichten besteht in der prinzipiellen Verstärkung ihrer Geltungskraft, hat jedoch ihre Wurzel in dieser primären Bedeutung“; vgl. dazu auch BVerfGE 50, 290 (337); 7, 198 (204f.); aiehe auch oben Kap. 2.2.2.

807 Auch „bei der Abwehr von Beeinträchtigungen der Grundlagen einer freiheitlichen demokratischen Ordnung“ und insofern auch bei der „Verfolgung der fundamentalen Staatszwecke der Sicherheit und des Schutzes der Bevölkerung“ müssten „die Regeln des Rechtsstaat“ eingehalten werden, *BVerfG* NJW 2001, 2076, 2077.

808 BVerfGE 115, 320 (359).

809 BVerfGE 100, 313 (376); 107, 299 (318 ff.); 109, 279 (353); 115, 320 (348).

810 BVerfGE 115, 320 (348).

811 Dem einzelnen gehen aufgrund der Heimlichkeit sowohl die Möglichkeit Rechtsschutz zu erhalten, als auch faktisch durch auf den Gang des Verfahrens einzuwirken verloren. Aufgrund dessen wird das Gewicht des Grundrechtseingriffs verstärkt, vgl. dazu auch BVerfGE 113, 348 (383 f.); 115, 320 (353); 120, 274 (325), vgl. dazu auch schon oben S. 80.

Das *Bundesverfassungsgericht* hat wiederholt aus dem Verhältnismäßigkeitsgrundsatz heraus dezidierte Anforderungen an die Ausgestaltung von Sicherheitsinstrumenten entwickelt.[812] Aufgrund der Schwere des Eingriffs seien bestimmte rechtliche, technische und organisatorische Maßnahmen erforderlich, um die Verhältnismäßigkeit zu wahren. Daran wird deutlich, dass das *Bundesverfassungsgericht* zwar grundsätzlich dem Gesetzgeber bei der Justierung der Balance zwischen Freiheit und Sicherheit einen Gestaltungsspielraum zubilligt, dieser aber durch die grundgesetzlichen Vorgaben insofern beschränkt ist, als keine der Positionen zu Gunsten der anderen aufgegeben werden darf und absolut geschützte Grenzen nicht überschritten werden dürfen.[813]

Das *Bundesverfassungsgerichts* hat bei der Beurteilung neuer Sicherheitsinstrumente in den vergangenen Jahren in einer klaren Linie jeweils die Ermächtigungsgrundlagen nicht als generell unangemessen beurteilt, sondern stets nur die aktuelle Umsetzung als unverhältnismäßig bewertet.[814] In den Entscheidungen hat das Gericht betont dass durch eine grundrechtsschonende Umsetzung unter Einsatz technischer, rechtlicher und organisatorischer Gestaltungsmaßnahmen ein verhältnismäßiger Ausgleich erzielt werden könne.

Kritisiert werden kann, dass auf diese Weise durch die Betonung der Anforderungen an die Verhältnismäßigkeit Schritt für Schritt vormals absolut gedachte Grenzen weiter ausgedehnt werden. Freiheitsräume werden so über die Zeit in einem schleichenden Prozess weiter beschnitten.

Dennoch ist die Leistung des Gerichts rechtliche, technische und organisatorische Anforderungen aus dem Verhältnismäßigkeitsgrundsatz heraus zu entwickeln, beachtenswert. Denn darin wird deutlich, dass es letztlich eine Frage der Begrenzung von Maßnahmen und dem Schutz vor Missbrauch ist, die, wenn sie der Gesetzgeber berücksichtigt, diesem einen großen Entscheidungsspielraum bei der Gestaltung neuer technischer Sicherheitsinstrumente einräumt.

3.3 Sicherheit für Freiheit

Ein klares Vorrangverhältnis von Freiheit und Sicherheit kann der Verfassung nicht entnommen werden. Insofern gibt es keine verfassungsrechtlich fundierten eindeutigen Abwägungsregeln, die geeignet sind, Kollisionsfälle aufzulösen. Vielmehr dienen dem Ausgleich zwischen Freiheit und Recht verschiedene im Grundgesetz vorgesehene Mechanismen: Gesetzesvorbehalt und Bestimmtheitsgebot, Grundrechte, Verhältnismäßigkeitsgrundsatz, Kernbereichsschutz sowie Regelungen des Umwelt- und Technikrechts sowie des Gesundheitsschutzes.[815] Der Staat ist auf die Anwendung rechtsstaatlicher Mittel und die Einhaltung rechtsstaatlicher Verfahren beschränkt – dies gilt auch im Ausnahmefall.[816]

---

[812] BVerfGE 120, 274 (309); 120, 378 (399).

[813] Einschlägig sind hier die durch die Identität der Verfassung vorgegebenen Grenzen, dazu noch ausführlich Kap. 5.1 u. Kap. 6.2.

[814] Etwa in BVerfGE 112, 304; 120, 274; 120, 378; vgl. dazu schon oben S. 56 ff.

[815] *Papier*, DVBl. 2010, 801, 803 ff.

[816] *Hopfauf*, in: *Schmidt-Bleibtreu/Klein*, GG 2011, Einl., Rn. 145.

Letztlich zeigt diese Analyse, dass das *Bundesverfassungsgericht* versucht (ebenso wie Stimmen in der Literatur) mittels einer gestuften Betrachtungsweise die Auflösung von Kollisionsfällen zu systematisieren: je höher der Freiheitsverlust, desto höher muss der (potentielle) Sicherheitsgewinn sein.

Die Auflösung von Kollisionsfällen im Sinne eines Ganz oder Gar-nicht verbietet sich in Anbetracht der Komplementarität von Freiheit und Sicherheit: „Ein Staat der vollständige Sicherheit garantieren will, muss alles wissen, alles können und alles dürfen. Ein solcher Sicherheitsstaat würde nicht nur das Ende jegliche Freiheit bedeuten, sondern wäre zudem Quelle dessen, was er ausschließen wollte, nämlich der Unsicherheit.“[817] In diesem Sinne betont auch *Hoffmann-Riem*: „Nicht Maximierung des einen auf Kosten des anderen ist der Königsweg, sondern wechselseitige Optimierung durch Balancierung.“[818]

Dabei muss Sicherheit stets der Verwirklichung von Freiheit dienen. Deutlich wird dies letztlich auch in der Rechtsprechung des Verfassungsgerichts, dass eine Einschränkung von Freiheitsinteressen nie vollständig zulässt, sondern selbst im Angesicht besonders schwerwiegender Bedrohungen den Schutz verfassungsrechtlich absolut geschützten Güter betont und damit das Sicherheitsstreben begrenzt.[819]

Wesentlich eingeschränkt wird die Gestaltungshoheit des Gesetzgebers neben absoluten Schranken wie der Menschenwürdegarantie durch das Rechtsstaatsprinzip: „Bei aller Einsicht in die Notwendigkeit des strafrechtlichen Schutzes unserer freiheitlichen Gesellschaft sollte nicht aus dem Blick geraten, dass ihr Elixier die gelebte Freiheit ist. Zwar erfordert die Ausübung der Freiheit zwingend auch das Vorhandensein von Sicherheit. Eine Sicherheit, die immer mehr zu Lasten der individuellen Freiheit geht, ist aber rechtsstaatlich wertlos.“[820]

So ist es auch dem Rechtsstaatsprinzip in seiner im Grundgesetz verankerten Konzeption immanent, dass Sicherheit eine dienende Funktion zugewiesen ist. Sicherheit ist nicht als Selbstzweck zu gewährleisten, sondern wird als der Freiheitsausübung vorgelagert begriffen. Es ist insofern richtig, dass sie Staatszweck und Grundlage der Staatlichkeit und insofern Voraussetzung der Freiheit ist.

Das Grundgesetz hat an erste Stelle aber Menschenwürde und Grundrechte gesetzt und diese primär als Abwehrrechte gegenüber dem Staat konzipiert. Insofern zeigt gerade auch die Struktur der Grundrechte, dass die Regel die Freiheit sein soll und Einschränkungen dieser nur ausnahmsweise zulässig sein sollen. Gesichert wird der freiheitliche Kern zudem durch absolute Grenzen, die dem Sicherheitsstreben durch die Verfassung gesetzt sind. Insofern muss bei jeder sicherheitspolitischen Maßnahme abgewogen werden – soweit sie sich innerhalb des verfassungsrechtlich zulässigen bewegt – wie

---

817 *Gusy*, VerwArch 2010, 309, 312.

818 *Hoffmann-Riem* 2009, 57.

819 Deutlich wird dies insbesondere in der Entscheidung über das Luftsicherheitsgesetz. Hier betont das Gericht, dass es eine Abwägung Würde gegen Würde Art. 1 GG verletze und daher strikt verfassungswidrig sei, BVerfGE 115, 118.

820 *Brenneisen/Bock*, DUD, 685, 690.

groß ihr Beitrag zur Freiheitsicherung ist und auf der anderen Seite wie hoch der Sicherheitsgewinn durch diese Maßnahme ist.[821] Besteht hier ein Patt, sprechen gute Gründe dafür der Freiheit den Vorrang zu gewähren.[822] Denn „das Maß der Ausstattung des Staats mit Machtmitteln und Eingriffskompetenzen muss (…) immer die Optimierung der Freiheit aller sein. Die Machtausübung des Staats ist kein Selbstzweck, sondern hat nur dienende Funktion. Sie muss im Endeffekt zu mehr und darf nicht zu weniger Freiheit führen. Sie darf nicht die Freiheit gefährden, die sie schützen soll."[823] Der moderne Rechtsstaat ist geprägt dadurch, dass der Staat „die Freiheit des Einzelnen im Interesse aller und einer freiheitsorientierten Gesellschaftsordnung" schützt und zu verwirklichen sucht.[824]

Für eine derartige Betrachtungsweise im Sinne einer „Sicherheit als Diener der Freiheit" spricht schließlich eine historische Betrachtung. Das Grundgesetz wurde auch als Manifest gegen Faschismus und Totalitarismus gefasst mit dem obersten Ziel, die Freiheit des Einzelnen und der Gesellschaft zu gewährleisten.[825] Gerade aus diesem Grund stehen staatliche Maßnahmen und Vorkehrungen für die Sicherheit des Einzelnen oder der Gesellschaft insgesamt unter dem Vorbehalt, Freiheit zu ermöglichen. Sicherheitsstreben darf daher unter Geltung des Grundgesetzes seine freiheitsdienende Funktion nicht einbüßen.

Damit sind jedoch nur die äußersten Grenzen für die Auflösung des Spannungsverhältnisses von Freiheit und Sicherheit grob markiert. Wie im Einzelnen die Verfassung einem wachsenden Überwachungsstreben scharfe Grenzen entgegenstellt, ist eine Frage, die erst in Teil 2 dezidiert untersucht werden wird.

3.4 Praktisch konkordanter Ausgleich zwischen Freiheit und Sicherheit?

Grundsätzlich obliegt die Entscheidung darüber, wie eine angemessene Balance zwischen Freiheits- und Sicherheitsinteressen geschaffen werden kann, dem Gesetzgeber.[826] Die Frage wie ein optimierter Interessenausgleich bei der Ausgestaltung sicherheitsrechtlicher Instrumente erzielt werden kann, ist nicht allein von politischem Interesse, sondern ist auch für die rechtswissenschaftliche Bewertung derartiger Eingriffe von Bedeutung. Für die Gesetzgebung ist ein solcher Ansatz vielversprechend, wenn im Interesse einer möglichst hohen Akzeptanz sicherheitspolitischer Maßnahmen versucht wird, nicht *Maximal*- sondern *Ideal*konzepte zu entwickeln.

---

821 Ganz ähnlich *Calliess,* vgl. dazu oben S. 127.

822 a. A: *Thiel* ist hingegen aufgrund der Komplementarität von Freiheit und Sicherheit und dem daraus folgenden Doppelauftrag an den Gesetzgeber der Ansicht, dass ein Vorrang der Freiheit im Kollisionsfall sich „auch in der Tendenz nicht begründen" lasse; *Thiel* 2011, 182; auch *Stern,* Staatsrecht III, BND. 2, 1994, § 84 IV 6, S. 829 lehnt „eine prinzipielle Präponderanz" der Freiheitsgrundrechte ab.

823 *Roßnagel*, Informatik-Spektrum 2002, 33, 37; vgl. auch Freiheit ist nur in Sicherheit möglich, aber Sicherheit muss der Freiheit dienen, *Ronellenfitsch* 2008, 35.

824 *Roßnagel*, Informatik-Spektrum 2002, 33, 35.

825 Vgl. dazu oben, S. 75.

826 „Die Verfassung verlangt vom Gesetzgeber eine angemessene Balance zwischen Freiheit und Sicherheit herzustellen." *Hopfauf*, in: *Schmidt-Bleibtreu/Klein*, GG, Einl., Rn. 145.

In der Grundrechtstheorie ist der Grundsatz praktischer Konkordanz für die Auflösung von Grundrechtskollisionen weitgehend anerkannt.[827] Fraglich ist, ob nicht ebenso für den Ausgleich der beiden mit Verfassungsrang ausgestatteten Werte Freiheit und Sicherheit auf den Grundsatz praktischer Konkordanz für die Auflösung von Kollisionsfällen zurückgegriffen werden könnte.

Der Grundsatz praktischer Konkordanz hat Eingang in die moderne Verfassungslehre über *Konrad Hesse* gefunden. Dieser leitete ihn aus dem Prinzip der Einheit der Verfassung ab. Verfassungsrechtlich geschützte Rechtsgüter müssten in der Problemlösung so einander zugeordnet werden, „dass jedes von ihnen Wirklichkeit gewinnt."[828] Praktische Konkordanz erfordert insoweit „die „verhältnismäßige" Zuordnung von Grundrechten und grundrechtsbegrenzenden Rechtsgütern: bei der Interpretation verfassungsmäßiger Begrenzungen oder der Begrenzung auf Grund eines Gesetzesvorhaltes geht es darum, beide zu optimaler Wirksamkeit gelangen zu lassen. Da die Grundrechte, auch so wie sie unter Gesetzesvorbehalt stehen, zu den Wesensbestandteilen der verfassungsmäßigen Ordnung gehören, darf diese Verhältnismäßigkeitsbestimmung niemals in einer Weise vorgenommen werden, die eine grundrechtliche Gewährleistung mehr als notwendig oder gar gänzlich ihrer Wirksamkeit im Leben des Gemeinwesens beraubt."[829] Ziel praktischer Konkordanz ist es demnach zwei (gleichrangige) Rechtsgüter in der Weise einander zuzuordnen, dass sie beide optimale Wirksamkeit erlangen.

Lerche formuliert anknüpfend an *Hesse,* dass es darum ginge einen nach allen Seiten hin schonendsten Ausgleich zu erzielen.[830] Auch *Alexy* meint, dass die Abwägung zwischen kollidierenden Grundrechten keine „Alles-oder-Nichts-Frage" sei, sondern es sich um eine „Optimierungsaufgabe" handle.[831] Der Grundsatz praktischer Konkordanz ist auch höchstrichterlich anerkannt. So hat das *Bundesverfassungsgericht* sich wiederholt der Formel praktischer Konkordanz bedient, soweit das Kollisionsverhältnis zweier vorbehaltlos gewährter Grundrechte betroffen war.[832] Selbst in das Völker-

---

827 *Antoni,* in: *Hömig,* GG Komm 2007, Vor 1, Rn. 17; *Jarass,* in: *Jarass/Pieroth,* Einl. Rn. 10; *Dieterich,* ErfKomm, 2012, Einl. GG Rn. 70 ff.; in Bezug auf die Geltung im Rahmen der Berufsfreiheit, *Scholz,* in: *Maunz/Dürig,* GG Komm 2012, Art. 12 Rn. 2; generell kritisch zum Grundsatz praktischer Konkordanz: *Fischer-Lescano*, KJ 2008, 166.

828 *Hesse* 1995 (1977), Rn. 72.

829 *Hesse* 1995 (1977), Rn. 318.

830 *Lerche* 1961, 153.

831 *Alexy* 1986, 152.

832 Bspw. in er Mutzenbacher-Entscheidung 1990 als das *BVerfG* feststellt, dass die Kunstfreiheit aus Gründen des Jugendschutzes eingeschränkt werden könne: „Gerät die Kunstfreiheit mit einem andren Recht von Verfassungsrang in Widerstreit, müssen (…) beide mit dem Ziel der Optimierung zu einem angemessenen Ausgleich gebracht werden. Dabei kommt dem Grundsatz der Verhältnismäßigkeit besondere Bedeutung zu (…). All dies erfordert eine Abwägung der widerstreitenden Belange und verbietet es, einem davon generell - und sei es auch nur für eine bestimmte Art von Schriften - Vorrang einzuräumen.", BVerfGE 83, 130 (143); Auch in der Entscheidung über die Vereinbarkeit der Schulpflicht mit der Religionsfreiheit, rekurriert das Gericht auf diesen Grundsatz: „Im Einzelfall sind Konflikte zwischen dem Erziehungsrecht der Eltern und dem Erziehungsauftrag des Staates im Weg einer Abwägung nach den Grundsätzen der praktischen Konkordanz zu lösen (…).", *BVerfG*, Entsch. v. 31.5.2006 – 2 BvR 1693/04 Rn. 9.

recht hat die Formel praktischer Konkordanz Eingang gefunden. So schlägt *Blumenwitz* im Diskurs um die Zulässigkeit der Kosovo-Intervention vor, dass auch, wenn im Völkerrecht zwei Rechtsgüter (hier das Gewaltverbot mit Menschenrechten) kollidieren, „sich der Rechtsanwender um einen Interessenausgleich, mithin (…) um die Herstellung praktischer Konkordanz zu bemühen" habe.[833]

Der Gedanke die Idee der praktischen Konkordanz für andere Kollisionsfälle fruchtbar zu machen ist insofern nicht neu. Unmittelbar anwendbar auf die Kollision von Freiheits- und Sicherheitsinteressen ist der Grundsatz praktischer Konkordanz nicht, da es sich nicht um zwei unmittelbar kollidierende vorbehaltlos gewährleistete Grundrechte handelt. Zwar kollidieren im Fall von neuen sicherheitspolitischen Maßnahmen diese mit den spezifischen individuellen Freiheitsrechten, da es aber kein Grundrecht auf Sicherheit gibt, kann der Grundsatz praktischer Konkordanz nicht unmittelbar angewendet werden.

Da jedoch beidem – Freiheit wie Sicherheit – ein hoher verfassungsrechtlicher Rang beizumessen ist und sie sich vielfach gegenseitig ergänzen und bedingen kann zumindest der Grundgedanke für eine Optimierung des Interessenausgleichs genutzt werden. Denn auch für das Verhältnis von Freiheit zu Sicherheit gilt, dass beiden Gütern Grenzen gezogen werden müssen, damit beide zu optimaler Wirksamkeit gelangen können.

Allerdings kann der Grundsatz praktischer Konkordanz nicht als allgemeine Abwägungsregel für die Auflösung von Kollisionsfällen von Freiheits- und Sicherheitsinteressen dienen. Denn es ist keineswegs so, dass stets ein „schonendster Ausgleich" erzielt werden muss. Wie aufgezeigt wurde, garantiert das Grundgesetz Sicherheit allein, um die Freiheit des Bürgers zu sichern und nicht als abstrakten Wert. Zentral ist daher für den einzelnen Kollisionsfall immer die Beachtung der verfassungsrechtlichen, freiheitsschützenden Vorgaben. Es muss insofern zunächst die freiheitsdienende Funktion des Sicherheitsinstruments geprüft und sichergestellt werden.[834] Erst dann kann nach einer Optimierung des Interessenausgleichs gefragt werden, wenn es das Ziel sein soll eine verfassungsverträgliche Gestaltung zu finden. Denn zwingend erforderlich ist eine solche Abwägung aber nicht. Sie ist aber zu begrüßen im Sinne der Einheit der Verfassung, da sie die Perspektive auf die Komplementarität von Freiheit und Sicherheit lenkt. Sie ist aber nur dann zulässig, wenn feststeht, dass durch das sicherheitspolitische Instrument das Freiheitsrecht und die freiheitssichernden Garantien nicht gänzlich ausgehöhlt werden. Insofern lässt sich der Grundsatz praktischer Konkordanz nicht unmittelbar als Abwägungsregel auf das Verhältnis von Freiheit und Sicherheit übertragen. Er kann aber dazu dienen, Kollisionsfälle verfassungsverträglich aufzulösen.

---

833 *Blumenwitz*, Politische Studien 1999, 19, 30 f.

834 *Bethge* betrachtet unter einem ähnlichen Gesichtspunkt das Konzept praktischer Konkordanz an sich kritisch, da es Extremlösungen nicht verhindern könne. Es bedürfe vielmehr einer „inhaltlichen Justierung der kollidierenden Grundrechtspositionen, und zwar gerade im Blick auf die jeweilige Grundrechtssubstanz." Diese Substanz sei im Verhältnis zueinander nicht zwangsläufig halbteilig oder arbeitsteilig zu bemessen. Die Verfassung entbehre für die Lösung von Grundrechtkollisionen eines überzeugenden und vor allem übergreifenden Maßstabs entbehre, *Bethge ,* in: *Merten/Papier,* GR II, 2009, § 72, Rn. 76, 85.

3.5 Die verfassungsrechtliche Gewährleistung von Freiheit und Sicherheit vor neuen Herausforderungen

Das digitale Zeitalter stellt mit rasanten technischen Entwicklungen, neuen globalen Bedrohungslagen und durch veränderte Lebensbedingungen die Verfassung vor neue Herausforderungen. Vor dem Hintergrund einer durch ein Gefühl der Verletzbarkeit geprägten Gesellschaft hat das Sicherheitsdogma Konjunktur. Ermöglicht durch Informatisierung und Digitalisierung wird präventiv Gefahrenvorsorge betrieben indem die Freiheitswahrnehmung der Bürger verstärkt erfasst und registriert wird. Insbesondere im Zuge der Terrorismusbekämpfung wurden immer neue Überwachungsmaßnahmen eingeführt. Sicherheit wird in der politischen Realität vielfach Vorrang vor Freiheit eingeräumt.

Anders die Gewährleistungen des Grundgesetzes: dieses verpflichtet zwar den Staat Sicherheit zu gewährleisten, jedoch Sicherheit nicht zum Selbstzweck, sondern immer nur, um Freiheit zu ermöglichen. Das Grundgesetz gebietet keine maximale Sicherheit, sondern ein adäquates Maß. Wie dies zu erzeugen ist, unterfällt der Gesetzgebungsprärogative.

Fest steht jedenfalls, dass die veränderten Verwirklichungsbedingungen sowohl die Gewährleistung von Freiheit als auch von Sicherheit vor neue Herausforderungen stellen. Deutlich wird dies am Beispiel Internet: Anders als in der Off-Line-Welt sind es nicht Personen die unmittelbar miteinander kommunizieren, sondern es wird über Nick-Names, Mail-Adressen und vielfach pseudonyme Accounts miteinander kommuniziert. Die Kommunikation von einem Rechner zu einem anderen erfolgt IP basiert. Zwar ist grundsätzlich jedem Rechner zu einem bestimmten Zeitpunkt eine bestimmte IP-Adresse zuordnungsfähig, wer den Rechner zu diesem Zeitpunkt benutzt hat, ergibt sich daraus aber noch nicht. Diese veränderten Bedingungen, die insbesondere Strafverfolgungsbehörden vor neue Herausforderungen stellen, ändern nichts daran, dass sich Verbrechen zunehmend auf das Internet verlagern und dort begangen werden. Es stellt sich hier konkret die Frage, wie sowohl Freiheit im Internet und zugleich Sicherheit gewährt werden können.

Teil 2: Die Einführung der Vorratsdatenspeicherung und das Verbot umfassender gesamtgesellschaftlicher Überwachung

Konstituiert wurde im Grundgesetz vor über 60 Jahren eine freiheitlich, demokratische Grundordnung. Nunmehr steht die verfassungsrechtliche Gewährleistung von Freiheit und Sicherheit durch Digitalisierung, Internationalisierung und der Ausweitung des Sicherheitsstrebens vor neuen Herausforderungen.[835] Vermag die Verfassung mit diesen Entwicklungen Stand zu halten oder wird das Verhältnis von Freiheit und Sicherheit, wie sie im Grundgesetz als Sicherheit für Freiheit angelegt sind,[836] umgekehrt? Ist die die Architektur des Grundgesetzes den neuen Anforderungen gewachsen?[837] Zum Synonym für den Anspruch des Staates möglichst viele personenbezogene Daten der Bürger zu Sicherheitszwecken zu sammeln und zu verwenden, ist die Vorratsdatenspeicherung geworden.[838] Entsprechend soll den aufgeworfenen Fragen nun im zweiten Teil der Arbeit mit Blick auf die Einführung der Vorratsdatenspeicherung[839] nachgegangen werden.

Im Einzelnen ist zu erörtern, ob mit der Entscheidung für eine Vorratsdatenspeicherung das in der Verfassung konstituierte Verhältnis von Freiheit und Sicherheit, in eine Sicherheit für Freiheit, verkehrt wird – im Sinne der vielfach aufgeworfenen Frage, ob mit der Vorratsdatenspeicherung der Damm auf dem Weg in einen Überwachungsstaat gebrochen wurde.[840]

Um die aufgeworfenen Fragen beantworten zu können, wird zunächst erörtert, inwiefern die Vorratsdatenspeicherung paradigmatisch für das Kollisionsverhältnis von Freiheit und Sicherheit gesehen werden kann (Kap. 4). In Kap. 5 wird dann in rechtlicher Hinsicht untersucht, inwieweit tatsächlich die Gewährleistung eines ausgewogenen Verhältnisses zwischen Freiheits- und Sicherheitsinteressen vor neuen Herausforderungen steht. Es wird gefragt, ob die klassischen Schranken-Schranken in der Lage sind eine Verabsolutierung des Sicherheitsstrebens und damit einen schleichenden Prozess der schrittweisen Einschränkung von Freiheitsräumen zu verhindern. Danach wird das Verbot umfassender gesamtgesellschaftlicher Überwachung, welches das *Bundesverfassungsgericht* erstmals im Urteil zur Vorratsdatenspeicherung vom 2. März 2010 genannt hat, im Hinblick darauf untersucht, ob dieses Verbot geeignet ist staatlichen Überwachungsstreben Grenzen zu setzen (Kap. 7). Dafür wird untersucht,

---

835 Vgl. dazu Teil 1.

836 Vgl. dazu Kap. 3.

837 Ganz in diesem Sinne wurde bereits 1990 gefragt, ob und welchen Schutz das Grundgesetz vor den Gefahren einer unkontrollierten Verarbeitung personenbezogener Daten bietet, *Heußner*, BB 1990, 1281, 1281; Sicherheitsstaat bzw. Sicherheitsgesellschaft wird in Fn. 411 definiert.

838 *Hornung,* PVS 2012, 377.

839 RL 2006/24/EG.

840 *Breyer*, StV 2007, 214 ff., Rn. 218; *Schuldt*, ZD 2011, 112; *Rusteberg*, VBlBW 2007, 171 ff., 172; generell kritisch zur Dammbruch-Argumentaiton *Hefendehl*, JZ 2009, 165; aus den Medien: Spiegel online, „Kritiker warnen vor Überwachungsstaat v. 15.12.2009, abrufbar unter: http://www.spiegel.de/politik/deutschland/0,1518,667192,00.html; *Rath,* „Warnung vor einem Dammbruch, taz v. 16.12.2009, abrufbar unter: http://www.taz.de/!45458/.

auf welchen Grundlagen das Verbot umfassender gesamtgesellschaftlicher Überwachung beruht, was dieses genau beinhaltet und welche Folgen sich aus diesem für Legislative, Exekutive und Judikative ergeben.

Damit soll in diesem Abschnitt, die nicht nur für die Vorratsdatenspeicherung relevante Frage, sondern auch im Hinblick auf andere Überwachungsmaßnahmen zu Sicherheitszwecken untersucht werden, in welchem Umfang Sicherheitspolitik in Freiheitsrechte einschneiden darf und wann sie droht die verfassungsrechtlich garantierte Freiheit zu gefährden. Anknüpfend an die Annahme des *Bundesverfassungsgerichts*, dass eine totale Überwachung nicht mit der verfassungsrechtlichen Identität vereinbar ist[841], wird der Ansatz einer Überwachungs-Gesamtrechnung[842] fortentwickelt.

[841] BVerfGE 125, 260, 324.
[842] *Roßnagel,* NJW 2010, 1238.

4 Vorratsdatenspeicherung - Paradigma für die Kollision zwischen Freiheit und Sicherheit

In Teil 1 wurde aufgezeigt, dass die Gewährleistung von Freiheit und Sicherheit zu Beginn des 21. Jahrhunderts vor neuen Herausforderungen steht. Das den beiden Staatsaufgaben immanente Spannungsverhältnis hat sich verschärft. Dies spiegelt sich in dem Streit um die Einführung einer Speicherung sämtlicher Telekommunikationsverkehrsdaten aller Bürger auf Vorrat. So steht die Vorratsdatenspeicherung paradigmatisch für das Spannungsverhältnis zwischen Freiheit und Sicherheit im digitalen Zeitalter. Warum dies so ist, wird im Folgenden im Einzelnen begründet.

Dafür werden zunächst die für die Vorratsdatenspeicherung zentralen Begriffe bestimmt und der Regelungsumfang der Vorratsdatenspeicherungsrichtlinie (VDS-RL) dargestellt (Kap. 4.1). Es wird dann die Einführungsgeschichte nachgezeichnet (Kap. 4.2) und erörtert, ob und inwiefern die europäische Richtlinie den nationalen Gesetzgeber bindet (Kap. 4.3). Schließlich wird die Kollision von Freiheits- und Sicherheitsinteressen im Rahmen der Vorratsdatenspeicherung anhand der Argumente von Befürwortern und Gegnern einer Vorratsdatenspeicherung dargelegt (Kap. 4.4).

4.1 Grundlagen

Vor dem Blick auf die Geschichte der Einführung der Vorratsdatenspeicherung werden zunächst die zentralen Begriffe bestimmt und die einzelnen Regelungen der Vorratsdatenspeicherungsrichtlinie beschrieben.

4.1.1 Begriffsbestimmungen

Der Begriff „Vorratsdatenspeicherung“ wird synonym für die anlassunabhängige Speicherung von Telekommunikationsdaten für Strafverfolgungs- und Gefahrenabwehrzwecke gebraucht.[843] Dabei werden sämtliche Bestands-, Verkehrsdaten und Standortdaten durch einen Telekommunikationsdiensteanbieter über einen vorher bestimmten Zeitraum für einen eventuellen späteren staatlichen Zugriff auf diese Daten vorgehalten.

Eingang in die rechtswissenschaftliche Diskussion fand die Vorstellung einer „Vorratsdatenspeicherung“ schon 1983 mit dem Volkszählungsurteil.[844] Das *Bundesverfassungsgericht* führte hier aus: „Ein Zwang zur Angabe personenbezogener Daten setzt voraus, daß der Gesetzgeber den Verwendungszweck bereichsspezifisch und präzise bestimmt und daß die Angaben für diesen Zweck geeignet und erforderlich sind. Damit wäre die Sammlung nicht anonymisierter Daten auf Vorrat zu unbestimmten oder noch nicht bestimmbaren Zwecken nicht zu vereinbaren.“[845] In der Literatur wurde auf Grund dieses strikten Verbots einer Datensammlung zu unbestimmten Zwecken auf Vorrat, auch die Vorratsspeicherung der Telekommunikationsverkehrsdaten, wie sie von der Vorratsdatenspeicherungs-

[843] *Sierck/Schöning/Pöhl* 2006.

[844] BVerfGE 65, 1 (47); siehe dazu auch *Gausling* 2010, 7; zum Volkszählungsurteil und der Anerkennung des Rechts auf informationelle Selbstbestimmung, vgl. auch oben Kap. 2.1.3.1.

[845] BVerfGE 65,1 (46).

A. Moser-Knierim, *Vorratsdatenspeicherung,* DuD-Fachbeiträge,
DOI 10.1007/978-3-658-04156-4_4, © Springer Fachmedien Wiesbaden 2014

richtlinie vorgeschrieben wird und mit Gesetz vom 21. Dezember 2008 in deutsches Recht überführt worden ist, als verfassungswidrig bewertet.[846]

Diese Sichtweise verkennt jedoch, dass es sich um keine zweckfreie Datensammlung handelt, soweit der Zweck auf die Daten für die Verfolgung schwerer Straftaten zuzugreifen, bei der Verpflichtung zur Speicherung bereits abschließend festgelegt ist,[847] wie es nunmehr im Urteil zur Vorratsdatenspeicherung vom 2. März 2010 das *Bundesverfassungsgericht* festgestellt hat.[848]

Das Befremdliche an dieser Konstruktion ist jedoch, dass von vorneherein feststeht, dass Daten gespeichert werden, auf die nie zurückgegriffen werden wird. Der Zweck ihrer Speicherung erledigt sich im zur Verfügung stehen für eine später zu treffende „Auswahl" durch die Strafverfolgungsbehörden. Es ist deswegen besonders wichtig, dass die Zweckbestimmung nicht unterlaufen wird.

Der Terminus Vorratsdatenspeicherung wird im Folgenden, im Sinne der Richtlinie über die Vorratsdatenspeicherung, als eine Speicherung von Telekommunikationsverkehrsdaten zu Strafverfolgungs- und Gefahrenabwehrzwecken für einen bestimmten Zeitraum auf Vorrat, verwendet.

Im Rahmen der Vorratsdatenspeicherung werden Telekommunikationsdiensteanbieter verpflichtet sämtliche Bestands-, Verkehrs- und Standortdaten jedweder Telekommunikationsverbindungen zu speichern.

Telekommunikationsdiensteanbieter werden auch „Service Provider" genannt. Gemeint sind damit die Anbieter von Telekommunikationsdiensten für die Öffentlichkeit. Anbieter, die ein eigenes Kommunikationsnetz betreiben, können sodann als (Telekommunikations-) Netzbetreiber bezeichnet werden.

Netzbetreiber gibt es in Deutschland im Gegensatz zu Telekommunikationsdiensteanbietern nur sehr wenige[849] während es weit über 1200 Dienstanbieter[850] gibt. Die

---

[846] *Gercke,* in: *Roggan* 2006, 176; Eine Datensammlung auf Vorrat widerspreche dem Zweckbindungsgrundsatz, so etwa *Gitter/Schnabel*, MMR 2007, 411, 413.

[847] So schon zuvor *Aulehner* 1998, 459 f.

[848] BVerfGE 125, 260 (317).

[849] Nach eigener Recherche können genannt werden: BITel Gesellschaft für Telekommunikation mbH; DATEL (Daten- und Telekommunikations-) GmbH; Deutsche Telekom *AG*; DNS:NET Internet Service GmbH; DOKOM GmbH; ComIngolstadt; Envia Tel; EWE Netz GmbH; Heli Net-Telekommunikations GmbH & Co. KG; Kabel Deutschland Holding *AG*; Kabel BW GmbH; KielNet GmbH; KurpflalzTel GmbH; LambdaNet Communications Deutschland *AG*; M-Net Telekommunikations GmbH; Multi Connect; NetCologne Gesellschaft für Telekommunikation mbH; PrimaCom GmbH; QSC *AG*; RelAIX Networks GmbH; R-Kom GmbH; std.net *AG*; Tele Columbus GmbH & Co. KG; Telefónica Germany; United Internet *AG*; Unitymedia *AG*; Versatel *AG*; Vodafone Deutschland *AG*; VSE NET GmbH; wilhelm.tel GmbH; Witcom GmbH (Kein Anspruch auf Vollständigkeit): Einige der Anbieter sind nur regional tätig und verfügen insoweit auch nur über lokale/ regionale Netze.

[850] Im Jahr 2008 gab es 1.221 ITK-Unternehmen auf dem deutschen Markt, davon 18 mit einem Umsatz von über 250 Mio. Euro; 380 mit einem Umsatz von unter 50.000 Euro; *Statistisches Bundesamt, „*Anzahl der ITK-Unternehmen in 2008", Stand 2010, abrufbar unter: http://www.bitkom.org/files/documents/Anzahl_ITK-Unternehmen_2008_Extranet.pdf.

Dienstanbieter, die über kein eigenes Netz verfügen, erwerben bei einem Netzbetreiber Nutzungsrechte, die sie dann an ihre eigenen Kunden weiterverkaufen.[851]

Zu den Telekommunikationsdiensteanbietern zählen auch Internetdienstanbieter. Sie werden auch Internetdienstleister oder Internet Service Provider (ISP) genannt. Zu beachten ist, dass von der Verpflichtung Telekommunikationsdaten zu speichern allein die Access-Provider, also die Zugangsanbieter betroffen sind, nicht jene die lediglich Inhalte anbieten.

Zu den zu speichernden Daten gehören zunächst die Bestandsdaten. Bestandsdaten sind in § 3 Nr. 3 TKG als die Daten eines Teilnehmers definiert, die „für die Begründung, inhaltliche Ausgestaltung, Änderung oder Beendigung eines Vertragsverhältnisses über Telekommunikationsdienste erhoben werden." Es handelt sich also um die Daten, die nicht in direktem Zusammenhang zu einer einzelnen Kommunikationsverbindung stehen, sondern die konstant einem bestimmten Anschluss zugeordnet werden können. Sie können so auch als Basisdaten, die für ein Vertragsverhältnis über einen Telekommunikationszugang erforderlich sind, bezeichnet werden. Bestandsdaten umfassen den Namen und die Anschrift des Kunden, die Art des kontrahierten Dienstes und schließlich die dem Kunden zum Gebrauch überlassenen Einrichtungen.[852] Bestandsdaten sind auch die dem Kunden konstant zugewiesenen Kennnummern.

Von der Vorratsdatenspeicherung sind darüber hinaus die Verkehrsdaten erfasst. Das sind jeweils die Daten, die „bei der Erbringung eines Telekommunikationsdienstes erhoben, verarbeitet oder genutzt werden"[853]. Der Begriff der Verkehrsdaten in § 3 Nr. 30 TKG ersetzt den früher genutzten Begriff der Verbindungsdaten. Schon aus den Bezeichnungen „Verkehrs-" und „Verbindungsdatum" ergibt sich, dass es sich dabei um Informationen handelt, die den Telekommunikationsdaten*verkehr* bzw. die jeweilige Telekommunikations*verbindung* betreffen.

In § 96 Abs. 1 TKG werden enumerativ Daten aufgelistet, die unter den Begriff der Verkehrsdaten zu subsumieren sind. Dazu gehören die beteiligten Rufnummern, bei mobilen Anschlüssen auch die Standortdaten (S. 1 Nr. 1); der Beginn und das Ende der Verbindung (S. 1 Nr. 2); die Art des in Anspruch genommenen Dienstes (S. 1 Nr. 3), bei festgeschalteten Verbindungen, die jeweiligen Endpunkte und die Datenmenge (S. 1 Nr. 4).

Mithin ergibt sich aus den Verkehrsdaten wer, wann, wie, mit wem, wie lange und von wo aus (mittels Telekommunikation) kommuniziert hat. Es handelt sich um die äußeren Umstände einer Telekommunikationsverbindung. Diese unterfallen dem Schutz

---

[851] Ein Service Provider ohne eigenen Netzbetrieb ist z. B. Debitel mit dem Angebot Debitel E-Plus. Hier kauft Debitel entsprechende Nutzungsrechte von E-Plus. Es ist nicht ungewöhnlich, dass ein Service Provider für mehrere Mobilfunkgesellschaften arbeitet und Verträge vermittelt. Bspw. verkauft Debitel sowohl E-Plus- als auch Telekom-Verträge.

[852] *Holznagel/Ricke,* in: *Spindler/Schuster,* 2011, § 3 TKG Rn.5.

[853] So die einfachgesetzliche Definition in § 3 Nr. 30 TKG.

des Fernmeldegeheimnisses aus Art. 10 Abs. 1 GG[854] und dessen spezialgesetzlicher Ausprägung in § 88 TKG.[855]

Dynamische IP-Adressen[856] sind rechtlich als Verkehrsdaten zu qualifizieren, da es sich bei ihnen um Daten handelt, die bei der Erbringung eines Telekommunikationsdienstes erhoben, verarbeitet oder genutzt werden (§ 3, S.1 Nr. 3 TKG).[857] Dies ändert sich auch nicht bei einer Umstellung auf IPv6 – soweit weiter eine dynamische Adressvergabe erfolgt. Denn soweit Adressen dynamisch, also nur für den jeweiligen Telekommunikationsvorgang vergeben werden, handelt es sich um Daten, die sich auf eine konkrete Telekommunikationsverbindung beziehen, also um Verkehrsdaten.[858]

Zwar wurde lange darum gestritten, ob eine Auskunft über den Inhaber einer dynamischen IP-Adresse über § 113 TKG zulässig ist. Strittig war dabei jedoch nicht, ob es sich bei IP-Adressen um ein Verkehrsdatum handelt, sondern allein die Frage, ob die Auskunft, die allein unter Rückgriff auf ein Verkehrsdatum möglich ist, bei der aber „nur" ein Bestandsdatum beauskunftet wird, als Verkehrs- oder Bestandsdatenauskunft zu charakterisieren ist. Dieser Frage kommt eine solche Brisanz zu, weil sie für die Bestimmung der einschlägigen Rechtsgrundlage entscheidend ist.[859] Im Ergebnis handelt es sich, auch wenn nur ein Bestandsdatum beauskunftet wird, um eine Auskunft, die nur unter Eingriff in das Telekommunikationsgeheimnis möglich ist, und die insoweit inhaltlich einer Verkehrsdatenabfrage gleichkommt.[860] Dies hat im Januar 2012 schließlich auch das *Bundesverfassungsgericht* bestätigt.[861] In diesem Sinne verlangt auch die einfachgesetzliche Regelung in § 101 Abs. 9 UrhG, dass wenn „die Auskunft nur unter Verwendung von Verkehrsdaten (§ 3 Nr. 30 TKG) erteilt werden" kann, „für ihre Erteilung eine vorherige richterliche Anordnung über die Zulässigkeit der Verwendung der Verkehrsdaten erforderlich, die von dem Verletzten zu beantragen ist".[862]

Statische IP-Adressen sind anders als dynamische IP-Adressen als Bestandsdaten zu qualifizieren. Sie sind zwar auch, soweit sie sich auf eine konkrete Verbindung beziehen, als Verkehrsdaten zu qualifizieren, da sie aber zur inhaltlichen Ausgestaltung eines Vertragsverhältnisses fest einem Kunden zugewiesen werden und so in engerem

---

854 Dazu schon oben Kap. 2.1.3.3.

855 *Gausling* 2010, 9.

856 Zur dynamischen IP-Vergabe, vgl. oben Kap. 1.1.2.1.2, S. 21 ff.

857 So auch *BVerfG* Beschl. v. 24.1.2012 – 1 BvR 1299/05; *LG Frankenthal*, Beschl. v. 21.05.2008, Az. 6 O 156/08.

858 *Gausling* 2010, 13; a.A. *Freund/Schnabel*, MMR 2011, 495, 497 f.

859 *Gausling* 2010, 13, Fn. 46 ff. weist zutreffend darauf hin, dass nur vermeintlich über die Frage gestritten wurde, ob es sich bei dynamischen IP-Adressen um Verkehrsdaten handelt. Zu unterscheiden ist der Streit von der Frage, ob es sich bei dynamischen IP-Adressen um personenbezogene Daten handelt, dazu oben S. 84.

860 Beschl. v. 13.11.2010, Az. 2 BvR 1124/10; a.A. *OVG Münster*, Beschl. V. 17.2.2009 - Az.: 13 B 33/09.

861 *BVerfG* Beschl. v. 24.1.2012, Az 1 BvR 1299/05.

862 *Spindler,* NJW-Beil. 2012, 98, 99; *Bohne,* in: *Wandtke/Bullinger,* UrhR 2009, § 101 UrhG Rn. 33.

Bezug zum Vertrag als zu den Umständen einer einzelnen Telekommunikationsverbindung stehen,[863] sind sie primär Bestandsdaten.

Verkehrsdaten sind auch die *Standortdaten* (vgl. § 96 S. 1 Nr. 1 TKG), die bei der Nutzung von Mobilfunkgeräten anfallen. In § 3 Nr. 19 TKG sind Standortdaten definiert als diejenigen Daten, „die in einem Telekommunikationsnetz erhoben oder verwendet werden und die den Standort des Endgeräts eines Endnutzers eines Telekommunikationsdienstes für die Öffentlichkeit angeben". Es handelt sich also um die Informationen über die Funkzelle in der sich ein Mobilfunkgerät während einer Telekommunikationsverbindung befindet. Die Informationen über den Standort sind bei Funkzellen umso genauer, je kleiner die Funkzelle ist.[864]

4.1.2 Regelungsinhalt der Vorratsdatenspeicherungsrichtlinie

Die Vorratsdatenspeicherungsrichtlinie beinhaltet in Art. 1 Abs. 1 die Verpflichtung der Mitgliedstaaten bestimmte Daten, soweit sie bei der Bereitstellung von Telekommunikationsdiensten erzeugt oder verarbeitet werden, auf Vorrat zu speichern, um sicherzustellen, dass diese Daten für die Ermittlung, Feststellung und Verfolgung schwerer Straftaten zur Verfügung stehen. Die Speicherung auf Vorrat kollidiert mit den gemeinschaftsrechtlichen Vorgaben der Datenschutzrichtlinie für elektronische Kommunikation vom 12. Juli 2002. Daher ändert Art. 11 VDS-RL den Art. 15 RL 2002/58/ EG dahingehend, dass die in Abs. 1 RL 2002/58/EG titulierten Löschungspflichten und Verwendungsvorschriften nicht für die gemäß der Vorratsdatenspeicherungsrichtlinie zu speichernden Vorratsdaten gelten sollen.

- Zu speichernde Daten

Welche Daten gespeichert werden müssen bestimmt Art. 5 VDS-RL. In dessen Abs. 1 sind die zu speichernden Daten enumerativ benannt und zunächst nach Verwendungszwecken geordnet.

Gespeichert werden sollen die Daten, die erforderlich sind:

(a) „zur Rückverfolgung und Identifizierung der Quelle des Adressaten einer Nachricht";

(b) „zur Identifizierung des Adressaten einer Nachricht";

(c) „zur Bestimmung von Datum Uhrzeit, Dauer und Art einer Nachrichtenübermittlung";

(d) „zur Ermittlung der Endeinrichtung oder der vorgeblichen Endeinrichtung";

(e) und „zur Bestimmung des Standorts mobiler Geräte".

Innerhalb dieser Verwendungszwecke werden sodann die zu speichernden Datentypen aufgelistet. Erfasst werden sämtliche Verkehrs- einschließlich aller Standortdaten, die

[863] *Gausling* 2010, 14.
[864] Dazu oben Kap. 1.1.2.2.

im Rahmen einer Telekommunikationsverbindung anfallen. Art. 2 a) VDS-RL verpflichtet auch dazu sämtliche mit den Verkehrs- und Standortdaten in Zusammenhang stehenden Daten, die für die Feststellung eines Teilnehmers erforderlich sind, zu speichern. Allerdings sind nur diejenigen Daten zu speichern, die bei den Telekommunikationsdiensteanbietern ohnehin anfallen. Ausdrücklich von der Speicherung ausgenommen sind (gemäß Art. 5 Abs. 2 VDS-RL) Daten, die Aufschluss über den Inhalt der Kommunikation geben.

Den Mitgliedstaaten verbleibt hier ein geringer Spielraum bezüglich der Subsumtion unter die genannten Datentypen. Auch wenn nahezu alle anfallenden Telekommunikationsverkehrsdaten erfasst werden, verlangt die VDS-RL nicht jede anonyme Telekommunikation zu unterbinden. So beinhaltet die Richtlinie keine Bestimmung zur Erhebung von Bestandsdaten bei Prepaid-Angeboten.[865] Auch verlangt sie nicht die Erfassung von nicht angenommenen Anrufen. Ebenso ist die Zuordnung von Ports beim Zugang über NAT[866] nicht von der Speicherungspflicht erfasst.

- Speicherzeitraum

Die Daten müssen gemäß Art. 6 VDS-RL mindestens für sechs Monate und dürfen maximal 24 Monate ab dem Zeitpunkt der Kommunikation auf Vorrat gespeichert werden. Darüber hinaus eröffnet Art. 12 Abs. 1 VDS-RL den Mitgliedstaaten die Möglichkeit die maximale Speicherfrist für einen begrenzten Zeitraum zu verlängern, wenn dies durch besondere Umstände gerechtfertigt ist. Über eine solche Maßnahme ist nach Art. 12 Abs. 2 VDS-RL die Kommission in Kenntnis zu setzen, die dann innerhalb von sechs Monaten das Vorgehen entweder stillschweigend billigt oder dieses als willkürliche Diskriminierung oder als verschleierte Beschränkung des Handels zwischen den Mitgliedstaaten ablehnt.

Mit einem Spielraum zwischen sechs und (über) 24 Monaten verbleibt den Mitgliedstaaten bei der Wahl des Speicherzeitraums ein erheblicher Gestaltungsspielraum.

- Adressaten

Art. 1 Abs. 1 und Art. 3 Abs. 1 VDS-RL bestimmen, dass die Anbieter „öffentlich zugänglicher elektronischer Kommunikationsdienste oder Betreiber eines öffentlichen Kommunikationsnetzes“ zur Vorratsdatenspeicherung zu verpflichten sind.

Es verbleibt den Mitgliedstaaten insofern zumindest die Möglichkeit zwischen einer Verpflichtung der Dienstanbietern oder der Netzbetreibern zu wählen.

---

865 *Breyer*, StV 2007, 215; *Leutheusser-Schnarrenberger*, ZRP 2007, 9; *Szuba* 2011, 54.
866 Zur Funktionsweise von NAT, vgl. oben S. 25, Fn. 120.

- Kostenerstattung

Auch wenn die Richtlinie auf eine Harmonisierung des Binnenmarktes zielt, enthält sie keine Vorgaben dazu, ob den verpflichteten Unternehmen die entstehenden Kosten erstattet werden sollen. Diese, gerade für die Harmonisierung zentrale Frage, lässt die Richtlinie offen und überlässt die Entscheidung darüber den einzelnen Mitgliedstaaten.

- Datensicherheit

Bezüglich etwaiger Maßnahmen zum Schutz der Daten verpflichtet die Richtlinie in Art. 7 a) bis d) VDS-RL die Mitgliedstaaten sicherzustellen, dass:

(a) die auf Vorrat gespeicherten Daten der gleichen Sicherheit und dem gleichen Schutz wie die im Netz vorhandenen Daten unterliegen;

(b) geeignete technische und organisatorische Maßnahmen getroffen werden, um die Daten gegen zufällige oder unrechtmäßige Zerstörung, Verlust, Veränderung, Speicherung, Verarbeitung, Zugänglichmachung oder Verbreitung zu schützen;

(c) Zugang zu den Daten allein besonders ermächtigte Personen erhalten, und

(d) alle Daten, die weder abgerufen noch gesichert wurden, zum Ende der Vorratsspeicherungsfrist vernichtet werden.

Zur Kontrolle, ob die Anforderungen an Datenschutz und -sicherheit eingehalten werden, müssen die Mitgliedstaaten gemäß Art. 9 VDS-RL eine oder mehrere öffentliche Stellen benennen, die für die Kontrolle zuständig ist und diese völlig unabhängig[867] durchführt. Kontrollstellen können dieselben sein, wie jene zu deren Errichtung die Mitgliedstaaten durch Art. 28 der Datenschutzrichtlinie[868] verpflichtet wurden. Diese Stellen sollen jährlich eine Statistik über gewisse Fragen der Anwendung, Umsetzung und des Einsatzes der auf der Richtlinie beruhenden nationalen Vorschriften, an die Kommission zu übermitteln.[869]

Insgesamt enthält die Richtlinie in Bezug auf die Datensicherheit nur Mindestanforderungen, die von den einzelnen Mitgliedstaaten verstärkt werden können.

---

867 Zur völligen Unabhängigkeit der Datenschutzbeauftragten, vgl. *EuGH* v. 9.3.2010 – Az. C 518/07 Kommission *./. Deutschland*; dazu *Albrecht* jurisPR-ITR 15/2010, Anm. 4; *Roßnagel* EuZW 2010, 299.

868 Vgl. Fn. 481.

869 Mit Hilfe dieser Daten sollte die Kommission bis zum 15.9.2009 einen Bericht für das Europäische Parlament und den Rat gem. Art. 14 erstellen. Der Bericht wurde schließlich zum 20.4.2011 fertig gestellt, KOM (2011) 225. Zum Evaluationsbericht und dem Umsetzungsstand in den anderen Mitgliedstaaten, siehe ausführlich unten Kap. 4.2.6.

- Verwendung der Daten

Art. 1 Abs. 1 VDS-RL legt fest, dass die Daten „zum Zwecke der Ermittlung, Feststellung und Verfolgung von schweren Straftaten" vorzuhalten sind. Art. 4 VDS-RL stellt sodann klar, dass die Fragen des Zugangs und der Verwendung der gespeicherten Daten durch die Mitgliedstaaten zu regeln seien. Dabei seien insbesondere die „Anforderungen der Notwendigkeit und Verhältnismäßigkeit einzuhalten". Ausdrücklich verlangt Art. 8 VDS-RL, dass die Daten so gespeichert werden, dass sie „unverzüglich an die zuständigen Behörden auf deren Anfrage hin weitergeleitet werden können".

Es ist insofern nahezu vollständig den Mitgliedstaaten überlassen, welche staatlichen Stellen unter welchen formellen und materiellen Voraussetzungen Zugriff auf die Daten erhalten sollen. Hier ist den Mitgliedstaaten ein weiter Gestaltungsspielraum überlassen.[870]

Die zum Teil von Kritikern der Vorratsdatenspeicherung vertretene Ansicht, dass die Mitgliedstaaten der Umsetzungspflicht nachkommen könnten, indem sie zwar eine Speicherungspflicht anordnen aber keine Ermächtigung zum Zugriff auf die Daten einführen,[871] dürfte jedoch nicht genügen, um die Richtlinie umzusetzen. Auch wenn sie überwiegend, so jedenfalls der *Europäische Gerichtshof*, der Harmonisierung des Binnenmarktes dient, ist in der Richtlinie auch geregelt, dass die Daten zum Zwecke der Strafverfolgung und Gefahrenabwehr vorzuhalten sind. Dürfte nun auf die Daten überhaupt nicht – auch nicht für diese Zwecke – zugegriffen werden, würde die Zweckbestimmung vollständig leerlaufen. Eine solche Speicherung auf Vorrat ohne jeden Zweck, würde eklatant den datenschutzrechtlichen Prinzipien (insbesondere dem Zweckbindungsgrundsatz und den Grundsatz der Erforderlichkeit)[872] verletzen.

- Rechtsbehelfe, Haftung und Sanktionen

Art. 13 VDS-RL verlangt von den Mitgliedstaaten mittels der in Kapitel III der DS-RL geregelten Instrumente (Rechtsbehelfe, Haftung und Sanktionen) im Hinblick auf die Datenverarbeitung die Umsetzung der Richtlinienvorgaben sicherzustellen. Das heißt, die Mitgliedsstaaten müssen gemäß Art. 13 VDS-RL sowohl dafür sorgen, dass der Speicherpflicht nachgekommen wird (Abs. 1), als auch, dass Missbrauch der Daten verhindert oder geahndet wird (Abs. 2). Wie konkret Rechtsbehelfe, Haftung und Sanktionen ausgestaltet werden, überlässt die Richtlinie vollständig den Mitgliedstaaten und bietet ihnen damit einen weiten Gestaltungsspielraum.

---

870 Vgl. etwa *Szuba* 2011, 55.

871 So etwa *Breyer* auf der Abschlusstagung des Forschungsprojekts INVODAS, dazu *Schuldt*, ZD 2011.

872 Vgl. zu diesen, oben S. 87 ff.

4.2 Rückblick: Die Einführung der Vorratsdatenspeicherung

Die Richtlinie 2006/24/EG (Vorratsdatenspeicherungsrichtlinie) wurde vom *Europäischen Parlament* und vom *Rat* am 15. März 2006 verabschiedet und trat zum 3. Mai 2006 in Kraft.[873] Den Mitgliedstaaten wurde eine Umsetzungsfrist bis 15. September 2007 und bezüglich der Internetdienste bis 15. März 2009 eingeräumt. Die Umsetzung in deutsches Recht folgte mit dem „Gesetz zur Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen sowie zur Umsetzung der Richtlinie 2006/24/EG" vom 21. Dezember 2007.[874] Das *Bundesverfassungsgericht* erklärte die Regelungen mit Urteil vom 2. März 2010 für nichtig. Die Einführung der Vorratsdatenspeicherung wurde wissenschaftlich durch eine Fülle an Publikationen begleitet.[875]

---

873 V. 13.4.2006; ABl. EU Nr. L 105 S. 54–60.

874 BGBl. 2007 I, 3198.

875 **Im Vorfeld:** *Zöller* 2003, 291 ff.; *Kühling*, K&R 2004, 105 ff.; *Mahnken* 2005; **Zur VDS-RL:** *Alvaro*, RDV 2005, 47; *Alvaro*, DANA 2006, 52; *Roßnagel*, EuZW 2006, 30; *Sierck/Schöning/Pöhl,* 2006; *Westphal*, EuR 2006, 706; *Breyer*, StV 2007, 214 ff.; *Leutheusser-Schnarrenberger*, ZRP 2007, 9; *Rusteberg*, VBlBW 2007, 171 ff.; *Roßnagel/Bedner/Knopp*, DUD 2009, 536 ff.; *Schlepper/Leese* NK 2011, 70; **Zur Umsetzung in deutsches Recht**: *Wüstenberg*, MMR-Int 2006, 91; *AK-Vorrat et al.,* 2007; *Gietl*, K&R 2007, 545; *Gitter/Schnabel*, MMR 2007, 411; *Gola/Klug/Reif*, NJW 2007, 2599; *Hornung*, MMR 2007, XIII; *ULD* 27.6.2007; *Zöller*, GA 2007, 392 ff.; *Bär*, MMR 2008, 215; *Czychowski/Nordemann*, NJW 2008, 3095; *Eckhardt*, DUD 2008, 520; *Feldmann*, NZA 2008, 1398; *Gietl*, DUD 2008, 317; *Hoeren*, JZ 2008, 668; *Ders.*, NJW 2008, 3099; *Jenny*, CR 2008, 282 ff.; *Klug/Reif*, RDV 2008, 89; *Koch*, NZA 2008, 911; *Petri*, DUD 2008, 729; *Puschke/Singelnstein*, NJW 2008, 113; *Bedner*, DUD 2009, 372; *Braun*, K&R 2009, 386; *Dix/Petri*, DUD 2009, 531 ff.; *Frenz*, EuZW 2009, 6; *Grimm/Michaelis*, Der Betrieb 2009, 174; *Hefendehl*, JZ 2009, 165; *Hensel*, DUD 2009, 527; *Kindt*, MMR 2009, 661; *Kurz/Rieger* 2009; *Maaßen,* MMR 2009, 511; *Mayer*, K&R 2009, 313; *Petri* DUD 2011, 607; *Polenz,* CR 2009, 225; *Schütze/Eckhardt,* CR 2009, 775; *Wettern,* DUD 2009, 343; *Eckhardt/Schütze,* K&R 2010, I; *Kramer*, ArbR Aktuell 2010, 164 ff.; *Orantek,* NJ 2010, 193; **Rspr. zur Kostenübertragung:** *OVG Berlin-Brandenburg,* Beschl. v. 2.12.2009 – 1l S 81.09, K&R 2010, 141; MMR 2010, 269 ff.; *VG Berlin,* Beschl. v. 16.1.2009 – VG 27 27 A 321.08, MMR 2009, 5; **Zur Umsetzung in Europa:** Forgó, et al., DUD 2008, 680; *Schweda* ZD-Aktuell 2012, 02882; **Zum Urteil des *EuGH*** (NJW 2009, 1801)**:** *Gietl/Tomasic*, DUD 2008, 795; *Ambos,* JZ 2009, 468; *Gundel,* EuR 2009, 536; *Simitis*, NJW 2009, 1782; *Terhechte,* EuZW 2009, 199; *Roßnagel*, EuZW 2010, 299; **Im Anschluss an das Urteil des BVerfG:** *Beukelmann*, NJW-Spezial 2010, 184 ff.; *Blankenburg*, MMR 2010, 587; *Breyer*, NJW aktuell 2010, 12; *Eckhardt/ Schütze*, CR 2010, 225; *Forgó/Krügel,* K&R 2010, 217; *Gercke,* StV 2010, 281; *Härting*, BB 2010, 839 ff.; *Heckmann*, jurisPR-ITR 2010, Anm. 1; *Heun*, CR 2010, 247; *Hornung/Schnabel*, DVBl. 2010, 824; *Kläner*, NJ 2010, 204; *Klesczewski*, JZ 2010, 629; *Marlie/Bock*, ZIS 2010, 524; *Möstl*, DVBl. 2010, 808; *Ohler*, JZ 2010, 626; *Rössel*, ITRB 2010, 74; *Roßnagel*, DUD 2010, 544; *Roßnagel*, NJW 2010, 1238; *van Ooyen*, Recht und Politik 2010, 98; *Volkmer*, NStZ 2010, 318; *Wehr/Ujica*, MMR 2010, 667; *Westphal*, EuZW 2010, 494; *Wolff*, NVwZ 2010, 751; *Bäcker*, EuR 2011, 103; *Britz*, JA 2011, 81; *Darnstädt*, DVBl. 2011, 263; *Hirsch* KritV 2011, 139; *Kinast/Schmitz*, NJW 2011, NJW-aktuell Nr. 40, 14; *Knierim* 2011a; *Knierim* 2011b; *Knierim*, ZD 2011, 17; *Meinicke*, HRRS 2011, 398; *Möstl* ZRP 2011, 225; *Wegener/Schramm*, MMR 2011, 9;*Wollweber*, NJW 2011, NJW-aktuell Nr. 25, 14; *Hornung,* PVS-Sonderheft 46/2012, 377; *Schweda* ZD Aktuell 2012, 02882; **Monographien:** *Breyer* 2005; *Gausling* 2010; *Greenawalt* 2009; *Szuba* 2011.; Die Aufzählung erhebt keinenAnspruch auf Vollständigkeit.

Vor der Einführung der Vorratsdatenspeicherung mittels der Vorratsdatenspeicherungsrichtlinie EG 24/2010 waren sowohl in Deutschland als auch auf europäischer Ebene verschiedene Versuche gescheitert eine solche einzuführen. Erste Ansätze zu einer Einführung einer Vorratsdatenspeicherung gab es bereits in den 1990er Jahren. Gerade in Anbetracht dieser langen Vorgeschichte, erstaunt es, dass die Richtlinie dann im bis dato kürzesten Rechtssetzungsverfahren verabschiedet wurde.[876]

Zunächst soll der Prozess auf europäischer Ebene nachgezeichnet werden (Kap. 4.2.1), bevor die Einführung in deutsches Recht und ihre fast zwei Jahrzehnte zurückgehende Vorgeschichte dargestellt wird (Kap. 4.2.2). Im Anschluss werden das Urteil des *Europäischen Gerichtshofs* (Kap. 4.2.3) und das des *Bundesverfassungsgerichts* skizziert (Kap. 4.2.4). Abschließend wird die aktuelle politische Diskussion um die Vorratsdatenspeicherung in Deutschland und Europa erläutert (Kap. 4.2.5) bevor noch der Stand der Umsetzung in den anderen Mitgliedstaaten überblicksartig dargestellt wird (Kap. 4.2.6).

4.2.1 Die Vorratsdatenspeicherungsrichtlinie

Auf europäischer Ebene war zunächst versucht worden, eine europaweite Verpflichtung zur Vorratsspeicherung der Telekommunikationsverkehrsdaten als Rahmenbeschluss in der damals dritten Säule der Europäischen Union (der Polizeilichen und Justiziellen Zusammenarbeit, kurz PJZ) einzuführen.[877] Den Entwurf für einen Rahmenbeschluss zur Vorratsspeicherung von Kommunikationsdaten hatten, unter dem Eindruck der Zuganschläge am 11. März 2004 in Madrid, Vertreter Frankreich*s*, Irlands, Schwedens und des Vereinigten Königreichs in das Europäische Parlament eingebracht.[878] Die Bundesregierung unterstütze den Vorschlag damals auf europäischer Ebene, obwohl der Bundestag zu dieser Zeit eine abwehrende Haltung gegenüber Mindestspeicherpflichten vertrat.[879]

Gemäß dem Entwurf eines Rahmenbeschlusses vom 29./30. April 2004 sollten Telekommunikationsverkehrsdaten für mindestens zwölf und maximal 36 Monate gespeichert werden. Vorgesehen war die Möglichkeit, im Rahmen von Rechtshilfeersuchen auf die in anderen EU-Staaten gespeicherten Daten zuzugreifen. Der Rahmenbeschluss enthielt keine Entschädigungsregeln. Der Vorschlag stieß auf massiven Widerstand im Europäischen Parlament. Auch der juristische Dienst des Rates sprach sich gegen eine

---

[876] Die Richtlinie wurde nur drei Monate nach ihrer Vorlage im damit bis dahin kürzesten Rechtssetzungsverfahren der Union verabschiedet, so *Alvaro*, DANA 2006, 52; vgl. dazu auch oben Fn. 51, S. 14.

[877] Dieser wurde jedoch abgelehnt. Der Grundstein für die Einführung einer Vorratsdatenspeicherung auf europäischer Ebene wurde bereits mit der Formulierung von Art. 15 Abs. 1 RL 2002/58/EG geschaffen. Danach kann die Verpflichtung zur Löschung von Verbindungsdaten gesetzlich gelockert werden um „Strafverfolgungen durchzuführen oder der nationale und öffentliche Sicherheit zu schützen", *Orantek*, NJ 2010, 193, 197; ausführlich zum Prozess bis zur Verabschiedung der Richtlinie und danach auch *Schweda,* SIRA 2011, 56 ff.

[878] Ratsdokument 8954/04 vom 28.4.2004. Für ein solches Vorgehen – absichtlich den „Umweg über Europa" zu wählen, weil eine nationale Umsetzung scheiterte – hat sich in der Politikwissenschaft der Begriff des „Policy Laundering" („Politikwäsche") durchgesetzt, *Westphal* EuR 2006, 706, 717.

[879] *Orantek*, NJ 2010, 193, 198.

Regelung einer Vorratsdatenspeicherung im Rahmen der polizeilichen und justiziellen Zusammenarbeit (innerhalb der damals dritten Säule) aus. Es fehle hier an einer tragfähigen Rechtsgrundlage. Darüber hinaus bestünden erhebliche Bedenken gegen die Vereinbarkeit mit den Gemeinschaftsgrundrechen.[880] Schließlich wurde der Rahmenbeschluss nicht zur Abstimmung gebracht. Denn es zeichnete sich ab, dass die für den Rahmenbeschluss erforderliche einstimmige Mehrheit nicht erzielt werden könnte: Das niederländische Parlament hatte seine Regierungsvertreter ausdrücklich angewiesen, gegen die Verabschiedung des Rahmenbeschlusses zu stimmen.[881]

Unter dem Eindruck der Bombenanschläge vom 7. Juli 2005 auf vier U-Bahnen und einen Bus in London wurde dann ein Vorschlag für eine Regelung der Vorratsdatenspeicherung in einer Richtlinie vorgelegt.[882] Das heißt die Vorratsdatenspeicherung sollte nicht mehr im Rahmen der Polizeilichen und Justiziellen Zusammenarbeit und so auch nicht mehr als Rahmenbeschluss, der nur einstimmig beschlossen werden kann, gefasst werden, sondern im Rahmen der wirtschaftlichen Zusammenarbeit (also innerhalb der ersten Säule, der Europäischen Gemeinschaft). Sie sollte damit als Instrument zur Harmonisierung des Binnenmarktes eingeführt werden, auf Grundlage von Art. 95 EGV (a.F.; Art. 114 AEUV). Begründet wurde die Erforderlichkeit der Harmonisierungsmaßnahme damit, dass es zu Wettbewerbsverzerrungen käme, da es in manchen Ländern eine Vorratsspeicherung der Telekommunikationsverkehrsdaten gebe und in anderen nicht.[883] An dieser Ansicht wurde vielfach Kritik geübt.[884]

Das Europäische Parlament nahm den Entwurf an. Was erstaunen kann, da ursprünglich eine anlassunabhängige Speicherung vom Plenum abgelehnt wurde. Auch der Berichterstatter *Alvaro* votierte gegen den Richtlinienentwurf.[885]

Die Vorratsdatenspeicherung kann als Resultat einer gelungenen Versicherheitlichung[886] gesehen werden. Als Reaktion auf die Attentate in Madrid und dann vor al-

---

880 *Alvaro* RDV 2005, 47, 48.

881 *Rusteberg*, VBlBW 2007, 171, 173.

882 KOM (2005) 438; Annahme durch die Kommission am 21.9.2005; Übermittlung an den Rat und das Parlament am 23.9.2005; Verfahren 2005/0182(COD); Ein Bericht des Berichterstatters *Alvaro* zum Verfahren ist abrufbar unter: http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+REPORT+A6-2005-0365+0+DOC+XML+V0//DE&language=DE; dazu auch *Rusteberg*, VBlBW 2007, 171, 173. Der Bundesrat begrüßte in einem Beschluss vom 25.11.2005 diese Initiative mit einem Beschluss, BR-Drs. 723/05.

883 Erwägungsgrund 6 VDS-RL.

884 So sah etwa auch der Wissenschaftliche Dienst des Bundestags in der Richtlinie zum einen Verstoß gegen Gemeinschaftsgrundrechte, zum anderen fehle es an einer tauglichen Rechtsgrundlage *Sierck/Schöning/Pöhl* 2006, 19.

885 Stellungnahme von *Alvaro* abgedruckt in RDV 2005, 47; Stellungnahmen, Berichte und Reden des Abgeordneten abgerufen werden unter: http://www.alexander-alvaro.de/topics/themen/burgerrechteinneres/vorratsdatenspeicherung.

886 Dazu schon oben S. 14.

lem auf jene in London wurde sie entgegen aller Bedenken in einem sehr schnellen Verfahren verabschiedet.[887]

4.2.2 Die Einführung einer Vorratsdatenspeicherung in deutsches Recht

Die Richtlinie wurde kurz nach Ablauf der Umsetzungsfrist mit dem Gesetz zur Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen vom 21. Dezember 2007 in nationales Recht umgesetzt.[888]

Erstaunlich erscheint diese Umsetzung mit großer Mehrheit in Anbetracht der Tatsache, dass sämtliche vorangegangenen Versuche eine Vorratsdatenspeicherung in deutsches Recht einzuführen gescheitert waren.[889] Hier waren immer wieder die verfassungsrechtlichen Bedenken gegen eine Vorratsspeicherung betont worden. Zum Teil wurde vermutet, dass dieser Umweg über Europa absichtlich genommen worden wäre.[890] In der Politikwissenschaft wird ein solches Vorgehen als Policy Laundering bezeichnet.[891] Dies beschreibt letztlich treffend das Umschwenken von einem Entwurf eines Rahmenbeschlusses auf eine Richtlinie.

So gab es in Deutschland bereits erste Ansätze zur Einführung einer Speicherung von Telekommunikationsdaten auf Vorrat Mitte der 1990er Jahre. Im Jahr 1996 forderte der Bundesrat im Rahmen der Novellierung des Telekommunikationsgesetzes die Einführung von Mindestspeicherfristen. Dies stieß damals auf breite Ablehnung. Die Bundesregierung war zu dieser Zeit der Ansicht, dass Mindestspeicherpflichten gegen den Verhältnismäßigkeitsgrundsatz und gegen die Grundsätze von Zweckbindung und Erforderlichkeit verstoßen würden.[892]

Im Jahr 2000 forderte dann die Innenministerkonferenz der Länder die Einführung einer Vorratsdatenspeicherung, die jedoch von den Datenschutzbeauftragten heftig kritisiert wurde. Sie sei unverhältnismäßig und würde dem vom *Bundesverfassungsgericht* wiederholt betonten Verbot einer Rundumüberwachung widersprechen.[893]

Fünf Jahre später wurde dann erneut, im Zug der verschärften Sicherheitspolitik im Anschluss an die Terroranschläge vom 11. September 2001, ein Gesetzesentwurf zur Einführung von Mindestspeicherfristen in den Bundesrat eingebracht.[894] Auch dieser wurde wegen verfassungsrechtlicher Bedenken abgelehnt.[895]

---

[887] Beschleunigend wirkte auf dieses Verfahren die Tatsache, dass die Attentate von *London* unter anderem durch die Auswertung der Verbindungsdaten eines Attentäters aufgeklärt werden konnten. Dazu schon oben S. 13 f.

[888] Verabschiedung im Bundestag mit Stimmen der SPD und CDU/CSU-Fraktionen, Zustimmung durch den Bundesrat erfolgte am 30.11.2007 (BGBl. 2007 I, 3198), Inkrafttreten am 1.1.2008. Das Gesetz wurde mit eindeutiger Mehrheit angenommen; vgl. dazu *Orantek*, NJ 2010, 193, 199.

[889] Dazu auch eine umfassende Darstellung bei *Orantek*, NJ 2010, 193, 195 ff.

[890] So etwa *Westphal,* EuR 2006, 706, 717.

[891] Zum Policy Laundering allgemein, http://www.policylaundering.org/PolicyLaunderingIntro.html.

[892] BR. Drs. 13/4438 v. 23.4.1996; siehe dazu auch *Orantek*, NJ 2010, 193, 196, Fn. 31 m. w. Nachw.

[893] *Innenministerkonferenz* am 24.11.2000, zitiert nach *Scholz* 2004, 276.

[894] Antrag des Freistaats Bayerns und Hessens, vgl. PM 29/2002 (BR) v. 26.2.2002; http://www.bundesrat.de/nn_15524/DE/presse/pm/2002/029-2002.html.

[895] BR-Drs. 1014/01; Ablehnungsbeschluss vom 22.3.2002.

Kurz zuvor war in den Bundestag der Entwurf eines „Gesetzes zur Verbesserung der Bekämpfung von Straftaten der organisierten Kriminalität und des Terrorismus", mit dem ebenso eine Verpflichtung zur Vorratsdatenhaltung eingeführt werden sollte, eingebracht worden.[896] Der Entwurf wurde ebenfalls abgelehnt.[897]

Im März 2002 verabschiedete sodann der Bundesrat, nunmehr im Namen der „Verbesserung der Ermittlungsmaßnahmen wegen des Verdachts sexuellen Missbrauchs von Kindern und der Vollstreckung freiheitsentziehender Sanktionen" einen Gesetzesentwurf zur Vorratsspeicherung von Telekommunikationsdaten.[898] Dieser wurde unter anderem wegen datenschutzrechtlicher Bedenken vom Bundestag abgelehnt. Auch wurde die Verhältnismäßigkeit des Eingriffs in die Berufsfreiheit bezweifelt.[899]

Im Jahr 2003 forderte der Bundesrat in seiner Stellungnahme zum Regierungsentwurf des neuen Telekommunikationsgesetzes die Telekommunikationsdiensteanbieter zur Speicherung von Verkehrsdaten, soweit diese erhoben werden, zu verpflichten.[900] Die Bundesregierung entsprach dem nicht. Schließlich kam das Gesetzgebungsvorhaben vor den Vermittlungsausschuss. In diesem Verfahren konnte sich der Vorstoß des Bundesrats nicht durchsetzen.[901]

Dass auch bei der Verabschiedung des Gesetz zur Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen vom 21. Dezember 2007 noch erhebliche Zweifel an der Verfassungsmäßigkeit einer Vorratsdatenspeicherung bestanden, zeigt eine von mehreren Abgeordneten der SPD abgegebene Erklärung:[902] „Trotz schwerwiegender politischer und verfassungsrechtlicher Bedenken werden wir im Ergebnis dem Gesetzentwurf aus folgenden Erwägungen zustimmen. Erstens. Grundsätzlich stimmen wir mit dem Ansatz der Bundesregierung und der Mehrheit unserer Fraktion dahingehend überein, dass die insbesondere durch den internationalen Terrorismus und dessen Folgeerscheinungen entstandene labile Sicherheitslage auch in Deutschland neue Antworten benötigt. (…) Eine Zustimmung ist auch deshalb vertretbar, weil davon auszugehen ist,

---

896 Durch Abgeordnete der CDU/CSU Fraktion, BT-Drs. 14/6834 vom 29.8.2001.

897 BT-PlPr 14/227 v 21.3.2002, 22515 auf Empfehlung des Rechtsausschusses BT-Drs. 14/8627.

898 Gesetzentwurf vom. 27.3.2002, BR-Drs. 275/02; Der Bundesrat vertrat die Ansicht, dass es große Schwierigkeiten für die Strafverfolgung gebe auf Grund veränderter technischer Rahmenbedingungen vor allem wegen der Schwierigkeit, dass es bei Prepaid-Angeboten häufig an Bestandsdaten fehle. Das Artikelgesetz sah vor, dass der Gesetzgeber ermächtigten werden solle eine Vorratsspeicherung per Rechtsverordnung einzuführen. Genauere Angaben zu Speicherkategorien und Speicherfristen enthielt der Gesetzesentwurf nicht. Das Rechtsgut der verletzten Kinder auf Schutz ihrer körperlichen und seelischen Unversehrtheit und ihrer körperlichen Integrität überwiege gegenüber dem Eingriff in die Grundrechte der Bürger. Und zwar indem er Mindestspeicherfristen von „Bestands-, Nutzungs- und Abrechnungsdaten" für eine effektive Strafverfolgung und Gefahrenabwehr und die Erfüllung der Aufgaben der Nachrichtendienste erlässt.

899 BT-Drs. 14/9801, 15 ff.

900 BR-Drs. 755/03 Beschluss v. 19.12.2003, S. 33.

901 BR-Drs. 200/1/04 v. 23.3.2004, S. 3.

902 nach § 31 GoBT.

dass in absehbarer Zeit eine Entscheidung des *Bundesverfassungsgerichts* möglicherweise verfassungswidrige Bestandteile für unwirksam erklären wird."[903]

Der nationale Gesetzgeber zeigte sich darüber hinaus bemüht den Eindruck zu vermitteln, dass er zu der Einführung sämtlicher Regelungen, die mit dem Umsetzungsgesetz zur Vorratsdatenspeicherungsrichtlinie erfolgt sind, gezwungen sei. Dass er in Teilen der Regelung weit über das von der Richtlinie geforderte Maß hinausging, verschwieg er hingegen.[904] So fordert die Richtlinie weder Übermittlungsbefugnisse für mittels Telekommunikation begangener Straftaten noch für Zwecke der Gefahrenabwehr und jene der Nachrichtendienste.[905]

Insgesamt erfasste das Artikelgesetz Änderungen des TKG, der StPO, des BKAG und des JVEG. Der neu eingeführte § 113a TKG begründete die Verpflichtung der Betreiber öffentlich zugänglicher Telekommunikationsdienste (Abs. 1 S. 1) sämtliche Verkehrsdaten (Abs. 2), die Auskunft über die an einer Telekommunikationsverbindung beteiligten Anschlüsse, den Zeitpunkt der Telekommunikation und den Ort geben, für sechs Monate zu speichern und sie für die staatliche Aufgabenwahrnehmung verfügbar zu halten. Auch Anbieter von Diensten elektronischer Post (Abs. 3) und von Internetzugangsdiensten (Abs. 4) wurden zu einer Verkehrsdatenspeicherung verpflichtet. Zudem wurden gemäß § 113a Abs. 7 TKG die Betreiber von Mobilfunkzellen verpflichtet Daten über die geografische Lage der Funkzelle sowie ihrer Hauptstrahlrichtung vorzuhalten. Daneben sah die deutsche Regelung eine Verpflichtung von Anonymisierungsdiensten zur Vorratsspeicherung vor.[906] Inhaltsdaten waren gemäß §113a Abs. 8 TKG von der Speicherverpflichtung ausgenommen.

In Bezug auf die Datensicherheit wurde verlangt, die im Bereich der Telekommunikation erforderliche Sorgfalt zu beachten (Abs. 10). Zur Löschung der Daten wurde in § 113a Abs. 11 TKG eine Frist von einem Monat eingeräumt.

Die Zwecke zu denen die nach § 113a TKG gespeicherten Daten verwendet werden dürfen, wurden in § 113b TKG geregelt. Auf Verlangen der zuständigen Stellen sollten die Daten nur zur Verfolgung von Straftaten, zur Abwehr von erheblichen Gefahren für die öffentliche Sicherheit oder zur Erfüllung der gesetzlichen Aufgaben der Nachrichtendienste, übermittelt werden, soweit dies in den gesetzlichen Bestimmungen unter Bezugnahme auf § 113a TKG vorgesehen und die Übermittlung im Einzelfall angeordnet worden ist. Daneben sollte eine Verwendung der Daten nur für die Auskunftserteilungen nach § 113 TKG zulässig sein.

Die Ermächtigungsgrundlage zur Verwendung der Daten im Rahmen der Strafverfolgung wurde mit § 100g StPO geschaffen. Ein heimlicher Zugriff auf die Daten war

---

[903] Stenographischer Bericht der 124. BT-Sitzung vom 9.11.2007, Anlage 4, 13032.

[904] Pointiert formuliert *Zöller*, dass eine Durchsicht des Regierungsentwurfs deutlich mache, „dass der Gesetzgeber einmal mehr nicht der Versuchung wiederstehen kann, unter dem Deckmantel eines vermeintlich unumgänglichen Umsetzungs- bzw. Änderungsbedarfs zugleich auch weitere Wünsche der Sicherheitsbehörde nach einer Ausweitung von Überwachungsbefugnissen zu erfüllen", *Zöller*, GA 2007, 392 ff., 414.

[905] *Klug/Reif,* RDV 2008, 89, 95; *Ziebarth*, DUD 2009, 25, 27.

[906] So ausdrücklich in den Erwägungsgründen zu § 113 Abs. 4, 6 TKG-E, BT-Drs. 16/5846.

hier vorgesehen für den Fall, dass der Verdacht begründet ist, dass jemand als Täter oder Teilnehmer entweder eine Straftat „von auch im Einzelfall erheblicher Bedeutung, insbesondere eine in § 100a Abs. 2 StPO bezeichnete“ oder eine „Straftat mittels Telekommunikation“ begangen hat und der Zugriff „für die Erforschung des Sachverhalts oder die Ermittlung des Aufenthaltsortes erforderlich ist“.

§ 113a Abs. 4 StPO begründete die Pflicht eine jährliche Statistik über die Anzahl der Verfahren, die Art der Anlassstraftat und den Umfang der abgerufenen Daten zu erstellen.

§ 20m BKAG ermächtigt dazu, zur Wahrnehmung der Aufgaben der Nachrichtendienste, auf die gemäß § 113a TKG gespeicherten Daten zuzugreifen.

Das Umsetzungsgesetz wurde in weiten Teilen von der Literatur für zu unbestimmt oder unverhältnismäßig oder auch aus anderen Gründen als verfassungswidrig erachtet.[907]

Bereits der Europäische Gesetzgebungsprozess war in der wissenschaftlichen Diskussion vielfach beachtet worden.[908] Gleiches gilt für das nationale Umsetzungsgesetz.[909] Es formierte sich ein breiter gesellschaftlicher Widerstand. Umgehend wurden zahlreiche Verfassungsbeschwerden eingereicht. Zum einen klagten Vertreter von *FDP* und *Grünen* und einer zur Vorratsdatenspeicherung verpflichteten Anonymisierungsdienstleisterin, zum anderen organisierte der *AK Vorratsdatenspeicherung* erstmals in der Geschichte der Bundesrepublik ein Massenbeschwerdeverfahren. Insgesamt legten 34.443 Bürger Verfassungsbeschwerde ein.[910]

Ein Urteil des Verfassungsgerichts wurde erst zwei Jahre später gefasst. Bis dahin wurde in mehreren Vorabentscheidungen die Verwendung der Daten stark eingeschränkt.[911] Es kann nur vermutet werden, dass das *Bundesverfassungsgericht* die Ent-

---

907 Zu unbestimmt: *Roßnagel/Bedner/Knopp*, DUD 2009, 536 ff., 538; *Ziebarth*, DUD 2009, 25, 28; zahlreiche Nachweise zur Diskussion um die Vorratsdatenspeicherung in Fn. 875.

908 *Alvaro*, RDV 2005, 47; *Alvaro*, DANA 2006, 52; *Roßnagel*, EuZW 2006, 30; *Sierck/Schöning/Pöhl,* 2006; *Westphal*, EuR 2006, 706; *Breyer*, StV 2007, 214 ff.; *Leutheusser-Schnarrenberger*, ZRP 2007, 9; *Rusteberg*, VBlBW 2007, 171 ff.; *Roßnagel/Bedner/Knopp*, DUD 2009, 536.

909 *Wüstenberg*, MMR-Int 2006, 91; *AK-Vorrat et al.,* 2007; *Gietl*, K&R 2007, 545; *Gitter/Schnabel*, MMR 2007, 411; *Gola/Klug/Reif*, NJW 2007, 2599; *Hornung*, MMR 2007, XIII; *ULD* 27.6.2007; *Zöller*, GA 2007, 392 ff.; *Bär*, MMR 2008, 215; *Czychowski/Nordemann*, NJW 2008, 3095; *Eckhardt*, DUD 2008, 520; *Feldmann*, NZA 2008, 1398; *Gietl*, DUD 2008, 317; *Hoeren*, JZ 2008, 668; *Ders.*, NJW 2008, 3099; *Jenny*, CR 2008, 282 ff.; *Klug/Reif*, RDV 2008, 89; *Koch*, NZA 2008, 911; *Petri*, DUD 2008, 729; *Puschke/Singelnstein*, NJW 2008, 113; *Bedner*, DUD 2009, 372; *Braun*, K&R 2009, 386; *Dix/Petri*, DUD 2009, 531 ff.; *Frenz*, EuZW 2009, 6; *Grimm/Michaelis*, Der Betrieb 2009, 174; *Hefendehl*, JZ 2009, 165; *Hensel*, DUD 2009, 527; *Kindt*, MMR 2009, 661; *Kurz/Rieger* 2009; *Maaßen,* MMR 2009, 511; *Mayer*, K&R 2009, 313; *Petri* DUD 2011, 607; *Polenz,* CR 2009, 225; *Schütze/Eckhardt,* CR 2009, 775; *Wettern,* DUD 2009, 343; *Eckhardt/Schütze,* K&R 2010, I; *Kramer*, ArbR Aktuell 2010, 164.

910 *Krempl,* heise online v. 29.2.2008, abrufbar unter: http://www.heise.de/-185285.html.

911 BVerfGE 121, 1; erweitert durch Beschl. v. 28.10.2008; BVerfGE 122, 120.

scheidung in der Sache herauszögerte, da es zunächst die anstehende Entscheidung des *Europäischen Gerichtshofs* abzuwarten suchte.

4.2.3 Das Urteil des Europäischen Gerichtshofs vom 10. Februar 2009

Unmittelbar nach Verabschiedung der Vorratsdatenspeicherungsrichtlinie hatte Irland unterstützt von der Slowakischen Republik den *Europäischen Gerichtshof* angerufen.[912] Hintergrund der Klage war nicht, dass sich Irland generell gegen eine Vorratsdatenspeicherung wendete, sondern es eine weitergehende Vorratsdatenspeicherung umsetzen wollte. Es gründete die Klage auf Bedenken gegen die Wahl der Rechtsgrundlage (Art. 95 EGV (a.F.)).[913] Gegenstand der Klage waren insofern rein formelle Rechtsfragen. Auf deren Prüfung beschränkte sich dann auch der *Europäische Gerichtshof* im Urteil vom 10. Februar 2009.[914]

Auch in der rechtswissenschaftlichen Diskussion war vielfach bestritten worden, dass mit Art. 95 EGV a.F. (jetzt Art. 114 AEUV) die korrekte Rechtsgrundlage gewählt worden sei. [915]

Der *Europäische Gerichtshof* war jedoch anderer Ansicht. Das Gericht schloss sich im Urteil den Anträgen des Generalanwalts *Bot* an und stellte fest, dass sich die Regelungen zur Vorratsdatenspeicherung unmittelbar auf das Funktionieren des Binnenmarkts auswirken würden und der Erlass entsprechender Harmonisierungsvorschriften daher gerechtfertigt gewesen sei. Da sich die angegriffenen Regelungen vornehmlich mit der Tätigkeit der Dienstanbieter befassten und eben nicht den Zugriff der Polizei- und Justizbehörden auf die gesammelten Daten regelten, sei der Erlass der Regelungen aufgrund ihres überwiegenden Bezugs zum Binnenmarkt als Richtlinie auch geboten gewesen.

Das im Jahr 2006 ergangene Urteil zur Weitergabe von Fluggastdaten,[916] in dem das Gericht Art. 95 EGV a.F. als untaugliche Rechtsgrundlage qualifiziert hatte, sei nicht einschlägig. Im Fall des Fluggastdaten-Abkommens sei wesentlicher Bezugspunkte des zugrundeliegenden Ratsbeschlusses die Übermittlung von Fluggastdaten aus den Buchungs- und Abfertigungssystemen der europäischen Fluggesellschaften an Sicherheitsbehörden in den USA gewesen. Anders im Fall der Vorratsdatenspeicherung: Hier sei allein die Tätigkeit der Dienstanbieter im Europäischen Binnenmarkt betroffen und

---

912 Vgl. dazu auch *Schweda,* SIRA 2011, 56, 58.

913 Entsprechende Bedenken hatte bspw. in der deutschsprachigen Literatur *Westphal*, EuR 2006, 706, 712 geäußert; kritisch auch *Rusteberg*, VBlBW 2007, 171 ff., 174; sowie im Folgenden *Ziebarth*, DUD 2009, 25, 27; *Gausling* 2010, 30 f.

914 *EuGH* C-301/06, Irland ./. Parlament u. Rat.

915 „Der *EuGH* sollte die RL für nichtig erklären" *Ziebarth*, DUD 2009, 25, 27; in diesem Sinne auch *Zöller*, GA 2007, 392 ff., 414; dazu auch ausführlich *Gausling* 2010, 30; zum Vorwurf es handle sich um „Policy Laundering" vgl. oben Fn. 891; *Kotzur* meint, dass die „Leidenschaftlichkeit des Streits (um die Einführung der VDS, *Anm. d. Autorin)* gründet nicht zuletzt in der Sorgte, durch eine stärker exekutivische Auslagerung rechtsstaatlich sensibler Sicherheitsgesetzgebung auf die Union versuchten die Mitgliedstaaten sowohl der strikten Grundrechtsbindung ihrer Verfassungen als auch den mitwirkungs- und Kontrollbefugnissen ihrer Parlamente zu entfliehen", *Kotzur,* EuGRZ 2011, 105, 106

916 Urt. v. 30.5.2006, Az. C-317/04.

es sei ausdrücklich keine Regelung zur Übermittlung der Daten an staatliche Stellen enthalten.[917]

Das Urteil enttäuschte Kritiker der Vorratsdatenspeicherung, die sich eine umfassende Prüfung anhand der europäischen Grundrechte gewünscht hatten, weil sich das Gericht darauf beschränkt hat, allein die formellen Fragen zu prüfen. Dies ist jedoch nur konsequent, da Gegenstand der Klage letztlich nur formelle Fragen waren.

Nicht überzeugend ist jedoch die Annahme, die Richtlinie weise einen überwiegenden Bezug zum Binnenmarkt auf. Zwar sind von den Regelungen der Richtlinie die Telekommunikationsunternehmen betroffen. Die Richtlinie regelt aber gerade jene Punkte nicht, die Einfluss auf den Binnenmarkt haben, wie etwa die Frage der Kostenerstattung. Zudem wirkt die Begründung es handle sich um ein Instrument zur Harmonisierung vor dem Hintergrund der Entstehungsgeschichte der Richtlinie, vorgeschoben.[918] Auch wird rückblickend, so auch in der Evaluation der Umsetzung der Richtlinie, deutlich, dass die anvisierte Harmonisierung gerade nicht geglückt ist.[919]

4.2.4 Das Urteil des Bundesverfassungsgerichts vom 2. März 2010

Erst im März 2010 und damit über zwei Jahre nach der Verabschiedung des Gesetzes entschied das *Bundesverfassungsgericht* über die zahlreichen Verfassungsbeschwerden.[920] Dem Judikat vorangegangen waren mehrere einstweilige Anordnungen.[921] In diesen hatte das Gericht die Möglichkeiten die auf Vorrat zu speichernden Daten abzurufen eingeschränkt. So hatte es den Zugriff auf die Daten nur nach richterlicher Anordnung im Fall eines konkreten Verdachts für eine schwere Straftat für zulässig erachtet. Wie das Gericht in der Hauptsache entscheiden würde, war in den Entscheidungen allerdings nicht erkennbar.

Viele Kritiker der Vorratsdatenspeicherung hofften auf eine Vorlage an den *Europäischen Gerichtshof,* oder dass das Gericht selbst die Vorgaben der Richtlinie für verfassungswidrig erklären würde.[922] Die Hauptsache-Entscheidung war so mit großer Spannung erwartet worden.[923]

---

[917] Kritisch zum Urteil *Ohler*, JZ 2010, 626, 626f.; *Ambos*, JZ 2009, 468, 471; *Gausling* 2010, 30f.; 34, 37f.

[918] So *Gausling* 2010, 34, die vermutet, dass die Harmonisierung nur vorgeschoben sei. Die für eine Harmonisierung benötigte Regelung der Kostenfrage sei eben nicht geregelt worden. Gleiches gilt für den Sicherheitsstandard. Da dieser die Belastung der Telekommunikationsanbieter wesentlich präge sowie um einen europaweit einheitlichen Grundrechtsschutz zu gewähren, sei es für eine Harmonisierung erforderlich, dass diesbezüglich eine europaweit einheitliche Regelung getroffen wird. Dazu auch *Roßnagel,* DuD 2010, 544.

[919] EU Kom (2011), 225, 33; dazu noch ausführlich unten Kap. 4.2.6.

[920] Vgl. dazu auch schon oben S. 153.

[921] BVerfGE 121, 1; erweitert durch Beschl. v. 28.10.2008; BVerfGE 122, 120.

[922] *Westphal*, EuR 2006, 706, 720; *Dix/Petri,* DuD 2009, 531, 534; *Gausling* 2010, 42 m. w. Nachw.

[923] vgl. auch *Hornung,* PVS 2012, 377, 387, 399 (zu den verschiedenen Wegen, die vor dem Urteil des BVerfG diskutiert wurden).

4.2.4.1 Die Entscheidung des Verfassungsgerichts

Das *Bundesverfassungsgericht* hat sich in der Entscheidung erst gar nicht mit der Frage der Vereinbarkeit der Richtlinie mit Gemeinschaftsgrundrechten auseinandergesetzt. Es hat die Entscheidung so auch nicht dem *Europäischen Gerichtshof* zur Entscheidung vorgelegt. Eine Vorlage sei nicht erforderlich, da eine Vorratsdatenspeicherung, wie sie von der Richtlinie verlangt wird, „nicht schlechthin mit Art. 10 GG unvereinbar" sei.[924]

Das Gericht führt aus, dass es sich bei einer vorsorglich anlasslosen Speicherung der Telekommunikationsdaten nicht zwingend um eine von vornherein verbotene Form der Datensammlung handele, wie es in der Literatur vertreten wurde.[925] „Erfolgt sie zu bestimmten Zwecken, kann eine solche Speicherung, eingebunden in eine dem Eingriff adäquate gesetzliche Ausgestaltung, vielmehr auch den Verhältnismäßigkeitsanforderungen im engeren Sinne genügen".[926]

Das Gericht sieht zwar die Identität der Verfassung durch eine an den Mindestanforderungen orientierte Ausgestaltung als noch nicht verletzt an. Auf der anderen Seite betont das Gericht, dass das Konzept einer Vorratsdatenspeicherung nicht generell unbedenklich sei. Die Einführung der Vorratsdatenspeicherung dürfe „nicht als Schritt hin zu einer Gesetzgebung verstanden werden, die auf eine möglichst flächendeckende vorsorgliche Speicherung aller für die Strafverfolgung oder Gefahrenprävention nützlichen Daten zielte. Eine solche Gesetzgebung wäre (…) von vornherein mit der Verfassung unvereinbar." Ausdrücklich stellt das Gericht fest, dass die verfassungsrechtliche Unbedenklichkeit der Vorratsdatenspeicherung voraussetze, „dass diese eine Ausnahme bleibt."[927] „Dass die Freiheitswahrnehmung der Bürger nicht total erfasst und registriert werden darf, gehört zur verfassungsrechtlichen Identität der Bundesrepublik Deutschland für deren Wahrung sich die Bundesrepublik in europäischen und internationalen Zusammenhängen einsetzen muss."[928]

In Bezug auf die Umsetzung der Richtlinienvorgaben formuliert das Gericht hohe verfassungsrechtliche Hürden. Eine verfassungskonforme Umsetzung der Richtlinie sei zwar möglich, insgesamt unterliege die Einführung einer anlasslosen Speicherung der Telekommunikationsverkehrsdaten sämtlicher Bürger aber „sowohl hinsichtlich ihrer Begründung als auch hinsichtlich ihrer Ausgestaltung, insbesondere auch in Bezug auf die vorgesehenen Verwendungszwecke, besonders strengen Anforderungen".[929]

Das Gericht stellt fest, dass die überprüften Vorschriften in das durch Art. 10 Abs. 1 GG geschützte Telekommunikationsgeheimnis eingreifen.[930] Den Eingriff wer-

---

[924] BVerfGE 125, 260 (LS 1).
[925] Siehe dazu schon oben S. 139 f.
[926] BVerfGE 125, 260(321).
[927] BVerfGE 125, 260 (324).
[928] BVerfGE 125, 260 (324).
[929] BVerfGE 125, 260 (317).
[930] Gegenüber dem Recht auf informationelle Selbstbestimmung stellt dies die speziellere Garantie dar. Das durch Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG geschützte Recht auf informationelle Selbstbestimmung ist daher daneben nicht anwendbar, BVerfGE 125, 260 (310); Zum Schutzbereich des Telekommunikationsgeheimnisses, vgl. auch schon oben Kap. 2.1.3.3, S. 95 ff.

tet das Gericht als besonders intensiv auf Grund der Streubreite der Maßnahme, ihrer Anlasslosigkeit, dem Risiko weiteren Ermittlungsmaßnahmen ausgesetzt zu werden ohne dazu Anlass gegeben zu haben, sowie der Möglichkeit, aus den Daten umfassende Bewegungs- und Persönlichkeitsprofile zu erstellen. Darüber hinaus erlaube eine Auswertung der Daten, Rückschlüsse auf den Inhalt der Kommunikation zu ziehen.[931] So könne dann auch „nicht ohne Weiteres davon ausgegangen werden, dass der Rückgriff auf diese Daten grundsätzlich geringer wiegt als eine inhaltsbezogene Telekommunikationsüberwachung".[932]

Aus diesen Erwägungen zur Eingriffsintensität folgert das Gericht, dass es für die verfassungsrechtliche Unbedenklichkeit der Vorratsdatenspeicherung Voraussetzung sei, „dass die Ausgestaltung der Speicherung und der Verwendung der Daten dem besonderen Gewicht einer solchen Speicherung angemessen Rechnung trägt".[933] „Maßgeblich" für die Verhältnismäßigkeit sei zunächst, dass sie nicht unmittelbar durch den Staat erfolgt, Inhalte nicht erfasst werden und schließlich, dass die Speicherfrist auf sechs Monate begrenzt bleibt.[934] Die Datenverwendung muss dem Eingriffsgewicht entsprechen und kommt daher nur für besonders hochrangige Gemeinwohlgüter in Betracht. Auch bei einer Übermittlung der Daten muss die ausschließliche zweckgebundene Verwendung gesichert werden. Eine Kennzeichnung der Daten sei daher erforderlich.[935] Daneben müssten besondere Vertrauensbeziehungen geschützt werden.[936]

Darüber hinaus müsse gesetzlich ein besonders hoher Standard der Datensicherheit gewährleistet werden.[937] Die Datensicherheit sei aufgrund des Umfangs und der potenziellen Aussagekraft der Datenbestände für die Verhältnismäßigkeit von großer Bedeutung.[938] Das Gericht nennt verschiedene technische Maßnahmen, die bei der Vorratsdatenspeicherung umgesetzt werden sollten. Hierzu gehören eine getrennte Speicherung, Stand-Alone Systeme, asymmetrische Verschlüsselung der Daten unter getrennter Verwahrung der Schlüssel, Vier-Augen-Prinzip in Verbindung mit fortschrittlichen Authentifizierungsverfahren für den Zugriff auf die Daten, eine revisionssichere Protokollierung der Zugriffe und der Löschung sowie den Einsatz automatisierter Fehlerkorrektur- und Plausibilitätsverfahren.[939]

Solch detaillierte technische Vorgaben sind ein Novum in der Rechtsprechung des *Bundesverfassungsgerichts*, auch wenn das Gericht gleichzeitig erklärt, dass diese Vorgaben nur beispielhaft seien. Die Ausführungen zeigen in jedem Fall, dass das Ge-

[931] BVerfGE 125, 260 (319) .
[932] BVerfGE 125, 260 (328).
[933] BVerfGE 125, 260 (324).
[934] BVerfGE 125, 260, (321 f.).
[935] BVerfGE 125, 260 (333).
[936] BVerfGE 125, 260 (334); siehe dazu unten Kap. 9.1.2.4.
[937] BVerfGE 125, 260 (LS. 4; 325 f.).
[938] BVerfGE 125, 260 (LS 4, 325).
[939] BVerfGE 125, 260 (326).

richt der technischen Ausgestaltung eine hohe Bedeutung für die Verhältnismäßigkeit der Maßnahme beimisst. [940]

Schließlich sei die Vorratsdatenspeicherung nur dann verhältnismäßig, wenn gesetzlich hinreichende Vorkehrungen zur Transparenz der Datenverwendung, der Gewährleistung eines effektiven Rechtsschutzes und effektiver Sanktionen vorgegeben sind.[941] Die Verwendung der Daten müsse grundsätzlich offen erfolgen, das heißt der Betroffene sei zu benachrichtigen. Wenn dies unterbleiben sollte, sei eine richterliche Entscheidung erforderlich, die in qualifizierter Weise zu begründen wäre.

In seiner abweichenden Meinung legt Richter *Schluckebier* dar, dass er die Feststellung der Senatsmehrheit, es handle sich um einen besonders schweren Eingriff in Art. 10 GG nicht teilt. [942] Die Daten würden nur bei den Privaten gespeichert, eine Kenntnisnahme durch den Staat fände nicht statt. So fehle es an jeder objektivierbaren Grundlage „für die Annahme eines eingriffsintensivierenden Einschüchterungseffekts“.[943] Entsprechend erachtet er die Ausgestaltung als zumutbar und verhältnismäßig im engeren Sinne. Die Kritik des Richters teilt in seiner ebenfalls abweichenden Stellungnahme auch Richter *Eichberger*.[944]

4.2.4.2 Kritische Würdigung des Urteils in der Literatur

Den Sondervoten schlossen sich auch kritische Stimmen aus der Literatur an.[945] „Bei der vorliegenden Konstellation nimmt das *Bundesverfassungsgericht* eine Funktion als Ersatzgesetzgeber ein, die in dieser Deutlichkeit selten ist. Der Gesetzgeber kann auf Grund der europarechtlichen Umsetzungspflicht nicht auf den Grundrechtseingriff insgesamt verzichten, sondern ist gezwungen, die verfassungsgerichtlichen Vorgaben in Gesetzesform zu gießen. Der Gesetzgeber wird „in die Zange” genommen, auf der einen Seite vom Grundgesetz gem. Art. 20 III GG und auf der anderen Seite vom europarechtlichen Anwendungsvorrang“.[946]

Die Kritik basiert auf der in den Sondervoten der Richter *Schluckebier* und *Eichenberger* zum Ausdruck kommenden Ansicht, dass es sich bei der Vorratsdatenspeicherung

---

[940] Mit den exakten technischen Ausführungen hat sich das Gericht sehr stark an die von den Sachverständigen im Verfahren vorgebrachten Äußerungen gehalten. Diese sind verkürzt veröffentlicht in *Roßnagel*/*Bedner*/ *Knopp*, DUD 2009, 536 ff.; sämtliche sachverständigen Stellungnahmen sind auch abrufbar unter http://www.vorratsdatenspeicherung.de/content/view/51/70/lang,de/

[941] BVerfGE 125, 260 (334).

[942] BVerfGE 125, 260 (365 ff.).

[943] BVerfGE 125, 260 (366).

[944] BVerfGE 125, 260 (380 ff.).

[945] *Tomuschat*, „Die Karlsruher Republik“, Die Zeit v. 12.5.2010 , abrufbar unter: http://www.zeit.de/2010/20/P-oped-*Bundesverfassungsgericht* (Darauf folgte eine Erwiderung von *Hirsch*, Die Zeit v. 20.5.2010, abrufbar unter: http://www.zeit.de/2010/21/P-Widerspruch-*Bundesverfassungsgericht*-Tomuschat); *Schluckebier* führt aus: „Damit ersetzt das Urteil im praktischen Ergebnis die Gesetzgebung bis hin zu den Details einer vom Senat für verfassungsrechtlich allein statthaft erachteten Regelung“, BVerfGE 125, 260 (374).

[946] *Wolff*, NVwZ 2010, 751 ff; so auch die abweichende Meinung des Richters *Schluckebier,* BVerfGE 125, 260 (373).

um keinen besonders schweren Grundrechtseingriff handle.[947] Dieser habe zwar ein „besonderes Gewicht", er sei aber „im Vergleich zu inhaltsbezogenen Überwachungsmaßnahmen (…) von deutlich geringerer Schwere". Da die Daten bei demjenigen privaten Anbieter verblieben, zu dem der Einzelne auf Grund des bestehenden Vertragsverhältnisses ein vorauszusetzendes Grundvertrauen habe. Daher fehle es, wenn ein nach dem Stand der Technik mögliches, angemessenes Niveau der Datensicherheit gewährleistet werde an einer objektivierbaren „Grundlage für die Annahme eines eingriffsintensivierenden Einschüchterungseffekts oder eines (…) ‚Gefühls des ständigen Überwachtwerdens'". *Schluckebier* betont auch, dass die Speicherung nicht heimlich erfolge, „sondern auf Grund bekanntgemachten Gesetzes". Auch die Möglichkeit, aus den Daten Bewegungsbilder oder Sozialprofile zu erstellen, betreffe nicht die Verhältnismäßigkeit der Speicherung, sondern allein die der Zugriffsregelungen. Danach bliebe der Eingriff durch die Speicherungsverpflichtung auf Grund der Speicherung beim privaten Anbieter beschränkt, er könne lediglich als „besonders gewichtig" charakterisiert werden.[948]

Diese Sichtweise trennt strikt zwischen dem Eingriff durch die Speicherungsverpflichtung und dem Eingriff durch die Verwendung der Daten. Dies entspricht aber zum einen nicht den Bedingungen einer digitalen Datenverarbeitung und widerspricht darüber hinaus der Tatsache, dass gerade bei der Vorratsdatenspeicherung diese scharfe Trennung nicht möglich ist: Würde man sie annehmen, wäre die Speicherung an sich verfassungswidrig, da sie erst durch die Regelung des Zugriffs einem Verwendungszweck zugeführt wird. Es besteht insofern ein innerer Zusammenhang zwischen der Speicherung und der Verwendung.

Schon deshalb ist die Annahme der Senatsmehrheit folgerichtig, dass sich die Verwendungsmöglichkeiten auf das Eingriffsgewicht auswirken. Dafür spricht auch, was schon das *Bundesverfassungsgericht* im Volkszählungsurteil im Jahr 1983 grundsätzlich festgestellt hat: Entscheidend ist nicht allein die Art der Angaben, sondern „ihre Nutzbarkeit und Verwendungsmöglichkeit. Diese hängen einerseits von dem Zweck, dem die Erhebung dient, und andererseits von den der Informationstechnologie eigenen Verarbeitungsmöglichkeiten und Verknüpfungsmöglichkeiten ab. Dadurch kann ein für sich gesehen belangloses Datum einen neuen Stellenwert bekommen."[949] Mit der Mehrheit der Richter ist daher schon in der Speicherungsverpflichtung ein besonders schwerer Grundrechtseingriff zu sehen.

Ebenfalls nicht zu folgen ist der in der Literatur geäußerten Kritik (unter Hinweis auf die Entscheidung des *Bundesverfassungsgerichts* zum Luftsicherheitsgesetz[950]), dass die Annahme, dass die große Streubreite der Maßnahme den Eingriff intensiviere, nicht nachvollziehbar sei. Es wird argumentiert, dass ein Eingriff schwerer wiege, wenn nur ein Einzelner betroffen ist, es sich um ein Sonderopfer handle.[951] Für die Intensivierung des Eingriffsgewichts durch eine hohe Streubreite spricht jedoch, dass die

---

947 BVerfGE 125, 260 (364 ff. *Schluckebier*; 380 ff. *Eichberger*); vgl. dazu auch schon oben S. 158 ff.
948 BVerfGE 125, 260 (367); *Gercke,* in: *Roggan* 2006, S. 177.
949 BVerfGE 65, 1 (45).
950 BVerfGE 115, 118 (136).
951 *Cornils*, Jura 2010, 443, 447; in diesem Sinne auch *Bull* 2011, 98.

Grundrechtsbeeinträchtigung vervielfacht wird und eben diese ein Gefühl des Überwachtwerdens erzeugt und damit die einschüchternde Wirkung verursacht.[952] Während der Eingriff beim Einzelnen auf einer individuellen Entscheidung beruht, erfolgt eine infrastrukturelle Erfassung gerade ohne Bezug zum Verhalten des Einzelnen. Insofern gilt eben nicht, dass wer sich nichts zu Schulden kommen lässt, auch dem Grunde nach keine staatlichen Eingriffe fürchten muss.

Sodann wird dargelegt, dass die Argumentation des Verfassungsgerichts jener aus dem Kfz-Kennzeichenscanning widerspreche. Dort hatte das Gericht angenommen, dass kein Eingriff vorliege, wenn die Daten unmittelbar gelöscht würden.[953] Allerdings widerspricht eben dieses Judikat mit der Annahme, dass dann, wenn Daten unmittelbar gelöscht werden, kein Eingriff vorliege,[954] dem informationellen Selbstbestimmungsrecht, wie es in der Verfassungsdogmatik herausgebildet wurde. Ein Eingriff liegt in jeder Erhebung, Verarbeitung und Nutzung – selbst dann, wenn die Daten nur für einen minimal kurzen Zeitraum gespeichert werden, die Verarbeitung nur automatisiert abläuft und keine öffentliche Stelle davon Kenntnis erlangt. Daher liegt auch wenn Telekommunikationsverkehrsdaten überwiegend ungenutzt wieder gelöscht werden, bereits in der Speicherungsverpflichtung ein Eingriff in das Telekommunikationsgeheimnis.

Es wird des Weiteren kritisiert, dass das Gericht Rechtsgut bezogene Eingriffsermächtigungen für das präventiv-polizeiliche Vorgehen fordert, da das Wesen der Gefahrenabwehr, neben dem Rechtsgüterschutz auch die Rechtsdurchsetzung sei. Diese erfasst auch die Abwehr von Gefahren für die Unversehrtheit der Rechtsordnung. Eine straftatenbezogene Fassung polizeilicher Eingriffstatbestände sei daher unter rechtsstaatlichen Gesichtspunkten verzugswürdig, da sie der Polizei weitaus operablere Kriterien für die Beantwortung der Frage an die Hand gebe, wann ein zum Eingriff berechtigender Verstoß gegen die öffentliche Sicherheit vorliegt. Es handle sich daher bei der Forderung nach einer auf das Rechtsgut bezogenen Regelung um einen nicht gerechtfertigten Eingriff in die Gestaltungsfreiheit des Gesetzgebers.[955]

Darüber hinaus hat die Annahme des Gerichts, dass die Zweckbindung der Verwendungsregelungen auf die Speicherung zurückwirke viel Kritik geerntet. [956] Der 2. März

---

[952] Kritisch dazu, insbesondere zum Wechsel vom Individualschutz zu einem Schutz der Allgemeinheit, *Bull* 2011, 64.

[953] Vgl. Nachw. in Fn. 951.

[954] BVerfGE 120, 378 (399) „Andererseits begründen Datenerfassungen keinen Gefährdungstatbestand, soweit Daten unmittelbar nach der Erfassung technisch wieder spurenlos, anonym und ohne die Möglichkeit, einen Personenbezug herzustellen, ausgesondert werden. Zu einem Eingriff in den Schutzbereich des Rechts auf informationelle Selbstbestimmung kommt es daher in den Fällen der elektronischen Kennzeichenerfassung dann nicht, wenn der Abgleich mit dem Fahndungsbestand unverzüglich vorgenommen wird und negativ ausfällt (sogenannter Nichttrefferfall) sowie zusätzlich rechtlich und technisch gesichert ist, dass die Daten anonym bleiben und sofort spurenlos und ohne die Möglichkeit, einen Personenbezug herzustellen, gelöscht werden".

[955] *Möstl*, DVBl. 2010, 808, 812.

[956] *Eckhardt/Schütze*, CR 2010b, 225, 226 ff.; *Forgó/Krügel*, K&R 2010, 217; *Klesczewski,* JZ 2010, 629.

2010 sei „ein schwarzer Tag für den Datenschutz"[957] Andere deuten die Feststellung der grundsätzlichen Verfassungskonformität einer Vorratsdatenspeicherung als „Erosion des Fernmeldegeheimnisses"[958] und verweisen auf die „Gefahr, dass zukünftig auch Inhalte vorsorglich zu speichern sein könnten".[959]

In Frage gestellt wurde auch die Feststellung des Gerichts, dass es „maßgeblich" für die Rechtfertigungsfähigkeit sei, dass die Speicherung nicht unmittelbar durch den Staat, sondern durch die privaten Anbieter erfolge. Denn, so wird argumentiert, seien es doch gerade die großen Telekommunikationsunternehmen, die in den letzten Jahren durch Nichteinhaltung fundamentaler Datensicherheitsbestimmungen aufgefallen sind.[960] Auch wurde darauf hingewiesen, dass die privaten Anbieter nicht unmittelbar an die Grundrechte gebunden seien und die Durchsetzungsmechanismen hier mangelhaft wären.[961]

In Bezug auf die Verpflichtung der Unternehmen wurde auch die Annahme des Verfassungsgerichts, dass die Kostenübertragung grundsätzlich gerechtfertigt sei, kritisch hinterfragt.[962]

Neben dem Datenschutz wird die Demokratie als Verlierer ausgemacht.[963] Andere betonen, dass letztlich die Sicherheit auf Grund Tatsache, dass das Gericht die Regelungen für nichtig erklärt habe, beeinträchtigt werde. Die für die Arbeit der Sicherheitsbehörden besonders wichtigen Daten wären nun nicht mehr verfügbar und eine Sicherheitslücke entstünde.[964]

Nicht unbestritten blieb auch die Feststellung des Gerichts, dass für die Zuordnung von IP-Adressen zu einem Anschluss, also an eine sogenannte mittelbare Nutzung der Verkehrsdaten, geringere Anforderungen zu stellen seien.[965] Ein „nicht intendiertes Nebenprodukt (Auskünfte über IP-Adressen)" würde so zum Hauptanwendungsfall der Vor-

---

957 *Eckhardt/Schütze*, CR 2010b, 225 ff.

958 *Dix*/*Petri*, DUD 2009, 531, 534.

959 *Dix*/*Petri*, DUD 2009, 531, 534.

960 *Forgó/Krügel,* K&R 2010, 217, 219; mit Verweis auf *Kuri* v. 27.5.2008, abrufbar unter: http://heise.de/-210161.html.

961 *Gurlit*, NJW 2010, 1035, 1040.

962 So überzeugend *Klesczewski,* JZ 2010, 629, 630 f.; *Härting*, BB 2010, 839, 840; Dass eine zukünftige Indienstnahme dennoch wegen zu hoher Kosten verfassungswidrig sein könnte, betonen *Hornung*/*Schnabel*, DVBl. 2010, 824, 833; *Eckhardt/Schütze*, CR 2010, 225, 230; *Heun*, CR 2010, 247, 248; a.A: *Westphal*, EuZW 2010, 494, 499.

963 „Einen echten Gewinner gibt es nicht, einen Verlierer schon: die Demokratie. Parlamentarische Gesetzgebung wird erneut ein Stück mehr zum reinen Verfassungsvollzug, statt politischer Gestaltungsakt des unmittelbar demokratisch gewählten Parlaments zu sein. Deutschland ist aber nicht nur ein Rechtsstaat, sondern auch eine Demokratie (Art. 20 II GG)", *Wolff*, NVwZ 2010, 751.

964 *Marlie/Bock*, ZIS 2010, 524, 528; vgl. auch das Sondervotum des Richters *Schluckebier* BVerfGE 125, 260 (364 ff.).

965 „Generell ist die starke Verminderung des Schutzniveaus der verkehrsdatenvermittelten Auskunft bedenklich, da sich Persönlichkeitsprofile auch durch ein Datensammeln im Internet mit anschließender Aufhebung der Anonymität durch eine Bestandsdatenauskunft erstellen lassen", so etwa *Rössel*, ITRB 2010, 74, 77.

ratsdatenspeicherung, obwohl dieses Nebenprodukt die Einführung der Vorratsdatenspeicherung niemals hätte rechtfertigen können.[966]

Kritisch analysiert wurde darüber hinaus ganz grundsätzlich der Ansatz, mit dem das Gericht zur Entscheidung gelangte und insofern der europarechtliche Bezug des Urteils. Mit der Feststellung, dass eine verfassungskonforme Umsetzung der Richtlinie möglich sei und der Nennung der Mindestspeicherfrist von sechs Monaten als verfassungsrechtliche Obergrenze „muten die Ausführungen als diplomatischer Spagat an: Nicht die umstrittene EU-Richtlinie selbst sei das Problem, sondern allein die nationale Umsetzung".[967] Diagnostiziert wird, dass das *Bundesverfassungsgericht* mit dem Ziel einen europarechtlichen Affront durch die Vorlage der Richtlinie wegen verfassungsrechtlicher Bedenken zu vermeiden und um die Entscheidungsgewalt zu behalten, das Urteil in genau dieser Form gefasst habe.[968]

Die Feststellung, dass eine totale Erfassung und Registrierung nicht mit der Identität der Verfassung vereinbar sei, wurde als „Warnschuss" in Richtung Europa ausgelegt.[969] Datenschutz sei „zum Gradmesser für die Belastbarkeit des europäischen Rechtsprechungsverbandes geworden".[970] Das Gericht habe den verbleibenden Spielraum für die Entwicklung grundrechtssichernder Maßnahmen genutzt. Es sei im Hinblick auf das Problem, dass „die Europäisierung des grundrechtlichen Datenschutzes von einer überzeugenden Konzeption noch weit entfernt ist" zu hoffen, dass solche Entscheidungen in Luxemburg Gehör finden.[971]

4.2.4.3 Bewertung

Richtig ist, dass das *Bundesverfassungsgericht* nicht zum Ersatzgesetzgeber werden darf. Die verfassungsrechtlich zugewiesene Aufgabe des *Bundesverfassungsgerichts* ist die juristische Prüfung der Verfassungskonformität und eben nicht Gesetze zu formulieren. Allerdings greift diese Kritik nur, soweit Regelungsmaterie betroffen ist, für die die Verfassung dem Gesetzgeber einen Spielraum zubilligt, das *Bundesverfassungsgericht* diesen verkennt und somit willkürlich nicht unmittelbar aus der Verfassung ableitbare Anforderungen formuliert.

Zutreffend ist die Kritik etwa soweit das *Bundesverfassungsgericht* feststellt, dass exakt sechs Monate die Obergrenze einer zulässigen Speicherungsverpflichtung sei: Warum diese bei genau sechs Monaten und nicht bei sieben liegt, legt das Gericht nicht dar. Ähnlich im Urteil zum Rauchverbot in Gaststätten als das Gericht feststellt, dass, sollte sich der Gesetzgeber für ein eingeschränktes Rauchverbot entscheiden, er Ein-Raum-Lokale unter einer bestimmten Größe auch als Raucherlokale zulassen müsste.[972] Die Nennung der Größe hier, erscheint ebenso wie die Feststellung, dass die

---

966 *Eckhardt*/Schütze, K&R 2010, I.
967 *Störing*, c't 2010, 5.
968 *Störing*, c't 2010, 5; dazu auch *Ohler*, JZ 2010, 626, 627.
969 *Wolff*, NVwZ 2010, 751; so auch *Roßnagel,* DuD 2010, 544.
970 *Gurlit*, NJW 2010, 1035, 1041.
971 *Hornung,* PVS 2012, 377, 399.
972 „Bei der Bestimmung der genauen Voraussetzungen für den Ausnahmetatbestand zugunsten der Kleingastronomie sind die Landesgesetzgeber, weil es um die Ordnung von Massenvorgängen

Obergrenze für die Speicherung der Verkehrsdaten bei exakt sechs Monaten liege,[973] willkürlich. Wie diese konkreten Zahlen aus dem Grundgesetz abgeleitet werden können, ist nicht ersichtlich.

Nicht zutreffend ist die Kritik, das Gericht habe seine Kompetenz überschritten hinsichtlich der übrigen Gestaltungsanforderungen. Sowohl die technischen als auch die verfahrensrechtlichen Anforderungen stehen nicht zur Disposition des Gesetzgebers, sondern sind Folge des besonders schweren Gewichts des Grundrechtseingriffs einer Speicherung sämtlicher Telekommunikationsverkehrsdaten auf Vorrat. Die hohe Eingriffsintensität führt dazu, dass die Anforderungen an die Speicherung und Verwertung der Vorratsdaten besonders stark durch die verfassungsrechtlichen Vorgaben determiniert sind – da sich der Gestaltungsspielraum eben durch die Bindung des Gesetzgebers an die Verfassung verkürzt.

Die Ausführungen des *Bundesverfassungsgerichts* im Urteil zur Vorratsdatenspeicherung beschränken zwar faktisch die Prärogative des Gesetzgebers, allerdings nicht auf Grund von Willkür der Verfassungsrichter, sondern auf Grund des verfassungsrechtlich reduzierten Spielraums. Insofern zeigt sich hier, dass die Verfassung, dem Sicherheitsstreben eindeutige und strikte Grenzen setzt. Auch billigt eben das Grundgesetz dem *Bundesverfassungsgericht* die Letztentscheidungsbefugnis zu und nicht dem Gesetzgeber oder gar der Exekutive. Durch bestimmte technische und organisatorische Maßnahmen kann eine verhältnismäßige Ausgestaltung gefunden werden. Umgekehrt wird ein Ausgleich ohne diese aber nicht gelingen.

Zwar führt dies dazu, dass dem Gesetzgeber nur eine sehr geringe Gestaltungsfreiheit bei der Umsetzung der Vorratsdatenspeicherungsrichtlinie verbleibt.[974] Denn der Beachtung der vom Gericht aufgezeigten Grundrechtssichernden Gestaltungsanforderungen ist deshalb so hoch, da es sich, wie die Senatsmehrheit zutreffend festgestellt hat, um einen besonders schweren Grundrechtseingriff handelt. Der Eingriff wiegt schon deshalb besonders schwer, weil anlasslos personenbezogene Daten eines jeden erhoben und gespeichert werden. Diese können zu umfassenden Bewegungs- und Persönlichkeitsprofilen zusammengeführt werden. Ins Gewicht fällt sodann, dass eine Überwachungsinfrastruktur geschaffen wird, welche einen Einschüchterungseffekt auf die Grundrechtsausübung insgesamt entfalten kann. Denn Telekommunikation ist heute Basis und Bestandteil nahezu sämtlicher Freiheitsrechte.[975]

---

geht, an typisierenden Regelungen nicht gehindert. So lässt sich dem Merkmal des spezifisch getränkeorientierten Angebots der betroffenen Gaststätten dadurch Rechnung tragen, dass Betriebe, für die das Verabreichen zubereiteter Speisen gemäß § 3 GastG erlaubt worden ist, von der Ausnahme nicht erfasst werden. Zur Eingrenzung der Ausnahme auf kleinere Gaststätten ohne abtrennbaren Nebenraum kommt die Festlegung eines Höchstmaßes für die Grundfläche des Gastraums oder die Zahl der für Gäste vorgehaltenen Sitzplätze in Betracht; beide Parameter können auch kombiniert werden.“, BVerfGE 121, 317 (375).

973 BVerfGE 125, 260 (322).

974 Die europarechtlich vorgegebenen Mindestanforderungen, sieht das Gericht als das „Äußerste dessen (…) was das Grundgesetz gerade noch erlaubt“ an, *Hornung,* PVS 2012, 377, 399 m.w.Nachw.

975 Vgl. oben Kap. 2.1.3.4.

Das Gericht erkennt zwar an, dass auf Grund der veränderten gesellschaftlichen und technischen Rahmenbedingungen eine Vorratsdatenspeicherung nicht schlechthin unverhältnismäßig sei. Es macht jedoch zugleich deutlich, dass eine Ausdehnung staatlicher Sicherheits- und Überwachungsmaßnahmen nicht grenzenlos möglich sei – auch nicht über den Umweg Europa.[976] Das Grundgesetz ist mit einer Verabsolutierung des Sicherheitsstrebens nicht vereinbar.

4.2.5 Der politische Diskurs um die Vorratsdatenspeicherung in Deutschland und Europa

Von Beginn an war die Diskussion um die Vorratsdatenspeicherung erhitzt. Ihre Einführung provozierte nicht nur rechtlichen Widerstand, sondern führte zu einer politischen Mobilisierung.[977] So wurde 2005 der Arbeitskreis Vorratsdatenspeicherung gegründet,[978] der bis heute den politischen Prozess aktiv begleitet und immer wieder öffentlichkeitswirksam auf die politische Diskussion einwirkt.

Im Sommer 2010 kündigte die EU-Innenkommissarin *Malmström* an, dass die Vorratsdatenspeicherung umfassend geprüft und unter Umständen auch reformiert werden solle. Die Vorratsdatenspeicherung sei „zu hastig" beschlossen worden.[979]

Im Juni 2010 kam es zu einer Debatte um eine Ausweitung der Vorratsdatenspeicherung. Zwei Abgeordnete der Europäischen Volkspartei[980] gaben die schriftliche Erklärung 29[981] ab. Hinter dem Titel „Schaffung eines europäischen Frühwarnsystems gegen Pädophilie und sexuelle Belästigung" verbirgt sich die Forderung nach einer Speicherung sämtlicher Suchanfragen (in Suchmaschinen im Internet) auf Vorrat.[982] Die Erklärung wurde von der Mehrheit der Mitglieder des Europäischen Parlaments verabschiedet.[983]

Insgesamt rückte mit zunehmender Distanz zu den Terroranschlägen in den USA und Europa die Begründung, dass die Vorratsdatenspeicherung zur Bekämpfung von Kinderpornographie erforderlich sei, ins Zentrum der Argumentation pro Vorratsdaten-

---

976 A.a. und generell kritisch zum Identitätsvorbehalt in der Rspr des *BVerfG v. Bogdandy/Schill,* ZaöRV 2010, 701, 724 f.

977 Ausführlich zur politischen Mobilisierungswirkung der Vorratsdatenspeicherung *Hornung,* PVS 2012, 377, 384 ff.

978 http://www.vorratsdatenspeicherung.de/.

979 *Dülffer,* Zeit Online v. 1.9.2010, abrufbar unter: http://www.zeit.de/digital/datenschutz/2010-09/vorratsdatenspeicherung-malmstroem.

980 http://www.eppgroup.eu/home/de/aboutus.asp.

981 http://smile29.eu/doc/DS29_DE.pdf.

982 Dazu: *Hochstätter,* ZDNet v. 8.6.2010, abrufbar unter: http://www.zdnet.de/sicherheits_analysen_vorratsdatenspeicherung_2_0_eu_will_googles_sucharchive_story-39001544-41532960-1.htm; auf Grund der Undurchsichtigkeit der Kampagne, hatten mehrere Abgeordnete „versehentlich" das Dokument unterzeichnet, da nicht eindeutig aufgeklärt wird, dass eine Vorratsdatenspeicherung begehrt wird, dazu *Twister,* Telepolis v. 6.6.2010, abrufbar unter: http://www.heise.de/tp/r4/artikel/32/32761/1.html.

983 Abl. EU 2010/C 257 E/303 v. 24.9.2010 – Protokoll der Sitzung v. 23.6.2010.

speicherung.[984] Im Bereich der Kinderpornographie könnten etwa 80 Prozent der Delikte nicht mehr bearbeitet werden, weil die Polizei nicht mehr an die Daten käme, meint etwa der Vorsitzende der Deutschen Polizeigewerkschaft.[985] Auch wird vermittelt, dass ein kausaler Zusammenhang zwischen sexuellem Missbrauch von Kindern und digitalen Verbreitungswegen bestünde: Wer mit der notwendigen Gesetzgebung (der Wiedereinführung einer Vorratsdatenspeicherung) warte, ignoriere „unendliches, irreparables und lebenslanges Leid traumatisierter Kinder und Jugendlicher".[986]

Doch die Annahme eines inneren Zusammenhangs zwischen Fällen sexuellen Missbrauchs und modernen Verbreitungsmöglichkeiten, lässt sich nicht nachweisen.[987] Ebenso wenig nachweisbar ist auch die Annahme, dass retrograde Verkehrsdaten die Ermittlungen bei Kinderpornografie erleichtern würden.[988] Vielmehr zeigt etwa eine Studie von White-IT, einem Bündnis aus Opferverbänden, Netzwirtschaft, IT-Industrie, Ermittlungsbehörden und Ärzteverbänden mit dem Ziel, Kinderpornografie im Internet zu bekämpfen,[989] dass die Schwierigkeit auf die Daten zuzugreifen auch in der Zeit bestand, als in Deutschland Telekommunikationsverkehrsdaten auf Vorrat gespeichert wurden. In manchen Regionen dauere die Auswertung bestimmter Funde

---

[984] So etwa der Unionsfraktionschef *Kauder* „Die Unionsfraktionen sind zusammen mit der Bundespolizei und den Landespolizeibehörden der Auffassung, dass wir die Vorratsdatenspeicherung brauchen". Dabei gehe es „gar nicht in erster Linie um Terrorismusbekämpfung, sondern um schwere Kriminalität wie Kinderpornografie"; zitiert nach *dpa*, Zeit Online v. 24.11.2010, abrufbar unter: http://www.zeit.de/politik/deutschland/2010-11/terrorgefahr-deutschland-justiz.

[985] So *Wendt*, Vorsitzender der DPolG: „Bei der Kinderpornografie gibt es mittlerweile erhebliche Einbußen. Schätzungsweise 80 Prozent der Delikte können wir nicht mehr bearbeiten, weil wir nicht an die Daten kommen." *Treichel,* Stern v. 25.11.2010, abrufbar unter: http://www.stern.de/panorama/teenager-morde-in-bodenfelde-ermittlungen-im-internet-fuehrten-zu-jan-o-1627601.html.

[986] So etwa der schleswig-holsteinische Innenminister *Schlie,* vgl. *Krempl,* heise online v. 2.11.2010, abrufbar unter: http://www.heise.de/-1129498.html. In diesem Sinne fordert auch die bayrische Staatsministerin für Justiz und Verbraucherschutz *Merk* die Wiedereinführung der Vorratsdatenspeicherung, da es für die effektive Bekämpfung von Cybergrooming erforderlich sei, dass die Verbindungsdaten gespeichert werden, *Merk,* FAZ v. 2.11.2010, abrufbar unter: http://www.faz.net/s/Rub475F682E3FC24868A8A5276D4FB916D7/Doc~EBE72B64610D641E2BBA42153A77FF510~ATpl~Ecommon~Scontent.html; auch der Präsident des *BKA Ziercke* erklärte im September 2010, dass 60 Prozent der Internet-Ermittlungen mangels Vorratsdatenspeicherung ins Leere liefen, 2/3 der unbeantworteten Anfragen habe Kinderpornographie zum Gegenstand; zitiert nach *Wilkens,* heise online v. 6.9.2010, abrufbar unter: http://www.heise.de/-1073196.html.

[987] *Albrecht/Kilchling* legen dar, dass im Bereich der Ermittlungen von Kinderpornographie zwar von Seiten der Ermittler ein großes Interesse an den Daten bestünde, „über den Zufall hinaus" könne aber mit der VDS Kinderpornografie nicht verhindert werden (S. 222). Sie fragen so auch, ob die hier verausgabten Mittel nicht besser in andere Maßnahmen zur Prävention von Kinderpornographie investiert werden sollten, *Albrecht/Kilchling* 2011, 221.

[988] Ausführlich dazu und zur Auswertung vorhandener Studien und Fälle *Albrecht/Kilchling* 2011, 94 ff.

[989] http://www.whiteit.de.

und Kontakte bis zu zwei Jahren, so dass auch die sechsmonatige Speicherung der Verkehrsdaten hier nicht weiter geholfen habe.[990]

Die politische Diskussion um eine Wiedereinführung der Vorratsdatenspeicherung trat innerhalb der Bundesrepublik als Koalitionsstreit zu Tage.[991] Während durch die Union (dabei insbesondere durch die unionsgeführten Innenministerien) konstant die Wiedereinführung gefordert wurde,[992] widersetzte sich dem das FDP geführte Justizministerium. Anders als die Innenminister, die immer wieder auf das Bestehen erheblicher Schutzlücken verweisen,[993] vertrat das Justizministerium die Ansicht, dass die bei den Telekommunikationsdiensteanbietern vorhandenen Daten genügten.[994] Die FDP sprach sich wiederholt für ein „Quick Freeze" als „verfassungskonforme Alternative zur Vorratsdatenspeicherung" aus.[995]

Im November 2010 sprach der Bundesinnenminister *De Maiziere* eine konkrete Terrorwarnung für Deutschland aus.[996] Mit der Terrorwarnung wurde das Bewusstsein in der Bevölkerung, dass eine akute Bedrohung durch Terrorismus bestehe, geweckt. Diese Situation wurde von Sicherheitspolitikern genutzt, erneut und mit Nachdruck die Einführung der Vorratsdatenspeicherung zu fordern.[997] In der Folgezeit setzte sich der hessische Ministerpräsident *Bouffier* sogar in der Haushaltsdebatte für die Wiedereinführung der Vorratsdatenspeicherung ein.[998] Auch Bundeskanzlerin *Merkel* schaltete

---

990 Die Ergebnisse der Studie belegen vielmehr, dass es zur effektiven Bekämpfung der Verbreitung von Kinderpornographie mehr Beamte braucht und einer besseren Kommunikation zwischen den Behörden, vgl. *Kleinz,* Zeit online v. 25.11.2010, abrufbar unter: http://www.zeit.de/digital/internet/2010-11/kinderpornografie-whiteIT-schuenemann?page=1.

991 *Steinke,* taz v. 5.10.2010, abrufbar unter: http://www.taz.de/1/netz/netzpolitik/artikel/1/eine-frage-der-verunsicherung/.

992 *Krempl,* heise online v. 2.11.2010, abrufbar unter: http://www.heise.de/-1129498.html.

993 *Lutz,* Die Welt v. 3.10.2010, abrufbar unter: http://www.welt.de/politik/deutschland/article10043217/Geheimpapier-enthuellt-die-Machtlosigkeit-des-*BKA*.html; *Ders.* Die Welt v. 9.10.2010, abrufbar unter: http://www.welt.de/print/die_welt/politik/article10169228/Innenminister-klagt-ueber-erhebliche-Schutzluecke.html; dazu auch: *Ehrmann,* heise online v. 2.10.2010, abrufbar unter: http://heise.de/-1100528; zu den vermeintlichen Schutzlücken: *Biermann,* Die Zeit v. 8.10.2010, abrufbar unter: http://www.zeit.de/digital/datenschutz/2010-10/*BKA*-vorratsdaten-panik.

994 *Krempl,* heise online v. 11.10.2010, abrufbar unter: http://www.heise.de/-1105527.html.

995 *Krempl,* heise online v. 10.11.2010, abrufbar unter: http://www.heise.de/-1134049.html.

996 *Musharbash/Gebauer,* Spiegel online v. 17.11.2010, abrufbar unter: http://www.spiegel.de/politik/deutschland/0,1518,729603,00.html.

997 „Wer sich jetzt noch gegen die Vorratsdatenspeicherung wehrt, hat die Bedrohungslage nicht verstanden", sagt etwa der innenpolitische Sprecher der CDU/CSU-Bundestagsfraktion *Uhl*; *Krempl,* heise online v. 18.11.2010, abrufbar unter: http://heise.de/-1138506; ganz anders die Justizministerin, so AFP v. 19.11.2010, abrufbar unter: http://www.zeit.de/politik/deutschland/2010-11/leutheusser-schnarrenberger-vorratsdatenspeicherung-terror; obwohl selbst der damalige Innenminister *De Maiziere* aus, dass es in Zeiten akuter Terrorwarnungen keinen Anlass für politische Schnellschüsse gebe *König,* SZ v. 18.11.2010, abrufbar unter: http://www.sueddeutsche.de/politik/innenministerkonferenz-keine-panik-minister-de-maizire-rueffelt-die-hardliner-1.1025591.

998 *Dpa,* v. 25.11.2010, abrufbar unter: http://www.focus.de/politik/schlagzeilen/nid_58209.html.

sich in den Koalitionsstreit ein und plädierte für die Wiedereinführung einer Vorratsdatenspeicherung.[999]

Die Justizministerin *Leutheusser-Schnarrenberger* konstatierte hingegen in einem Presseinterview: „Für die FDP wird es kein massenhaftes, grundloses Speichern von Daten über Monate geben".[1000] Im Januar 2011 stellte das Justizministerium ein Eckpunktepapier vor zur Einführung eines Quick-Freeze-Verfahrens verbunden mit einer Speicherung der IP-Zugangsdaten beim Internet-Provider für sieben Tage als Alternative zur Vorratsdatenspeicherung vor.[1001] Im Entwurf wird auf Grund der Annahme, dass die bei den Providern zu Rechnungszwecken gespeicherten Daten, auch für Strafverfolgungszwecke ausreichen würden, vorgeschlagen, Polizei und Staatsanwaltschaft Möglichkeit einzuräumen eine Sicherungsanordnung zu erlassen, aufgrund derer die beim Telekommunikationsunternehmen vorhandenen Daten gesichert werden sollen bis ein Richter über den Zugriff auf die Daten entschieden hat. Um Bestandsdatenauskünfte im Internet zu ermöglichen, solle sodann für dynamische IP-Adressen eine eng befristete Verpflichtung zur Speicherung der dynamisch vergebenen IP-Adressen auf Vorrat eingeführt werden.

Der Entwurf des Justizministeriums ist insgesamt auf wenig Zustimmung gestoßen. Gegner der Vorratsdatenspeicherung sahen im Vorschlag des Justizministeriums einen Wortbruch der FDP-Fraktion, da der Vorschlag zwar eine begrenzte, aber dennoch eine Vorratsdatenspeicherung vorsieht.[1002] Ganz anders reagierte die Gewerkschaft der Polizei, deren Sprecher den Vorschlag als untauglich für die Bekämpfung schwerster Kriminalität und als „Augenwischerei" bezeichnete.[1003]

Die Vorratsdatenspeicherung ist nicht nur politischer Streitpunkt und in der Wissenschaft viel beachtet, sie ist auch gesellschaftlich scharf kritisiert worden, was sich schon am Entstehen der Bürgerrechtsorganisation *AK Vorratsdatenspeicherung*, dem durch sie organisierten „Massenverfassungsbeschwerdeverfahren" vor dem *Bundesverfassungsgericht*[1004] und den jährlichen Großdemonstrationen unter dem Titel „Frei-

---

[999] *Fischer,* v. 24.11.2010, abrufbar unter: www.spiegel.de/politik/deutschland/0,1518,730939,00.html.

[1000] *Dapd, v.* 26.11.2010, abrufbar unter: www.spiegel.de/politik/deutschland/0,1518,731267,00.html.

[1001] *FDP* Eckpunktepapier 17.1.2011; zu diesem *Arning/Moos,* ZD 2012, 153 ff

[1002] http://wiki.vorratsdatenspeicherung.de/Wort_halten_FDP. ; http://www.vorratsdatenspeicherung.de/images/brief_bminj_2011-01-17_anon.pdf. Es gebe zudem keine Gründe für die Differenzierung zwischen IP-Daten und Verkehrsdaten. Die Strafverfolgung im Internet sei auch ohne Vorhalten der IP-Adressen möglich; Dazu auch *Breyer* vom AK-Vorrat im Interview: http://www.heise.de/tp/r4/artikel/34/34046/1.html.

[1003] http://www.gdp.de/gdp/gdp.nsf/ID/p110106/$file/p110106Vorratsdatenspeicherung.pdf ; ähnlich auch der Deutsche Richterbund: http://Beck-aktuell.Beck.de/news/vorratsdatenspeicherung-polizei-und-richterbund-kritisieren-bundesjustizministerin.

[1004] Ein Massenverfassungsbeschwerdeverfahren sieht das *BVerfG*G nicht vor. Es handelt sich vielmehr um einzelne Verfassungsbeschwerden zum gleichen Gegenstand und mit gleichem Inhalt, die vertreten durch einen Anwalt gesammelt eingereicht wurden; zur Anzahl der Klagen, vgl. oben S. 153.

heit statt Angst“[1005] zeigt. Dass gesellschaftlich viele Bedenken gegen die Vorratsdatenspeicherung bestehen, belegen auch statistische Untersuchungen, nach denen über 60 Prozent der Bevölkerung eine Vorratsdatenspeicherung ablehnen.[1006]

Immer wieder wird im Zuge neuer gesellschaftlicher Verunsicherungen, wie dem Anschlag des Einzeltäters *Breivik* in Schweden oder dem Bekanntwerden der Existenz der Zwickauer Terrorzelle (Nationalsozialistischen Untergrund, kurz NSU) die Forderung nach einer Neueinführung der Vorratsdatenspeicherung laut.[1007]

Bislang ist weder absehbar, ob und bis wann es einen erneuten Vorschlag für die Umsetzung der Vorratsdatenspeicherung geben wird. Beide Lager nutzen die Vorratsdatenspeicherung, um sich politisch zu profilieren – im Sinne eines Mehr an Sicherheit im Fall von CDU/CSU – im Fall der FDP als Bürgerrechtspartei.

Ebenfalls ist nicht absehbar, ob und gegebenenfalls, in welcher Form die Vorratsdatenspeicherungsrichtlinie überarbeitet werden wird, oder ob und wann der *Europäischer Gerichtshof* über die Vereinbarkeit der Richtlinie mit Gemeinschaftsrecht entscheiden wird. Im Januar 2012 hat der *Irische High Court* eine Beschwerde gegen die Vorratsdatenspeicherungsrichtlinie dem *Europäischer Gerichtshof* wegen Bedenken gegen die Vereinbarkeit der Richtlinie mit Gemeinschaftsgrundrechten vorgelegt.[1008]

4.2.6 Umsetzung der Vorratsdatenspeicherungsrichtlinie in der EU

Da es sich um eine europäische Richtlinie handelt, soll im Folgenden in einem kurzen Überblick der Umsetzungsstand der Vorratsdatenspeicherungsrichtlinie in den anderen europäischen Mitgliedstaaten dargestellt werden.[1009] Die Erkenntnisse beruhen zum

---

[1005] http://de.wikipedia.org/wiki/Freiheit_statt_Angst; 2008 demonstrierten in Berlin über 50.000 Menschen.

[1006] http://www.heise.de/tp/blogs/8/150430 (Studie des Meinungsforschungsinstituts Allensbach im September 2011: demnach lehnen 66 Prozent der Befragten eine Vorratsdatenspeicherung ab); dieses Ergebnis bestätigt auch eine Studie der Bitkom (Januar 2011), S. 42; abrufbar unter: http://www.bitkom.org/files/documents/BITKOM_Publikation_Datenschutz_im_Internet.pdf .

[1007] http://www.focus.de/politik/ausland/terror-in-norwegen/tid-23087/der-fall-anders-behring-breivik-braucht-deutschland-schaerfere-sicherheitsmassnahmen_aid_649447.html; http://www.tagesspiegel.de/politik/wolfgang-bosbach-wir-wissen-zu-wenig-ueber-die-nazizelle /6005584.html; http://www.heise.de/tp/blogs/8/150853.

[1008] Diese beruht auf einer Klage von Digital Rights Irland (Klage v. 14.9.2006, Digital Rights Ireland Ltd. ./. The Minister for Communications, Marine and Natural Resources et al., http://www.mcgarrsolicitors.ie/wp-content/Files/StatementProzent20ofProzent20claim.pdf); dazu: http://www.thejournal.ie/ecj-asked-to-rule-on-mandatory-retention-of-phone-and-internet-data-339434-Jan2012/; Beck-aktuell v. 31.1.2012, Becklink 1018486; Zudem wurde, zwar nicht in Bezug auf die VDS-RL, sondern gegen die erlaubte Speicherung und automatisierte Auswertung von Verkehrsdaten bei der Kommunikation mit Bundesbehörden, gemäß § 5 BSIG, im Januar 2012 Beschwerde beim *EGMR* eingelegt. Die Beschwerdeschrift ist abrufbar unter: http://www.datenspeicherung.de/wp-content/uploads/*EGMR*-Beschwerdeschrift_BSIG_anon.pdf; Auch dieses Verfahren könnte zu einer generellen Bewertung der Vereinbarkeit einer Speicherung und Verwertung von Telekommunikationsverkehrsdaten führen, die auch Schlüsse auf die Bewertung einer Vorratsdatenspeicherung im Sinne der VDS-RL zu lassen würde.

[1009] Eine umfassende Darstellung zum Umsetzungsstand findet sich bei Roßnagel/Schweda/Moser-Knierim, 2013, 25 ff., Steckbriefe zur Umsetzung in den einzelnen Mitgliedstaaten, S. 191 ff.

einen auf dem Evaluationsbericht zur Vorratsdatenspeicherungsrichtlinie der Europäischen Kommission[1010] und zum anderen auf den Erkenntnissen einer rechtsvergleichenden Untersuchung, die im Rahmen des Forschungsprojekts INVODAS[1011] durchgeführt wurde. Nach den Vorgaben der Vorratsdatenspeicherungsrichtlinie sollte der Kommissionsbericht zur Evaluation der Richtlinie schon im September 2010 vorliegen.[1012] Das Erscheinen des Berichts wurde zunächst auf Ende des Jahres verschoben.[1013] Schließlich erschien der Bericht erst im April des Jahres 2011.[1014]

Die Richtlinie wurde nicht in allen europäischen Staaten, trotz bestehender Umsetzungspflicht und zum Teil bereits erfolgter Verurteilungen durch den *Europäischer Gerichtshof*,[1015] umgesetzt.[1016] Zuletzt wurde in Schweden die Einführung der Vorratsdatenspeicherung beschlossen.[1017] Bis März 2012 hatte sich das Land geweigert, eine Verpflichtung zur anlasslosen Speicherung der Telekommunikationsverkehrsdaten aller Bürger einzuführen.[1018] Am 30.5.2013 wurde Schweden vom Europäischen Gerichtshof wegen der verspäteten Umsetzung zu einer Strafzahlung in Höhe von 3 Millionen Euro verurteilt.[1019] Auch gegen Österreich und Deutschland sind Verfahren anhängig. In Österreich trat eine Regelung zur Vorratsdatenspeicherung erst zum 1. April 2012 in Kraft.[1020]

[1010] KOM (2011) 225.

[1011] Hier wurde eine rechtsvergleichende Untersuchung durch durch das Institut für Europäisches Medienrecht (EMR, Saarbrücken) durchgeführt. Erste Erkenntnisse daraus wurden in *Schweda* SIRA 2011, 56 (S. 60 mit näheren Informationen zum Forschungsprojekt) veröffentlicht ; der gesamte Forschungsbericht wurde publiziert in: *Roßnagel/Moser-Knierim/Schweda* 2013.

[1012] Art. 14 Abs. 1 VDS-RL.

[1013] *Twister,* telepolis v. 23.9.2010, abrufbar unter: http://www.heise.de/tp/r4/artikel/33/33340/1.html.

[1014] vgl. Fn. 869.

[1015] Verurteilungen durch den *EuGH* erfolgten gegen Schweden und Österreich. *EuGH*, Urt. v. 4.2.2010, Kommission ./. Schweden, Rs. C-185/09; *EuGH* Urt. v. 29.7.2010 Kommission / Österreich, Rs. C-189/09.

[1016] Eine zumindest zeitweise Umsetzung bestand jedenfalls in 24 der 26 Mitgliedstaaten, *Schweda,* SIRA 2011, 56, 64 – mit einer Umsetzung in Schweden ist nun 2012 in 25 der 26 Mitgliedstaaten eine zeitweilige Umsetzung erfolgt.

[1017] *Schweda,* ZD-Aktuell 2012, 02882.

[1018] Die Stellungnahme *Schwedens* ist abrufbar unter: http://www.edri.org/files/sw_C-270-11_slutligt.pdf: in einem zweiten Verfahren fordert nunmehr die Kommission die Festsetzung eines Zwangsgeldes i.H.v. 40.947,20 Euro für jeden Tag der Nichtumsetzung nach dem zweiten Urteil; vgl. Klageschrift v. 31.5.2011, Kommission./. Schweden, Rs. C-270/11.

[1019] https://www.unwatched.org/EDRigram_11.11_Kommission_geht_gegen_Mitgliedslaender_wegen_Nicht-Umsetzung_der_Richtlinie_zur_Vorratsdatenspeicherung_vor.

[1020] Bundesgesetz, mit dem das TKG 2003 geändert wird, BGBl. I Nr. 27/2011 v. 18.5.2011; Bundesgesetz, mit dem die Strafprozessordnung 1975 und das Sicherheitspolizeigesetz geändert werden, BGBl. I Nr. 33/2011 v. 20.5.2011; Österreich war zuvor vom *EuGH* wegen der fehlenden Umsetzung verurteilt worden, *EuGH* Urt. v. 29.7.2010 Kommission / Österreich, Rs. C-189/09; ausführlich zur Umsetzung *Gerhartinger,* MMR-Aktuell 2011, 318504. Gegen das Gesetz plant das Land Kärnten Klage vor dem Verfassungsgerichtshof zu erheben, *Sokolov,* heise online v. 27.3.2012, abrufbar unter: http://www.heise.de/-1484130.html; ausführlich zum Gesetzgebungsverfahren in Österreich *Schweda,* SIRA 2011, 56, 66.

Innerstaatliche Umsetzungen, die zunächst erfolgt waren, wurden neben dem deutschen Urteil,[1021] im Jahr 2008 in Rumänien[1022] sowie im Jahr 2011 in der Tschechischen Republik[1023] von den jeweiligen Verfassungsgerichten für nichtig erklärt.[1024] In Bulgarien wurden im Anschluss an ein Urteil des Obersten Verwaltungsgerichts[1025], in dem insbesondere die Definition der Verwendungszwecke als zu unbestimmt und damit verfassungswidrig beurteilt worden war, die Regelungen überarbeitet. Auch in Zypern hat der Oberste Gerichtshof den Abruf von Verkehrsdaten in mehreren Fällen für verfassungswidrig erachtet.[1026] Das französische oberste *Bundesverfassungsgericht* stellte hingegen fest, dass die französische Umsetzungsregelung verfassungskonform sei.[1027]

Nicht abgeschlossen sind bislang Verfahren in Irland[1028], Polen[1029] und Ungarn.[1030]

Von großer Bedeutung sind vor allem die Vorlagen des Irischen High Courts und des Österreichischen Verfassungsgerichtshofs an den *Europäischen Gerichtshof*. Beide legten Fragen hinsichtlich der Frage der Vereinbarkeit der Vorratsdatenspeicherungsrichtlinie mit der Europäischen Grundrechtecharta vor. Im Juli 2013 fand hier die erste

---

[1021] BVerfGE 125, 260.

[1022] Am 8.10.2009 entschied das rumänische *Bundesverfassungsgericht*, dass das Gesetz Nr. 298/2008, mit dem in dem Land eine Vorratsdatenspeicherung eingeführt worden war, gegen die in der Verfassung verankerten Grundrechte und Art. 8 EMRK nicht vereinbar sei, Verfassungsgerichthof *Rumäniens*, Entscheidung Nr. 1258 v. 8.10.2009, http://www.ccr.ro/decisions/pdf/ro/2009/D1258_09.pdf, deutsche Übersetzung abrufbar unter: http://www.vorratsdatenspeicherung.de/content/view/342/1/lang,de/#Urteil.

[1023] Am 31.3.2011 stellte der Verfassungsgerichtshof der Tschechischen Republik fest, dass Teile der nationalen Regelung zur Vorratsdatenspeicherung die Verfassung verletzen, insbesondere seien sie zu unbestimmt. Der Verfassungsgerichtshof hob die Regelungen auf, Verfassungsgerichtshof der Tschechischen Republik, Urt. v. 22.3.2011, Pl. ÚS 24/10, abrufbar unter: http://www.concourt.cz/clanek/GetFile?id=5075 im tschechischen Original; Eine englische Übersetzung der Leitsätze ist abrufbar unter: http://www.concourt.cz/view/pl-24-10.

[1024] Dazu ausführlich *Schweda,* SIRA 2011, 56, 67 f.

[1025] Bulgarisches Oberstes Verwaltungsgericht, Entsch. Nr. 13627 v. 11.12.2008, Verw.-Rs. Nr. 11799/2008; abrufbar unter: http://www.econ.bg/law86421/enactments/article153902.html. Das Gericht rügte eine Verletzung von Art. 8 EMRK und u.a. von Art. 32 (Recht auf Unverletzlichkeit des persönlichen Lebens) der bulgarischen Verfassung.

[1026] Oberster Gerichtshof Zyperns, Urt. v. 1.2.2011, Zivil-Rs. Nr. 65/2009, 78/2009, 82/2009 und 15/2010-22/2010, abrufbar unter: http://www.supremecourt.gov.cy/judicial/sc.nsf/All/5B67A764B86AA78EC225782F004F6D28/$file/65-09.pdf; 2010 erfolgte eine Verfassungsänderung, die den Verfassungsverstoß behoben haben dürfte, dazu *Schweda* SIRA 20121, 56, 69.

[1027] Verfassungsrat, Entsch. Nr. 2005-532 v. 19.1.2006, http://www.conseil-constitutionnel.fr/conseil-constitutionnel/francais/les-decisions/acces-par-date/decisions-depuis-1959/2006/2005-532-dc/decision-n-2005-532-dc-du-19-janvier-2006.979.html; dazu *Schweda* SIRA 2011, 56, 68.

[1028] Vgl. Fn. 1008.

[1029] Die Verfassungsbeschwerde wurde am 28.1.2011 von einer Gruppe Parlamentsabgeordneter der Sozialdemokratischen Partei Polens beim *Bundesverfassungsgericht* eingereicht. Die Beschwerdeschrift ist abrufbar unter: http://www.sld.org.pl/download/index/biblioteka/393.

[1030] Die Verfassungsbeschwerde wurde am 15.3.2008 von der Hungarian Civil Liberties Union beim *Bundesverfassungsgericht* eingereicht; vgl. http://tasz.hu/en/data-protection/constitutional-complaint-filed-hclu-against-hungarian-telecom-data-retention-regulat.

Verhandlung statt.[1031] Ob der Gerichtshof eine Verletzung der Grundrechtecharta durch die Richtlinie annehmen wird, ist aktuell nicht absehbar. Möglich erscheint dies insbesondere im Hinblick auf den weiten Gestaltungsspielraum den die Richtlinie den Mitgliedstaaten hinsichtlich der Umsetzung in Bezug auf den Umfang der Speicherung, Datenschutz, Zugriffsmöglichkeiten, etc. belässt.

So zeigt auch die Untersuchung der Umsetzungsgesetze in den Mitgliedstaaten, dass hier erhebliche Differenzen bestehen. Dies weckt auch Zweifel an dem Erfolg der anvisierten Harmonisierung.

- Datenkategorien

Zum Teil wurde die Speicherung noch weiterer als von der Richtlinie geforderter Datenkategorien angeordnet. Etwa verlangt die italienische Regelung, dass auch sämtliche beim E-Mail-Versand verwendeten IP-Adressen und die vollen Domain-Namen der E-Mail-Server, die an der Weiterleitung einer E-Mail beteiligt waren, gespeichert werden. Außerdem sind Daten über SMS und MMS, die über das Internet versendet wurden, zu speichern.[1032]

Auch das französische Gesetz verlangt über die Vorgaben der Vorratsdatenspeicherungsrichtlinie hinaus, dass Internetzugangsdienste und Hosting-Dienste die verwendeten Nutzer- und Endgerätekennungen, genauere Informationen zu Verbindungsart, zu Zahlungsvorgängen und schließlich weitere Bestandsdaten (unter anderem das aktuelle Passwort) speichern.[1033]

- Speicherfrist

In sechs Staaten wird bezüglich der Speicherung differenziert zwischen Telefondaten, die jeweils für einen längeren Zeitraum und Daten zu Internetzugang, E-Mail und Internet-Telefonie, die für einen kürzeren Zeitraum zu speichern sind.[1034] Die Mehrzahl der Mitgliedstaaten sieht jedoch einheitliche Fristen vor, wobei die Speicherfristen den gesamten Spielraum der Richtlinie ausnutzen und so zwischen sechs Monaten und zwei Jahren liegen.[1035]

[1031] *Krempl,* heise online v. 9.7.2013, abrufbar unter: http://heise.de/-1914223.

[1032] Art. 3 Gesetzesvertretendes Dekret 109/2008 v. 30.5.2008, "Attuazione della direttiva 2006/24/CE riguardante la conservazione dei dati generati o trattati nell'ambito della fornitura di servizi di comunicazione elettronica accessibili al pubblico o di reti pubbliche di comunicazione e che modifica la direttiva 2002/58/CE", Gazzetta Ufficiale Nr. 141 v. 18.6.2008.

[1033] *Schweda,* SIRA 2011, 56, 72, wohl: Art. 6 II Gesetz Nr. 2004-575 v. 21.6.2004 (Loi *n°2004-575* pour *la confiance dans l'économie numérique)*.

[1034] *Belgien* (wobei hier keine Speicherfrist für Internetdaten festgelegt wurde); *Irland* (Telefon: 2 Jahre/ Internet: 1 Jahr); *Italien*; (2 Jahre/ 1 Jahr); *Malta* (1 Jahr/ 6 Monate); *Slowenien* (14 Monate/ 8 Monate); *Slowakei* (1 Jahr/ 6 Monate); KOM (2011) 225, 17 f.; ausführlich zu den unterschiedlichen Speicherfristen, *Schweda,* SIRA 2011, 56, 70.

[1035] In15 Mitgliedstaaten (Bulgarien, Dänemark, Estland, Griechenland, Spanien, Frankreich, Zypern, Lettland, Litauen, Luxemburg, Niederlande, Polen, Portugal, Finnland, Vereinigtes Königreich) ist

Aufgrund dieser unterschiedlichen Ansätze zur Regelung der Speicherfrist ist innerhalb der Europäischen Union nur eine begrenzte Vorhersehbarkeit geboten. Die Kommission erwägt daher eine weitere Harmonisierung der Speicherungsfristen und dabei auch eine mögliche Differenzierung nach Datenkategorien oder Fristen für bestimmte Straftaten.[1036]

Im Evaluationsbericht der Europäischen Kommission wird auch darauf hingewiesen, dass sich aus den quantitativen Angaben der Mitgliedstaaten ergibt, dass 90 Prozent der Daten bei Abfrage nicht älter als sechs Monate waren und 70 Prozent der Daten nicht älter als drei Monate waren.[1037]

- Adressaten und Kostenerstattung

In Finnland und Österreich wurden nur die Dienstanbieter zur Speicherung verpflichtet, nicht aber die Netzbetreiber.[1038] Damit soll eine Doppelspeicherung vermieden werden. In Großbritannien sind nur die zur Speicherung verpflichtet, die von der Regierung gesondert benachrichtigt werden.[1039] So wurden kleine Anbieter von der Verpflichtung zur Vorratsspeicherung ausgenommen. Auch in Österreich sind kleine Anbieter nicht zur Vorratsdatenspeicherung verpflichtet.[1040]

Dem liegt die Erwägung zu Grunde, dass die mit der Verpflichtung verbundenen Kosten in keinem Verhältnis zu den Vorteilen für die Strafjustizsysteme und die Strafverfolgung stünden.[1041] Auch hier will die Kommission weiter prüfen, wie eine mögliche Änderung des Rechtsrahmens sich auf kleine und mittlere Unternehmen auswirkt.[1042]

Zudem zeigte die Evaluation, dass zum Teil kleine Betreiber von Kommunikationsnetzen die Verpflichtung zur Vorratsspeicherung ausgelagert haben oder Jointventures gebildet haben, um Kosten zu sparen.[1043] Dahinter steht die Problematik, dass die Vorratsdatenspeicherungsrichtlinie eben nicht vorgibt, ob die Kosten die durch die Speicherungspflicht entstehen, den Unternehmen ersetzt werden sollen. In vielen Mitgliedstaaten ist keine Kostenerstattung vorgesehen, während andere eine solche normiert haben.[1044] Dabei fällt auf, dass gerade diejenigen Staaten, die Kosten vollständig oder

---

eine einheitliche Speicherfrist vorgesehen, KOM (2011) 225, 17. Bulgarien hat die Möglichkeit vorgesehen, die Speicherfrist um sechs Monate zu verlängern.

[1036] KOM (2011) 225, 18.
[1037] KOM (2011) 225, 18.
[1038] *Schweda,* SIRA 2011, 56, 75.
[1039] *Schweda,* SIRA 2011, 56, 75.
[1040] *Schweda,* SIRA 2011, 56, 75.
[1041] KOM (2011) 225, 11.
[1042] KOM (2011) 225, 11.
[1043] KOM (2011) 225, 11.
[1044] *Schweda,* SIRA 2011, 56, 76.

zu einem überwiegenden Teil erstatten, auch die Adressaten der Speicherungsverpflichtung begrenzt haben.[1045]

- Datensicherheit

Der Bericht der Kommission ist in Bezug auf den Sicherheitsstandard der auf Vorrat zu speichernden Daten wenig aussagekräftig.[1046] Eine Tabelle gibt lediglich darüber Auskunft, ob die nationalen Gesetze Vorschriften zur Umsetzung der in Art. 7 VDS-RL verankerten Grundsätze beinhalten.[1047] Er enthält aber keine Angaben, durch welche rechtlichen, technischen und organisatorischen Maßnahmen diese Grundsätze umgesetzt werden oder wie hoch der Sicherheitsstandard genau ist, den die nationalen Vorschriften fordern.

Nähere Informationen dazu ergeben sich aus dem Bericht der Artikel-29-Gruppe,[1048] der als Eingabe Eingang in den Kommissionsbericht gefunden hat.[1049] Hier zeigt sich deutlich, dass zwar viele Staaten organisatorische Maßnahmen vorgesehen haben, aber insgesamt keineswegs ein einheitlich hoher Sicherheitsstandard gewährt wird.

Ein besonders hoher Sicherheitsstandard, wie ihn das *Bundesverfassungsgericht* für die Speicherung der Telekommunikationsverkehrsdaten auf Vorrat aus Gründen der Verhältnismäßigkeit fordert,[1050] ist in keinem der Mitgliedstaaten vorgeschrieben.[1051]

Doch auch die Kommission verweist in ihrem Bericht darauf, dass auf Grund der hohen Schutzwürdigkeit der Daten ein hoher Datenschutz- und -sicherheitsstandard zu beachten sei. Sie beabsichtigt daher „Optionen zur Verbesserung von Datensicherheit- und Datenschutzstandards einschließlich Lösungen mit eingebautem Datenschutz (Privacy by Design)“ zu prüfen.[1052] Allerdings wurde bislang von der Kommission noch kein Vorschlag für eine Neufassung der Richtlinie vorgelegt.

[1045] So werden in Finnland, Großbritannien und Österreich die erforderlichen Investitionskosten vollständig (bzw. in Österreich zu 80 Prozent) ersetzt. Auf diese Weise kann sichergestellt werden, dass es trotz er Beschränkung der Speicherungspflicht auf einige wenige Unternehmen, nicht zu Wettbewerbsverzerrungen kommt, *Schweda,* SIRA 2011, 56, 76

[1046] Nähere Informationen zum Stand der Datensicherheit finden sich bei *Schweda,* SIRA 2011, 56, 77 f.

[1047] Art. 7 VDS-RL verlangt, a) einen gleichen Schutz wie im öffentlichen Kommunikationsnetz vorhandene Daten; b) geeignete technische und organisatorische Maßnahmen zum Schutz der Daten gegen Zerstörung, Verlust, Änderung, Missbrauch; c) geeignete Maßnahmen um den Zugang auf bestimmte ermächtigte Personen zu beschränken; d) Löschung der Daten am Ende der Speicherfrist.

[1048] *Art. 29 DP WP*, v. 13 July 2010, WP 172.

[1049] KOM (2011) 225, 2

[1050] BVerfGE 125, 260 (325); ausführlich zur verfassungsrechtlich erforderlichen Datensicherheit auch unten S. 345 ff.

[1051] Vgl. zu diesen Anforderungen im Urteil des *BVerfG*, oben S. 156 ff.; ausführlich dazu auch unten Kap. 9.1.2.1.3.1 u. Kap. 10.1.5.

[1052] KOM (2011) 225, 22.

- Verwendungszwecke und Datenabruf

Zum Teil erfolgt die Speicherung ausschließlich zu Strafverfolgungszwecken, allerdings können die Daten vielfach später trotzdem für andere Zwecke verwendet werden.[1053]

In anderen fehlt es vollkommen an einer Bestimmung der Zwecke im Zuge der Speicherungsverpflichtung.[1054]

Neben diesen Unterschieden bei der Zweckbestimmung der Speicherung treten deutliche Unterschiede bei den Ermächtigungen zum Datenabruf zu Tage: So ist etwa der Zugriff auf die Daten nach den ungarischen Regelungen nahezu keinen Einschränkungen unterworfen.[1055] Auch im Vereinigten Königreich sind die Straftaten zu deren Ermittlung, Feststellung und Verfolgung auf die Daten zugegriffen werden kann nicht näher beschränkt.[1056]

In vielen Mitgliedstaaten ist der Zugriff allerdings auf die Verfolgung schwerer Straftaten begrenzt. Wann eine schwere Straftat vorliegt, wird jedoch sehr unterschiedlich bestimmt. Zum Teil ist die Voraussetzung an einen Straftatenkatalog geknüpft.[1057] In anderen Staaten wird ein bestimmter Strafrahmen zu Grunde gelegt.[1058] Schließlich wird zum Teil an vorgegebene Mindeststrafen angeknüpft.[1059]

Insgesamt ergibt sich das Bild, dass auf die Vorratsdaten in der Mehrzahl der Mitgliedstaaten auch über die Anforderungen der Richtlinie (Zugriff zur Verfolgung schwerer Straftaten insbesondere des internationalen Terrorismus) hinaus zugegriffen werden darf. Die Europäische Kommission ist der Ansicht, dass dies auch mit der Datenschutzrichtlinie zu vereinbaren sei.[1060]

In allen Mitgliedstaaten, in denen die Richtlinie umgesetzt wurde, hat die nationale Polizei Zugriff auf die Daten. Außer in den Niederlanden und dem Vereinigten Königreich sind auch die Staatsanwaltschaften zugriffsberechtigt.[1061] Vierzehn Mitgliedstaaten ermächtigen darüber hinaus noch Sicherheits- und Geheimdienste oder das Militär

[1053] So etwa in Luxemburg und Rumänien. Strikte Begrenzungen auf die Zwecke der Ermittlung, Feststellung und Verfolgung von Straftaten enthalten dagegen die Umsetzungsnormen in Dänemark, Italien, Litauen, Portugal, der Slowakischen Republik und Zypern; ausführlich zur Zweckbestimmung von Datenspeicherung und Abruf, *Schweda,* SIRA 2011, 56, 78 f. mit zahlreichen Nachweisen.

[1054] So etwa in Estland, in der Tschechischen Republik und im Vereinigten Königreich.

[1055] Hier muss der Zugriff auf die Vorratsdaten durch die berechtigten Behörden, nur „zur Erfüllung ihrer Aufgaben" erforderlich sein (vgl. Art. 159/A Gesetz über elektronische Kommunikation).

[1056] *Schweda* SIRA 2011, 56, 79 Fn. 71 m.w.Nachw.

[1057] So etwa die mittlerweile für nichtig erklärte rumänische Regelung.

[1058] So etwa in den Niederlanden.

[1059] So in Malta, Dänemark und Litauen.

[1060] KOM (2011) 225, 10.

[1061] KOM (2011) 225, 11.

zum Zugriff.[1062] Steuer- und/oder Zollbehörden wird in sechs Mitgliedstaaten[1063] Zugriff auf die Daten gewährt. Grenzkontrollbehörden sind in drei Staaten[1064] ermächtigt die Daten abzurufen.

Der Zugang zu den Daten ist in den Mitgliedstaaten unterschiedlich organisiert.[1065] Die Prüfung durch einen Richter bevor die Daten verwendet werden dürfen, ist in einer Vielzahl der Mitgliedstaaten[1066] vorgesehen. Eine Genehmigung durch die Staatsanwaltschaft oder eine andere übergeordnete Behörde genügt in anderen Mitgliedstaaten.[1067] Allein in Irland und Malta genügt allein lediglich ein schriftlicher Antrag.[1068]

Auch hier hat die Kommission angekündigt zu prüfen, ob in diesem Bereich eine stärkere Harmonisierung erforderlich ist. Denn davon ausgeht, dass sich unterschiedliche Zwecke auf den Umfang und die Häufigkeit der Anfragen auswirken und damit auch auf die entstehenden Kosten.[1069]

Die Betrachtung der Umsetzung der Vorratsdatenspeicherungsrichtlinie zeigt, dass ein einheitliches System der Vorratsdatenspeicherung in Europa auch sieben Jahre nach Verabschiedung der Richtlinie nicht erreicht wurde.[1070] Die Harmonisierung ist insoweit bislang nicht geglückt.[1071]

4.3 Verfassungsrecht im Spannungsfeld mit Völker- und Europarecht

In der historischen Entwicklung wurde deutlich, dass Der Blick auf die Einführung der Vorratsdatenspeicherung in Deutschland hat gezeigt, dass sämtliche nationalen Vorhaben zur Einführung einer umfassenden Verpflichtung zur Speicherung von Telekommunikationsverkehrs- und -bestands Daten auf Vorrat gescheitert waren.[1072] Erst unter

---

[1062] Nationale Sicherheitsdienste und/bzw. Geheimdienste sind zugriffsberechtigt in Bulgarien, Spanien, Lettland, Litauen, Luxemburg, Malta, Polen, Portugal, Slowenien und im Vereinigten Königreich. Dem Militär ist ein Zugriffsrecht eingeräumt, in Irland, Griechenland, Luxemburg, Polen, Portugal und in Slowenien.

[1063] Irland, Spanien, Ungarn, Polen, Finnland und das Vereinigtes Königreich.

[1064] Estland, Polen und Portugal.

[1065] Eine Übersicht dazu findet sich KOM (2011) 225, 12 ff.

[1066] Bulgarien, Dänemark, Estland, Griechenland, Spanien, Litauen, Luxemburg, Portugal, Slowenien und für andere als Teilnehmerdaten auch in Finnland. In Belgien und den Niederlanden ist eine richterliche oder eine staatsanwaltliche Genehmigung erforderlich. In Zypern kann eine entsprechende richterliche Anordnung erlassen werden, es genügt aber auch eine staatsanwaltschaftliche Genehmigung.

[1067] In Frankreich durch eine von der Commission nationale de Controle des Interceptions de Sécurité benannte Person im Innenministerium; in Italien, Zypern, Ungarn und Polen durch den leitenden Beamten der jeweiligen Organisation; die Regelung im Vereinigten Königreich verlangt lediglich eine benannte Person.

[1068] KOM (2011) 225, 12.

[1069] KOM (2011) 225, 10 Zudem würde möglicherweise die Vorhersehbarkeit beeinträchtigt, die aber für jede gesetzgeberische Maßnahme, die das Recht auf Privatsphäre einschränkt.

[1070] Ausführlich zu den Defiziten und der aktuellen Diskussion auf europäischer Ebene, *Schweda,* SIRA 2011, 56, 83 ff.

[1071] Vgl. dazu schon oben Fn. 919.

[1072] Vgl. oben S. 150 ff.

dem Druck der Verpflichtung zur Umsetzung durch die Europäische Vorratsdatenspeicherungsrichtlinie erfolgte die Einführung in deutsches Recht.

Wie weit diese Pflicht reicht und inwiefern Europäisches Sekundärrecht das Verfassungsrecht der Bundesrepublik Deutschland verdrängt, wird im Folgenden erörtert (Kap. 4.3.1). Sodann wird der Frage nachgegangen, ob neben der Umsetzungspflicht aus der Vorratsdatenspeicherungsrichtlinie eine völkerrechtliche Verpflichtung zur Einführung einer Vorratsdatenspeicherung besteht (Kap.4.3.2).

4.3.1 Europarechtliche Verpflichtung zur Umsetzung der Vorratsdatenspeicherungsrichtlinie

Die Verpflichtung der Mitgliedstaaten zur Einführung einer Vorratsspeicherung der Telekommunikationsverkehrsdaten sämtlicher Bürger wurde in Gestalt einer Richtlinie eingeführt. Während Verordnungen allgemein und unmittelbar in den Mitgliedstaaten gelten, richten sich Richtlinien an die Mitgliedstaaten und sind insofern nicht unmittelbar anwendbar. Sie sind für die Mitgliedstaaten hinsichtlich des zu erreichenden Ziels verbindlich.[1073] Die konkrete Umsetzung, also insbesondere die Wahl von Form und Mittel der Umsetzung in nationales Recht, bleibt dabei der Entscheidung der Mitgliedstaaten überlassen. Richtlinien spiegeln insofern den, in der *Europäischen Union* als Staatenverbund erforderlichen, Kompromiss zwischen dem Bedürfnis einer Rechtsangleichung und dem Respekt vor nationalen Eigenheiten.[1074]

Wenn die Mitgliedstaaten der unionsrechtlichen Verpflichtung der Umsetzung von Richtlinien nicht nachkommen, können sie im Rahmen eines Vertragsverletzungsverfahrens vor dem *Europäischen Gerichtshof* verklagt werden.[1075] Dieser kann als Zwangsmittel ein Zwangsgeld oder einen Pauschbetrag festsetzen, wenn ein verurteilter Mitgliedstaat seiner Verpflichtung aus dem Urteil nicht nachkommt.[1076] So wurden Österreich und Schweden bereits wegen fehlender Umsetzung der Vorratsdatenspeicherungsrichtlinie vom *Europäischen Gerichtshof* wegen Nichtumsetzung verurteilt.[1077] Auch gegen Deutschland hat die Europäische Kommission ein Vertragsverletzungsverfahren eingeleitet.[1078]

Deutschland ist grundsätzlich zur Umsetzung der Vorratsdatenspeicherungsrichtlinie verpflichtet. Selbst nationales Verfassungsrecht wird durch europäisches Sekundärrecht überlagert. Der *Europäische Gerichtshof* hat bereits frühzeitig in seiner Rechtsprechung den Vorrang des Gemeinschaftsrechts betont und zwar auch vor nationalem

---

[1073] Art. 288 AEUV (ex-Art. 249 EGV).
[1074] *Härtel* 2006, 173.
[1075] Art. 258, 259 AEUV (ex-Art. 226, 227 EGV).
[1076] Art. 260 Abs. 2 AEUV, ex-Art. 228 EGV.
[1077] Vgl. Fn. 1015; Im Urteil gegen *Schweden*, sah der EuGH von der Festsetzung einer Geldbuße ab, dazu *Krempl,* heise online v. 6.2.2010, abrufbar unter: http://heise.de/-923756; Die Kommission forderte in einem zweiten Verfahren die Festsetzung einer Geldbuße in Höhe von 9.597 € für den Zeitraum zwischen erstem und zweiten Urteil und die Festsetzung eines Zwangsgeldes i.H.v. 40.947,20 € für jeden weiteren Tag der Nichtumsetzung, *Schweda* 2011, 56, 65.
[1078] *Wilkens,* heise online v. 27.10.2011, abrufbar unter: http://heise.de/-1367618; auch gegen Rumänien wurde das Verfahren eingeleitet.

Verfassungsrecht.[1079] Das *Bundesverfassungsgericht* hat zwar bis heute keinen absoluten Vorrang des Gemeinschaftsrechts anerkannt, jedoch hat es mit der Solange II-Rechtsprechung seine Jurisdiktionsgewalt stark eingeschränkt und europäischem Sekundärrecht weitgehend Vorrang vor nationalem Recht eingeräumt. Das *Bundesverfassungsgericht* hat hier festgestellt, dass es deutsche Gesetze nicht am Maßstab der Grundreche überprüfen werde, wenn sie durch (sekundäres) Europarecht zwingend vorbestimmt sind. Einschränkend betont es, dass dies nur solange gelte als auf europäischer Ebene ein Grundrechtsschutz generell gewährleistet sei, der im Wesentlichen dem Standard entspreche, den das Grundgesetz unabdingbar vorgibt.[1080] Entsprechend hat das *Bundesverfassungsgericht* daraufhin im Bananenmarkt-Beschluss festgestellt, dass wenn eine Verfassungsbeschwerde darauf zielt, die Rechtswidrigkeit einer europäisch vorgegeben Norm festzustellen, der Beschwerdeführer darzulegen habe, dass der unabdingbar gebotene Grundrechtsschutz auf europäischer Ebene generell nicht mehr gewährleistet sei.[1081] Lediglich für den Fall von Kompetenz-Überschreitungen (Ultra-Vires) hat sich das Verfassungsgericht stets die Prüfungskompetenz vorbehalten.[1082] Zudem hat es den Prüfungsvorrang des *Europäischen Gerichtshofs* unter den Vorbehalt der Wahrung der Verfassungsidentität gestellt.[1083] Von dieser strikten Beschränkung seiner Prüfungskompetenz auf wenige Ausnahmefälle ist das *Bundesverfassungsgericht* nun im Urteil zur Vorratsdatenspeicherung abgerückt.[1084]

Denn das Gericht prüft, ob eine Umsetzung der Richtlinie verfassungskonform möglich wäre. Es hätte sich nach der Solange-Doktrin aber allein auf das Wie beschränken müssen. Daran zeigt sich, wie *Bäcker* zutreffend feststellt, dass das *Bundesverfassungsgericht* den Solange II-Vorbehalt nicht (mehr), wie lange vermutet bei der Prüfungskompetenz verortet, sondern bei der Verwerfungskompetenz.[1085] Dies hat zur Folge, dass Verfassungsbeschwerden gegen europarechtlich determiniertes deutsches Recht zukünftig nicht ohne nähere Prüfung als unzulässig abgewiesen werden können.[1086]

[1079] *EuGH,* Urt. v. 15.7.1964, *Costa./. E.N.E.L.*, Rs. 6-64; Urt. V. 17.12.70, Rs. 11/70, Slg. 1970, 1125, *Internationale Handelsgesellschaft.*

[1080] BVerfGE 73, 339; so dann auch im Maastricht-Urteil, BVerfGE 89, 155 (174 f.); diese Rspr erstreckte sich zunächst nur auf Verordnungen, im Emissionshandel-Beschluss hat das *BVerfG* dann festgestellt, dass sich die Solange II-Rechtsprechung auch Richtlinien erfasse, BVerfGE 118, 79 (95 ff.). Demnach sind die Fachgerichte verpflichtet das Umsetzungsgesetz anhand der europäischen Grundrechte zu prüfen, ggf. müssten sie ein Vorabentscheidungsverfahren nach art. 267 AEUV durchführen. Erst wenn der *EuGH* daraufhin eine Richtlinie für ungültig erklärt hat, kann das Gericht das Umsetzungsgesetz anhand der deutschen Grundrechte prüfen.

[1081] BVerfGE 102, 147 (162 ff.).

[1082] BVerfG 2 BvR 2661/06 - Beschluss v. 6.7.2010, Rn. 62 (*Mangold).*

[1083] BVerfGE 123, 267, Rn. 351, 370.

[1084] *Bäcker*, EuR 2011, 103 ff.

[1085] *Bäcker*, EuR 2011, 103, 108 f.

[1086] *Bäcker*, EuR 2011, 103, 109 führt weiter aus, dass sich dadurch die Bedeutung der Substantiierungslast, wie sie im Bananenmarkt-Beschluss aufgezeigt wurde, dadurch erheblich vermindert werde. Zu den Chancen und Risiken dieses neuen Ansatzes, ausführlich *Bäcker*, EuR 103, 110 ff. Er sieht vor allem die Chance, dass ein fallbezogener Grundrechtsdialog zwischen *BVerfG* und *EuGH* entstehen könne.

Das Gericht beschränkt sich aber nicht nur auf die Prüfung des Ob einer Vorratsdatenspeicherung im Sinne der Richtlinie sondern formuliert in der Tradition des Lissabon-Urteils[1087] auch inhaltliche Anforderungen aus dem deutschen Verfassungsrecht.

Da diese von dem unionsrechtsfesten Kern der Verfassung, der Identität der Verfassung gefordert seien, richten sich diese Ausführungen (auch) an den europäischen Gesetzgeber. Dieser muss die Vorgaben des Verfassungsgerichts beachten, wenn er nicht in Konflikt mit der nicht aufgebbaren Identität der deutschen Verfassung geraten will.[1088] Zwar begründe die Vorratsdatenspeicherungsrichtlinie selbst noch keinen derartigen Konflikt. Es sei möglich, die Umsetzung der Richtlinie verfassungskonform zu gestalten. Insofern besteht in Bezug auf die Vorratsdatenspeicherung an sich auch kein Widerspruch zu nationalem Verfassungsrecht. Dies gilt aber nur, solange die Verpflichtung zur Vorratsdatenspeicherung eine Ausnahme bleibt.[1089] Sollten mehrere unionsrechtliche Verpflichtungen zur Speicherung personenbezogener Daten auf Vorrat kulminieren, würden die unionsrechtlichen Vorgaben die Identität der Verfassung und damit den europarechtsfesten Kern der Verfassung verletzen.[1090]

Allerdings ist fraglich, ob überhaupt die Richtlinie an sich materiell mit europäischem Recht vereinbar ist. Dies ist heftig umstritten und auch aktuell Gegenstand zweier anhängiger Vorlageverfahren des *irischen High Courts* und des *Österreichischen Verfassungsgerichts* zum *Europäischen Gerichtshof*, welche im Juli 2013 verhandelt wurden. Ob der *Europäische Gerichtshof* zur Feststellung gelangen wird, dass die Richtlinie europäische Grundrechte verletzt ist aktuell nicht absehbar. Der Schwerpunkt dieser Arbeit liegt nicht auf der Frage der Vereinbarkeit der Richtlinie mit Europäischem Recht, sondern der Frage, wie ein Ausgleich zwischen Freiheits- und Sicherheitsinteressen unter den Bedingungen einer digitalisierten Gesellschaftsordnung gelingen kann. Dabei wird auch der Frage, nach einer möglichst verfassungsschonenden Umsetzung der Richtlinie in nationales Recht nachgegangen. Dafür ist es zwar in gewisser Hinsicht eine notwendige Vorfrage, ob denn die Richtlinie an sich wirksam ist. Hier soll jedoch der Annahme des *Bundesverfassungsgerichts* gefolgt werden, welches an. Dieses geht anscheinend davon aus, dass die Richtlinie nicht gegen Unionsrecht verstößt. Wenn das Gericht eine Verletzung angenommen hätte, hätte sie die Frage dem *Europäischen Gerichtshof* zur Vorabentscheidung vorlegen müssen (Art. 267 AEUV). Zudem ist zu beachten, dass solange die Richtlinie in Kraft ist, Deutschland auch zu deren Umsetzung verpflichtet ist.[1091]

[1087] BVerfGE 123, 267.

[1088] BVerfGE 125, 260 (324); Siehe hierzu ausführlich unten Kap. 7.3.2.

[1089] BVerfGE 125, 260 (323 f.).

[1090] Ausführlich dazu *Roßnagel,* DuD 2010, 544 f.; *Knierim*, ZD 2011, 17; siehe auch unten S. 227 ff.

[1091] Die zuständige Kommissarin *Malmström* erklärte auf mehrere Anfragen des EP bzgl. der Vereinbarkeit der VDS-RL mit Europäischen Grundrechten, dass bei Einführung der VDS-RL die EU-GRCh. berücksichtigt worden wäre. Die Richtlinie sei so lange gültig und müsse von den Mitgliedstaaten umgesetzt werden, bis sie zurückgenommen oder vom *EuGH* für nichtig erklärt würde; Anfrage: E-2588/2010 v. 20.4.2010, E-4328/2010 v. 16.6.2010; Antwort von *Malmström* v. 1.6.2010 und v. 30.7.2010.

4.3.2 Völkerrechtliche Pflicht zur Einführung der Vorratsdatenspeicherung?

Neben der bestehenden unionsrechtlichen Pflicht zur Einführung der Vorratsdatenspeicherung, könnten sich aus völkerrechtlichen Vereinbarungen Anknüpfungspunkte für eine Verpflichtung zur Einführung einer Vorratsdatenspeicherung ergeben.

Die im Jahr 2001 verabschiedete Cyber-Crime-Convention des Europarats[1092] verpflichtet in Art. 16 Abs. 1 die Vertragsparteien dazu „die erforderlichen gesetzgeberischen und anderen Maßnahmen" zu treffen, „damit ihre zuständigen Behörden die umgehende Sicherung bestimmter Computerdaten einschließlich Verkehrsdaten, die mittels eines Computersystems gespeichert wurden, anordnen oder in ähnlicher Weise bewirken können, insbesondere wenn Gründe zu der Annahme bestehen, dass bei diesen Computerdaten eine besondere Gefahr des Verlusts oder der Veränderung besteht." Aus Art. 20 ergibt sich darüber hinaus die Pflicht der Vertragsstaaten sicherzustellen, dass die zuständigen Behörden ermächtigt werden, Dienstanbieter zu verpflichten, Verkehrsdaten in Echtzeit zu speichern. Diese Regelungen können aber nicht als eine Verpflichtung zur Datenspeicherung auf Vorrat ausgelegt werden. Vielmehr beinhalten sie nach dem ausdrücklichen Wortlaut lediglich die Pflicht, dass die Vertragsstaaten es ermöglichen müssen, die Speicherung von Verkehrsdaten anzuordnen.[1093]

Eine Mindermeinung leitet aus dem Urteil K. U. ./. Finnland des *Europäischen Gerichtshofs für Menschenrechte* indes eine Pflicht zur Vorratsdatenspeicherung ab.[1094] In der Entscheidung hat sich der Gerichtshof mit dem Zugang zu Telekommunikationsverkehrsdaten auseinandergesetzt.[1095] In dem entschiedenen Fall, hatte ein Unbekannter für einen Minderjährigen, ohne dessen Wissen eine Anzeige auf einer Dating-Plattform eingestellt, dass der Junge eine intime Beziehung zu einem anderen Jungen oder einem Mann suche. Der Vater des Jungen beantragte bei der finnischen Polizei, den Täter zu ermitteln. Die Ermittlungen scheiterten jedoch, da sich der Dienstanbieter unter Verweis auf Berufs- und Geschäftsgeheimnisse sowie auf Datenschutzbestimmungen weigerte, die beantragten Informationen herauszugeben. Hintergrund war, dass es im finnischen Recht zu diesem Zeitpunkt keine Ermächtigung für den Abruf der Daten gab. Daher bestätigten die nationalen Gerichte die Rechtsauffassung des Dienstanbieters. Der *Europäische Gerichtshof für Menschenrechte* stellt im Ergebnis fest, dass Finnland durch das Fehlen einer Rechtsgrundlage zum Zugriff auf die Verkehrsdaten seine Schutzpflichten aus Art. 8 EMRK verletzt habe. Das Urteil verpflichtet aber keineswegs dazu eine Verpflichtung zur anlasslosen Speicherung der Verkehrsdaten sämtlicher Bürger auf Vorrat einzurichten.

Die Ansicht, dass auf Grund der Tatsache, dass ein Herausgabeanspruch ins Leere liefe, wenn es keine Verpflichtung zur Vorratsdatenspeicherung gebe und daher eine Pflicht zur Speicherung bestünde, [1096] steht weder mit dem Urteil des *Europäischen Gerichtshofs für Menschenrechte* im Einklang, noch entspricht es dem Umfang staatli-

[1092] CETS No.: 185; Deutschland hat die Konvention 9.3.2009 ratifiziert; der Stand der Ratifikation ist abrufbar unter: http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CL=ENG.
[1093] *Gitter/Schnabel,* MMR 2007, 411, 416.
[1094] *Schmid,* CyLaw Report 2/2010, S. 1 ff.
[1095] *EGMR*, Urt. v. 2.12.2008, *K. U. ./. Finnland,* Nr. 2872/02.
[1096] *Schmid, CyLaw Report 2/2010*, 1 ff.

cher Schutzpflichten, wie sie allgemein anerkannt sind. Der Staat ist keineswegs verpflichtet durch eine umfassende Überwachung der gesamten Bevölkerung sicherzustellen, dass jegliche Straftat aufgeklärt werden kann. Es besteht eben keine Pflicht zur Gewährleistung einer hundertprozentigen Sicherheit.[1097]

Neben der Verpflichtung aus der Vorratsdatenspeicherungsrichtlinie besteht keine völkerrechtliche Pflicht eine Vorratsdatenspeicherung in Deutschland einzuführen.

4.4 Die Kollision von Freiheits- und Sicherheitsinteressen im Rahmen der Vorratsdatenspeicherung

Die Betrachtung des politischen Diskurses um die Einführung der Vorratsdatenspeicherung zeigt, dass diese vielfach als *der* Kollisionsfall von Freiheits- und Sicherheitsinteressen im digitalen Zeitalter betrachtet wird. So sehen die Befürworter der Vorratsdatenspeicherung in dieser das entscheidende Instrument zur Gewährleistung von Sicherheit im digitalen Zeitalter. Ganz anders die Gegner der Vorratsdatenspeicherung, die diese als den entscheidenden Schritt auf dem Weg in den Überwachungsstaat betrachten.

Im ersten Teil dieser Arbeit wurde aufgezeigt, dass die Kollision von Freiheits- und Sicherheitsinteressen zu Beginn des 21. Jahrhunderts durch Digitalisierung, Globalisierung und veränderte Bedrohungen geprägt ist.[1098] Der Eindruck der Verwundbarkeit entsteht, was dazu führt, dass Tendenzen zu einer immer stärkeren Sicherheitsvorsorge zu verzeichnen sind.[1099] Dadurch wird das, dem Grundgesetz immanente, Spannungsverhältnis zwischen Freiheits- und Sicherheitsinteressen verschärft. In der Verfassung wird ein Ausgleich zwischen Freiheit und Sicherheit als Sicherheit für Freiheit gewährt. Ein absolutes Sicherheitsstreben ist mit der freiheitlichen Grundordnung, wie sie das Grundgesetz garantiert, jedenfalls nicht vereinbar.[1100] Durch immer neue und weiter ins Vorfeld reichende Maßnahmen wird ein verfassungskonformer Ausgleich in Frage gestellt.

Die Speicherung sämtlicher Telekommunikationsverkehrsdaten aller Bürger auf Vorrat ist eine Maßnahme, die nach Ansicht der Kritiker geeignet ist, den verfassungsmäßigen Ausgleich zwischen Freiheit und Sicherheit grundsätzlich zu stören. Für die Befürworter ist sie hingegen unentbehrlich zur Gewährleistung von Sicherheit unter den Bedingungen digitaler Datenverarbeitung und im Angesicht der sich heute stellenden Herausforderungen für die Arbeit der Sicherheitsbehörden.

Im Folgenden wird die Bedeutung der Vorratsdatenspeicherung für Freiheit und Sicherheit anhand verschiedener Argumentationsstränge näher untersucht, um detailliert darzulegen, warum die Vorratsdatenspeicherung paradigmatisch für das Spannungsverhältnis von Freiheit und Sicherheit im digitalen Zeitalter ist. Es wird dabei der Widerstreit der Interessen nicht anhand der einzelnen betroffenen verfassungsrechtlich

[1097] Dazu schon oben Kap. 2.2.7.
[1098] Vgl. dazu oben Kap. 1.
[1099] Vgl. dazu oben Kap. 1.4.
[1100] Vgl. dazu oben Kap. 3.3.

geschützten Positionen dargestellt,[1101] sondern es werden die jeweiligen politischen Argumentationslinien der Befürworter und der Gegner in Bezug auf die Vorratsdatenspeicherung als Symbol für die Kollision von Freiheits- und Sicherheitsinteressen im digitalen Zeitalter nachgezeichnet. Dabei wird auch der Frage nachgegangen, wie hoch die Bedeutung der Vorratsdatenspeicherung für die Gewährleistung von Sicherheit tatsächlich ist.

4.4.1 Vorratsdatenspeicherung als „Dammbruch" auf dem Weg in den Überwachungsstaat

Die Vorratsdatenspeicherung wird als „Symbol für die schleichende Entwicklung des Rechtsstaats zum Präventions-und Überwachungsstaat" gesehen, in dem das Recht auf informationelle Selbstbestimmung immer mehr an Bedeutung verliert.[1102] Sie wird als „Dammbruch der traditionellen Grenzen staatlicher Eingriffe in die Rechte unbescholtener Bürger" bezeichnet.[1103] Mit dem Bild des Dammbruchs wird der Eindruck vermittelt, dass die Entscheidung für dieses Instrument zwangsläufig den Weg für weitere umfassende Überwachungsmaßnahmen öffnet.

Die Dammbruch-Argumentation knüpft zunächst daran an, dass es sich bei der Vorratsdatenspeicherung um ein Instrument handelt, das auf die „Beweisbeschaffung für ein eventuell in der Zukunft einzuleitendes Ermittlungsverfahren gerichtet ist". Dem Strafverfahrensecht seien „derartige Eingriffe, die ohne gegenwärtigen Anfangsverdacht vorgenommen werden, bislang fremd." Darin liege der „bislang massivste Ausdruck eines grundlegenden Wandels, der mit einem rechtsstaatlichen Strafverfahren unverträglich ist, der Unschuldsvermutung als zentralem rechtstaatlichen Prinzip entgegensteht und das Potential für eine Totalüberwachung hat".[1104]

Es wird argumentiert, dass im Fall der Vorratsspeicherung der Telekommunikationsverkehrsdaten schon durch das „bloße Vorhandensein der Daten" eine Entwicklung eingeleitet werde, die dazu führe, dass „bereits vorhandene Daten zwangsläufig immer mehr Stellen und Personen zugänglich gemacht werden".[1105]

Im Urteil des *Bundesverfassungsgerichts* zur Vorratsdatenspeicherung hat das Gericht betont, dass trotz der Feststellung, dass eine solche nicht schlechthin verfassungswid-

---

[1101] Eine verfassungsrechtliche Analyse der im Rahmen der Vorratsdatenspeicherung kollidierenden Interessen folgt in Teil 3, S. 263 ff.

[1102] *Gausling* 2010, 15.

[1103] *Breyer*, StV 2007, 214, 218; kritisch zur These der Vorratsdatenspeicherung als Dammbruch, vielmehr werde diese „überschätzt", *Rath,* vorgänge 184 (2008), 29, 80.

[1104] *Puschke/Singelnstein*, NJW 2008, 113, 118.

[1105] *Rusteberg*, VBlBW 2007, 171 ff., 175 f. betont in diesem Kontext, dass allerdings jede später hinzutretende Zugangsberechtigung gesondert verfassungsrechtlich geprüft werden kann. Als Beispiel für diese Entwicklung verweist er darauf, dass im Zuge der Novellierung des Urheberrechts bereits Überlegungen seitens des Justizministeriums laut wurden, Rechteinhabern Auskunftsansprüche gegen die Dienstanbieter zuzugestehen, um ihre zivilrechtlichen Ansprüche bei etwaigen Urheberrechtsverstößen besser verfolgen zu können. Ausführlich mit der Logik der Dammbruch-Argumentation bei der Vorratsdatenspeicherung setzt sich *Hefendehl*, JZ 2009, 165, 173f. auseinander.

[1105] *Forgó*/*Krügel*, K&R 2010, 217, 219.

rig sei, dürfe dies nicht als „Schritt hin zu einer Gesetzgebung verstanden werden (…), die auf eine möglichst flächendeckende vorsorgliche Speicherung aller für die Strafverfolgung oder Gefahrenprävention nützlichen Daten ziele".[1106] Diese Klarstellung ist nur erforderlich, weil auch das Gericht einen Dammbruch befürchtet. Letztlich zeigt das *Bundesverfassungsgericht* mit der Formulierung dieser normativen Anforderung, dass es die faktische Möglichkeit eines solchen anerkennt. Die Vorratsdatenspeicherung dürfe eben „nicht als Vorbild für die Schaffung weiterer vorsorglich anlassloser Datensammlungen dienen".[1107]

Trotz dieser ausdrücklich formulierten Schranke, befürchten Kritiker auch noch nach dem Urteil, dass die Vorratsspeicherung der Telekommunikationsverkehrsdaten als „Dammbruch im Hinblick auf die Zulässigkeit von Vorratsdatenspeicherungen zu sehen" sei.[1108] Das Gericht habe den im Volkszählungsurteil manifestierten Grundsatz aufgeweicht, „dass der Einzelne gegen die unbegrenzte Erhebung, Speicherung, Verwendung und Weitergabe seiner persönlichen Daten zu schützen sei, indem es eine vorsorglich, anlasslose Datenspeicherung als mit dem Telekommunikationsgeheimnis prinzipiell vereinbar qualifiziert."[1109] Damit habe es einen „Paradigmenwechsel" im Datenschutz vollzogen. Der Zweckbindungsgrundsatz würde durch die Anknüpfung an die Möglichkeit einer zukünftigen Straftat oder Gefahr konterkariert, da es sich dabei um keine konkreten Zwecke handle.[1110]

Neu ist an der Vorratsdatenspeicherung jedenfalls, dass es sich um ein quasi infrastrukturelles Überwachungsinstrument handelt. Infrastrukturell, da sie an einer der zentralen Infrastrukturen der modernen Informations- und Kommunikationsgesellschaft anknüpft und von ihr unabhängig von einem Verdacht jeder Nutzer von Telekommunikationsmitteln betroffen ist.[1111] Auf Grund dessen wird die Vorratsdatenspeicherung als Sinnbild für den Schritt in einen Überwachungsstaat begriffen.

Ob die Vorratsdatenspeicherung tatsächlich als Dammbruch zu bewerten ist, ist im Ergebnis davon abhängig, ob in der Praxis sichergestellt ist, dass sie nicht Vorbild für weitere Maßnahmen dient, wie es das *Bundesverfassungsgericht* ausgeführt hat. Es kommt insofern darauf an, ob und wie stark das Verbot einer totalen Erfassung und Registrierung, welches das *Bundesverfassungsgericht* im Urteil formuliert hat, realiter wirkt. Handelt es sich nur um eine Beschwichtigungsfloskel oder kann diese die schleichende Ausweitung von Sicherheitsmaßnahmen verhindern?[1112]

4.4.1.1 Analysemöglichkeiten von auf Vorrat gespeicherten TK-Verkehrsdaten

„Verbindungsdaten können aussagekräftiger als Inhaltsdaten sein, nicht zuletzt deshalb, weil sie automatisiert analysierbar sind", so der *Chaos Computer Club (CCC)* in seiner Stel-

[1106] BVerfGE 125. 260 (323).
[1107] BVerfGE 125, 260 (324).
[1108] *Forgó/Krügel*, K&R 2010, 217, 219.
[1109] *Forgó/Krügel*, K&R 2010, 217, 219.
[1110] *Gausling* 2010, 14.
[1111] Vgl. hierzu *Roßnagel* 2003.
[1112] Diese Fragen gilt es in den nächsten Kapiteln (Kap. 5 und 6) zu untersuchen.

lungnahme im Verfahren vor dem *Bundesverfassungsgericht*.[1113] Auch andere betonen, dass durch neue technische Entwicklungen, insbesondere neue Analysemethoden, zunehmend die Differenzierung zwischen Verkehrs- und Inhaltsdaten aufgelöst werde.[1114] Dies erkennt auch das *Bundesverfassungsgericht* an: „Da eine Auswertung dieser Daten tief in das Privatleben eindringende Rückschlüsse und unter Umständen detaillierte Persönlichkeits- und Bewegungsprofile ermöglicht, kann insoweit nicht ohne weiteres davon ausgegangen werden, dass der Rückgriff auf diese Daten grundsätzlich geringer wiegt als eine inhaltsbezogene Telekommunikationsüberwachung".[1115]

Ein eindrückliches Beispiel dafür, wie mit Telekommunikationsverkehrsdaten ein umfassendes und exaktes Bewegungsprofil erstellt werden kann, bietet der Selbstversuch von *Malte Spitz* (Mitglied im Bundesvorstand der *Grünen*). Dieser hat eine Analyse seiner Verkehrsdaten publiziert.[1116] Miteinbezogen in die Analyse wurden die Standortdaten, Uhrzeiten, die Dauer und Anzahl der Telefon- und Internetverbindungen sowie die Anzahl der SMS. Diese wurden verknüpft mit anderen, im Internet frei verfügbaren, Informationen. Der Politiker hat diese Daten aufbereiten lassen und dann in einer interaktiven Grafik veröffentlicht.[1117]

Wenn man sich die Daten als Film ansieht, laufen gefühlt sechs Monate im Leben von *Spitz* auf dem Bildschirm an einem vorbei. Da über sein Handy automatisch alle zehn Minuten seine E-Mails abgerufen wurden, sind alle zehn Minuten Daten der angewählten Funkzelle verfügbar. Aufgrund der Dichte an Funkmasten in der Hauptstadt Berlin, in der *Spitz* offenkundig seinen Wohnsitz und Lebensmittelpunkt hat, ergibt sich ein sehr exaktes Bewegungsprofil. Nicht miteinbezogen ist eine Analyse der Kontakte, welche − wohl noch weit über das erzeugte Bewegungsprofil hinaus − ein umfassendes Kontakt- und Persönlichkeitsprofil ermöglicht hätte.

Neben Bewegungs- und Persönlichkeitsprofilen, lassen sich in Bezug auf Gruppen und Verbände sodann interne Einflussstrukturen und Entscheidungsabläufe aufdecken.[1118] Aus anderen Verbindungsdaten, wie der Kommunikation mit bestimmten Beratungsstellen, spezialisierten Ärzten oder Therapeuten, ergeben sich zudem schon ohne weitere Analyse höchst sensitive Informationen.[1119] Doch auch hier gilt, wie für die Erstel-

---

[1113] *Kurz/Rieger* 2009, 3.

[1114] *Kindt*, MMR 2009, 661, 662; *Heinson/Freiling,* DuD 2009, 547 ff.

[1115] BVerfGE 125, 260 (328); zur Abfrage nach altem Recht vgl. BVerfGE 107, 299 (322)).

[1116] http://www.zeit.de/digital/datenschutz/2011-02/vorratsdaten-malte-spitz. Verwendet wurden dafür die Daten, die vor der Entscheidung des *BVerfG* zur Vorratsdatenspeicherung vom 2.3.2010 aufgrund der Verpflichtung zur Vorratsdatenspeicherung gemäß der §§ 113a TKG gespeichert wurden. *Spitz* hatte auf die Herausgabe der Daten erfolgreich geklagt, dazu *Krempl* v. 25.8.2009, c't, abrufbar unter: http://www.heise.de/ -752925.html); Dargestellt werden in einer über Zeit online verfügbaren interaktiven Grafik, die auch als Film abspielbar ist, die Standortdaten, Uhrzeiten, die Zahl der ein- und ausgehenden Anrufe und SMS sowie die Dauer der Verbindungen zum Internet. Die Kontaktdaten wurden aus datenschutzrechtlichen Gründen nicht mit in die Analyse einbezogen. http://blog.zeit.de/open-data/2011/02/24/vorratsdaten-unter-der-lupe/.

[1117] Vgl. Nachw. in Fn. 1116.

[1118] BVerfGE 125, 260 (319); vgl. die umfassenden Darstellungen im Gutachten des *CCC (Kurz/Rieger* 2009).

[1119] BVerfGE 125, 260 (328).

lung sämtlicher Profile, je umfangreicher der Datenbestand ist auf den zurückgegriffen werden kann – also je länger der Zeitraum über den Daten erhoben und je mehr Datenarten gespeichert wurden – desto exaktere Informationen lassen sich aus dem Datenbestand extrahieren.

Der Umfang der vorhandenen Daten hängt bei der Vorratsspeicherung von Telekommunikationsverkehrsdaten nicht nur von dem Umfang der Speicherverpflichtung ab, sondern auch von der Häufigkeit und der Art der Nutzung von Telekommunikationsmitteln. So ergibt sich für *Spitz* ein so umfassendes Bewegungsprofil, da er offensichtlich ein Smartphone nutzt, das sich alle zehn Minuten zum Abruf von E-Mails in eine Funkzelle einwählt.

Hingegen lassen sich mittels der Vorratsdaten über eine Person, die lediglich einen Festnetzanschluss hat und mit diesem nur selten telefoniert, im Ergebnis weder ein aussagekräftiges Bewegungs- noch ein umfassendes Persönlichkeitsprofil erstellen. Allerdings lassen sich wegen der Bedeutung der Telekommunikation im digitalen Zeitalter für das gesamte gesellschaftliche Leben[1120] auch aus der Nichtnutzung von Telekommunikationsmitteln Schlüsse über die Persönlichkeit und das Kontaktumfeld einer Person ziehen.

4.4.1.2 Neue Sicherheitsrisiken

Die vielfältigen Analysemöglichkeiten und die hohe Aussagekraft der Daten führt dazu, dass diese wirtschaftlich von hohem Wert sind. Denn gerade für die Wirtschaft sind Telekommunikationsverkehrsdaten von großem Interesse, da sie Rückschlüsse auf das Verhalten der Bevölkerung und potentieller Kunden ermöglichen.[1121] Auch die Analyse der Verkehrsdaten in Bezug auf Organisationsstrukturen von Protestbewegungen, Kontakte von und zu Journalisten oder die Machtstrukturen konkurrierender Konzerne,[1122] sind hoch brisant und entsprechend wertvoll. Entsprechend ist die wirtschaftliche Verwertbarkeit der Daten sehr hoch.[1123]

Gerade auf Grund dieser Tatsache besteht ein hohes Missbrauchsrisiko.[1124] Die Datenspeicherung verursacht insofern neue Sicherheitsrisiken.[1125] Selbst wenn die Daten un-

---

[1120] Vgl. dazu oben S. 101 f.

[1121] Telefonicá hat so etwa angekündigt die Standortdaten seiner Kunden wirtschaftlich nutzen zu wollen, *Kannenberg,* „Telefonica will mit Kundendaten Geld verdienen" heise online v. 30.10.2012, abrufbar unter: http://heise.de/-1738929; Dies führte zu harscher Kritik durch den Datenschutzbeauftragten und schließlich dazu, dass der Konzern sich entschuldigte und von dem Vorhaben in Deutschland zunächst Abstand nahm, *Bernau,* „Gläsern und Faul" Kommentar SZ v. 3.11.2012.

[1122] BVerfGE 125, 260 (319); vgl. die umfassenden Darstellungen im Gutachten des *CCC (Kurz/ Rieger* 2009).

[1123] Zur Verwertbarkeit der Daten in der Forschung (etwa für stadtplanerische Entscheidungen) und zur wirtschaftlichen Verwertbarkeit insgesamt *Simonite,* „Goldmine im Aether", Technology Review v. 31.5.2010, abrufbar unter: http://www.heise.de/ -1009726; zur Planung von Telefonica die Standortdaten der Kunden zu vermarkten, http://heise.de/-1738929 (vgl. Fn. 1121).

[1124] Verwiesen sei in diesem Zusammenhang auf den Telekomskandal. Hier wurden über ein Jahr lang die Verbindungsdaten genutzt, um eventuelle Verbindungen zwischen Aufsichtsräten, Managern und Journalisten aufzudecken, *Wilkens,* heise online v. 26.5.2008, abrufbar unter: http://www.heise.de/ -210039. Auf Grund dessen wurde dann zum Teil auch eine zentrale staatli-

ter hohen Sicherheitsvorkehrungen gespeichert werden, ist es nicht auszuschließen, dass missbräuchlich auf sie zugegriffen wird.[1126]

4.4.1.3 Chilling Effect

An der Vorratsspeicherung der Telekommunikationsverkehrsdaten wird kritisiert, dass sie die Grundrechtsausübung insgesamt beeinträchtige. So argumentiert auch das *Bundesverfassungsgericht*: die Vorratsdatenspeicherung sei geeignet „ein diffus bedrohliches Gefühl des Beobachtetseins hervorzurufen, das eine unbefangene Wahrnehmung der Grundrechte in vielen Bereichen beeinträchtigen kann".[1127] Das Gericht begründet diese Annahme einer freiheitsbeschränkenden Wirkung der Maßnahme, die auch als *Chilling Effect* bezeichnet wird,[1128] nicht näher.

In der Literatur finden sich jedoch Rechtfertigungen für diese Annahme. So seien langfristige Speicherungen geeignet, das Vertrauen in die Nutzung technischer Kommunikationsmittel zu zerstören, da der Einzelne sich nicht sicher sein könne, ob der Staat einmal gewonnene Daten nicht auch anderen Verwendungszwecken zuführe.[1129] Gegen diese Argumentation spricht jedoch, dass das *Bundesverfassungsgericht* wohl kaum der Exekutive grundsätzlich Rechtsbruch unterstellt. Schließlich ist diese an die Verfassung und die Gesetze gebunden. Andererseits ist ein Missbrauchsrisiko nicht zu verneinen – ob von staatlicher oder auch privater Seite.[1130] Besser untermauert die These, die Vorratsdatenspeicherung würde ein Gefühl des Überwachtwerdens hervorrufen, dass auf Grund der Streubreite der Maßnahme und der überwiegend heimlichen Verwendung und Auswertung der Daten, der Einzelne das Gefühl verliert, Herr über seine Daten zu sein. Dieser Annahme entspricht auch, dass das *Bundesverfassungsgericht* Transparenzregelungen und Rechtsschutzmöglichkeiten eine hohe Bedeutung beimisst.[1131]

Schließlich spricht für die Hypothese einer beschränkenden Wirkung, ganz generell, dass durch die Datenspeicherung das Risiko gesteigert wird, weiteren Ermittlungen ausgesetzt zu werden „ohne selbst dazu Anlass gegeben zu haben".[1132] Dies liegt insbesondere daran, dass die Erhebung von Verkehrsdaten es nur ermöglicht, eine bestimmte Handlung einem Anschluss zuzuordnen – damit ist aber noch lange nicht gesagt, dass die fragliche Handlung auch vom Anschlussinhaber vorgenommen wurde. Deutlich machen dies Fälle von Urheberrechtsverletzungen oder auch der Verbreitung von

---

che Speicherung der Vorratsdaten gefordert, so etwa auch der Bund deutscher Kriminalbeamter, zitiert nach *Kuri,* heise online v. 27.5.2008, abrufbar unter: http://heise.de/-210161; auch das *BVerfG* betont, dass ein Missbrauchsrisiko bestünde, BVerfGE 125, 260 (320).

[1125] So auch *Dix* 2012.

[1126] Wirklich sicher sind letztlich nur die Daten, die nicht gespeichert werden, *Roßnagel/Scholz* MMR 2000, 721 ff.; *Roßnagel/Bedner/Knopp* DuD 2009, 536 ff.

[1127] BVerfGE 125, 260 (320); Kritisch dazu, da es sich um keine rechtlich nachvollziehbaren Kriterien handle, *Pagenkopf*, in: *Sachs,* GG 2011, Art. 10, Rn. 8.

[1128] Die Chilling-Effect-Doktrin ist der Rspr des US-Surpreme-Court entlehnt; vgl. dazu *Grimm* NJW 1995, 1703 ff.

[1129] *Sievers* 2002, 192.

[1130] Vgl. zum Missbrauchsrisiko, S. 184.

[1131] BVerfGE 125, 260 (LS 2, 3).

[1132] BVerfGE 125, 260 (320).

Kinderpornographie, in denen offene WLAN-Netze von Fremden unbemerkt und missbräuchlich genutzt werden. In diesen Fällen geraten zunächst die Anschlussinhaber ins Blickfeld der Ermittlungsbehörden und unter Rechtfertigungsdruck.

Dass der Einzelne in der Folge einer Vorratsdatenspeicherung auch tatsächlich nur einschränkend von seiner Telekommunikationsfreiheit Gebrauch machen würde und sein Verhalten anpassen würde, scheint darüber hinaus eine *forsa*-Studie, die im Auftrag des *AK Vorratsdatenspeicherung* durchgeführt wurde, zu belegen.[1133] Allerdings wurde hier lediglich gefragt, ob die Menschen meinen, dass sie ihr Verhalten anpassen würden – ob die Befragten auch tatsächlich ihr Verhalten anpassen, kann die Untersuchung hingegen nicht belegen.

Eine solche Verhaltensanpassung ist aber zu erwarten.[1134] Denn auch wenn keine unmittelbare Auswertung der Daten erfolgt, ist davon auszugehen, dass das Wissen um eine umfassende Erfassung des Verhaltens geeignet ist eine Verhaltensanpassung hervorzurufen. Und zwar, dass sich in ihrem Verhalten nicht nur diejenigen an, „die etwas zu verbergen haben", sondern der entstehende Überwachungsdruck dazu führt, dass letztlich jeder sein Verhalten anpasst.[1135] Dies droht letztlich insbesondere da die Vorratsdatenspeicherung ausnahmslos jede Kommunikation erfasst, eben auch die mit Berufsgeheimnisträgern wie Ärzten oder Rechtsanwälten.

4.4.2 Vorratsdatenspeicherung als „zentrales Ermittlungsinstrument" im digitalen Zeitalter

Die Befürworter der Vorratsdatenspeicherung sehen in ihr das zentrale Instrument zur Gewährleistung von Sicherheit im digitalen Zeitalter. „Surfen ohne strafrechtliche Grenzen" wird getitelt und dargelegt, dass die Speicherung von Verkehrsdaten auf Vorrat unentbehrlich sei, um die Verfolgung von Internet- und Computerkriminalität zu ermöglichen.[1136]

Verkehrsdaten und Bestandsdaten hinter dynamisch vergebenen IP-Adressen werden im Rahmen unterschiedlichster kriminalistischer Strategien zur Aufklärung von Straftaten genutzt. Dabei geht es vornehmlich um retrospektive Abfragen. In einem geringen Umfang werden die Daten auch präventiv zur Verhinderung von Straftaten abgefragt.

Vorab sollen die unterschiedlichen ermittlungstechnischen Einsatzgebiete von auf Vorrat gespeicherten Verkehrsdaten dargestellt werden:

[1133] http://www.daten-speicherung.de/data/forsa_2008-06-03.pdf.

[1134] *Maras* 2009, 78 f.; Ein „Gefühl des Überwachtwerdens" ist angesichts der Vorratsdatenspeicherung vorprogrammiert" so *Grafe*, 350.

[1135] In Bezug auf das Verhalten Gefangener legte *Foucault* überzeugend dar, dass es irrelevant ist, ob tastsächlich kontinuierlich alles überwacht wird oder ob die konkrete Überwachung nur sporadisch erfolgt, da die Wirkung einer Überwachung selbst dann permanent sei, wenn die Durchführung nur sporadisch erfolgt, *Foucault* 1993, 258.

[1136] *Beukelmann,* NJW 2012, 2617 ff.

- Bestandsdatenauskünfte und die Ermittlung von Kontakten

Um einen Anschlussinhaber zu identifizieren, der zu einer bestimmten Zeit mit einem bestimmten Kommunikationsgerät ein anderes kontaktiert hat oder kontaktiert wurde, werden Suchläufe durch den jeweiligen Telekommunikationsanbieter durchgeführt.[1137] Dies ermöglicht beispielsweise die Ermittlung des Anschlusses, und des Anschlussinhabers hinter einer dynamischen IP-Adresse. Diese Daten sind für den gesamten Bereich der Verfolgung von Internetkriminalität von großem Interesse. Die Analyse der Kontakte zu bestimmten Anschlüssen im Bereich der Telefonie ist hingegen vor allem für die Verfolgung von Transaktionskriminalität (Handel mit Betäubungsmitteln, Menschenhandel), als auch bei Tötungs-, Raub- oder Erpressungsdelikten relevant. Auf der anderen Seite können Verkehrsdaten die Ermittlungsarbeit auch in eine falsche Richtung lenken.[1138] Dies ist vor allem dann der Fall, wenn gegen einen vermeintlichen Anschlussinhaber Ermittlungen aufgenommen werden, der Anschluss aber missbräuchlich genutzt wurde.[1139]

- Funkzellenabfrage

Mit der Funkzellenabfrage wird retrospektiv die Telekommunikation in einem bestimmten räumlichen und zeitlichen Sektor ausgewertet.[1140] Es werden dabei alle Verkehrsdaten mit Tatzeit- und Tatortbeziehung beim Telekommunikationsanbieter abgerufen. Diese werden, mit vorliegenden Verkehrsdaten abgeglichen. Sie können auch im weiteren Verlauf der Ermittlungen dazu genutzt werden, um über Bestandsdatenauskünfte weitere Ermittlungsansätze zu gewinnen.

Funkzellenabfragen werden sowohl für die Verfolgung von Serientaten als auch von Einzeltaten als wertvolles Ermittlungsinstrument erachtet, wobei zahlreiche Fälle von umfassenden Funkzellenabfragen (wie etwa in Berlin zur Ermittlung der Auto-Brandstifter,[1141] in Dresden zur Überführung vermeintlicher Straftäter bei Anti-Nazi-Demonstrationen[1142] oder zur Aufklärung eines Holzklopfwurfs auf eine Autobahn[1143]) die Wirksamkeit einer Funkzellenabfrage für die Ermittlungsarbeit in Frage stellen.[1144] Denn in all diesen Fällen wurden zwar zig Tausende Datensätze abgerufen, sie führten aber nicht zum Erfolg.

[1137] *Albrecht/Kilchling* 2011, 71 f.
[1138] *Albrecht/Kilchling* 2011, 72 m.w.Nachw.
[1139] Vgl. dazu schon oben S. 182 ff.
[1140] *Henrichs/Wilhelm* 2010; *Albrecht/Kilchling* 2011, 92.
[1141] http://www.heise.de/-1420960.
[1142] http://www.heise.de/-1268104; Eine vergleichende Betrachtung der Abfragen in Berlin und Dresden, dazu http://www.taz.de/!86387/.
[1143] Am 23.3.2008 wurde ein Holzklotz von einer Autobahnbrücke Nahe Oldenburg auf die Fahrbahn geworfen. Eine Frau kam dabei zu Tode. Hier wurden alle Kontakte, die sich zwischen 17 und 22 Uhr in der der entsprechenden Funkzelle aufgehalten hatten, abgefragt. Insgesamt waren laut Medienberichten etwa 12.000 Kontakte betroffen. Der Fall konnte jedoch nicht mit Hilfe der Funkzellenauswertung aufgeklärt werden, sondern letztlich durch andere Ermittlungsansätze, vgl. *Albrecht/Kilchling* 2011, Fn. 148.
[1144] *Albrecht/Kilchling* 2011, 72.

- Erstellen von Kommunikations- und Organisationsprofilen

Es wurde schon darauf hingewiesen, dass auch im Kontext der Ermittlungen bezüglich der NSU-Terrorzelle, die Forderung nach einer Vorratsdatenspeicherung laut wurde.[1145] Dahinter steckt die Annahme, dass eine Analyse der Telekommunikationsverkehrsdaten der Terroristen es ermöglicht hätte, die Organisationsstrukturen der NSU aufzudecken. Denn die Auswertung von auf Vorrat gespeicherten Verkehrsdaten enthält Aussagen darüber, wer wann mit wem wie oft und in welchen Abständen kommuniziert hat. So verspricht die Analyse des Kommunikationsverhaltens einer terroristischen Vereinigung Anhaltspunkte darüber, wer diese unterstützt, wer sie anleitet, wer Befehle gibt etc.[1146] Die Auswertung der Kommunikationsmuster ermöglicht es die Organisationsstrukturen zu ermitteln. Zudem kann mittels einer Analyse der Funkzelleninformationen festgestellt werden, wer alles zur gleichen Zeit gemeinsam in einer Funkzelle war. Die Schwierigkeit besteht aber etwa hinsichtlich der Ermittlungen im NSU-Prozess zum einen bereits darin, dass eine Speicherung der Verkehrsdaten über sechs Monate nicht genügt hätte für Ermittlungen hinsichtlich der zum Teil über zehn Jahre zurückliegenden Straftaten. Zum anderen kann bezweifelt werden, ob die seit über einem Jahrzehnt im Untergrund lebenden Rechtsterroristen Handys benutzt haben für ihre Kommunikation und nicht andere Kommunikationswege genutzt haben.

4.4.2.1 Anpassung der Polizeiarbeit an veränderte Rahmenbedingungen

Die Notwendigkeit einer Speicherung der Telekommunikationsverkehrsdaten auf Vorrat wird zunächst damit begründet, dass eine Anpassung der polizeilichen Fahndungs- und Ermittlungsmöglichkeiten an die Gegebenheiten des digitalen Zeitalters erforderlich sei. In diesem Sinne akzeptiert auch das *Bundesverfassungsgericht* die Einführung der Vorratsdatenspeicherung als Reaktion auf das spezifische Gefahrenpotenzial der Telekommunikation.[1147]

Die Telekommunikation erleichtere eine verdeckte Kommunikation von Straftätern und ermögliche so, selbst verstreuten Gruppen von wenigen Personen, sich zusammenzufinden und effektiv zusammenzuarbeiten.[1148] Richtig ist, dass das Internet auch von terroristischen Vereinigungen zur Information, Kommunikation und schließlich zu Propagandazwecken genutzt wird.[1149]

[1145] Vgl. dazu oben S. 168.

[1146] Zur Möglichkeit der Analyse von Organisationsstrukturen mittels Vorratsdaten, auch *Kurz/Rieger* 2009, 54 ff.

[1147] BVerfGE 125, 260 (322).

[1148] So werde „eine Bündelung von Wissen, Handlungsbereitschaft und krimineller Energie möglich, die die Gefahrenabwehr und Strafverfolgung vor neuartige Aufgaben stellt", BVerfGE 125, 260 (322 f.).

[1149] „Das Internet ist das wichtigste Kommunikations- und Propagandamedium für Islamisten und islamistische Terroristen. Die Möglichkeiten dieses Mediums zur Bildung „virtueller" Netzwerke werden von „Jihadisten" und ihren Sympathisanten rege genutzt, indem diese über Diskussionsforen und Chatrooms Kontakt zu Gleichgesinnten aufnehmen und sich offen oder in geschlossenen Foren miteinander austauschen." *BMI*, Verfassungsschutzbericht 2009, 205; dazu auch *Böckenförde* 2003, 49; in Bezug auf die spezifische Gefahr durch terroristische Selbstmordattentäter sieht

Auch in Bezug auf den Austausch kinderpornographischer Schriften wird mit drastischen Bildern gearbeitet und vermittelt, dass das Internet die Polizeiarbeit vor große Herausforderungen stellt: „Während früher in pädophilen Kreisen Bücher und Hefte „unter dem Ladentisch verkauft wurden, bietet das „World-Wide-Web völlig neue Verbreitungswege für die Kriminellen. Grenzenlose Freiheit im Netz würde bedeuten, dass ‚Kinderschänder' ihre perversen Neigungen ungehindert und ungestraft ausleben könnten und unzählige, unschuldige Kinder zu Opfern würden".[1150] Ganz in diesem Sinne wird vielfach die Vorratsdatenspeicherung als essenziell für die Bekämpfung von Kinderpornographie und internationalen Terrorismus bezeichnet. Vorratsdaten seien unabdingbar für die Arbeit der Polizeibehörden – Belege dafür können jedoch vielfach nicht vorgelegt werden.[1151]

Gegen die vielfach dramatischen Darstellungen, spricht zunächst, dass keineswegs eine freie Kommunikation im Internet die Straflosigkeit sexuellen Missbrauchs oder des Besitzes und Vertriebs kinderpornographischer Schriften bedeutet. Die Aufdeckung von kinderpornographischen Ringen gestaltet sich nicht nur auf Grund des Internets als riesigem und überwiegend unkontrollierten und unkontrollierbarem Kommunikations- und Informationsraum so schwierig, sondern weil – und hier besteht eine gewisse Parallelität zu terroristischen Vereinigungen – sich die Gruppen eng zusammenschließen und darauf bedacht sind so zu handeln, dass sie eben nicht entdeckt werden. Insbesondere ist der Zugang zu diesen Kreisen auch für verdeckte Ermittler sehr schwierig.[1152] Auch lässt sich ein kausaler Zusammenhang zwischen Verbreitungsmöglichkeiten im Internet und dem Missbrauch von Kindern und Jugendlichen nicht nachweisen.[1153] Vielmehr zeigt auch die Analyse der Kriminalstatistiken zu Fällen von Kinderpornographie, dass diese mit der zunehmenden Verbreitung des Internets insgesamt nicht angestiegen sind. Auch sind hier Schutzlücken auf Grund des Fehlens von auf Vorrat gespeicherten Verkehrsdaten kaum nachweisbar.[1154]

Das spezifische Gefahrenpotential der Telekommunikation begründet das *Bundesverfassungsgericht* darüber hinaus damit, dass die Telekommunikation „– etwa durch Angriffe auf die Telekommunikation Dritter – auch neuartige Gefahren" begründe.[1155] Gemeint sind damit Delikte die mittels Telekommunikation begangen werden sowie Angriffe auf die Telekommunikationsinfrastruktur. Dies steht in engem Zusammenhang mit der Abhängigkeit von der Informationstechnik im digitalen Zeitalter. Richtig ist, dass wie hier bereits in Teil 1 dargelegt wurde, dass aufgrund der Digitalisierung des Alltagslebens durch IT-spezifische Kriminalität, insbesondere aber internetspezifische

---

Sauer die Rationalität des Rechtsregimes durch derartige Taten in Frage gestellt und die Ausweitung und Verselbstständigung der Informationsvorsorge der Polizeiarbeit als Reaktion darauf, *Saurer*, NVwZ 2005, 275, 276; ausführlich zur Informatisierung der Polizeiarbeit als Reaktion auf die Bedingungen der digitalen Datenverarbeitung, oben Kap. 1.4.2.2.

[1150] *Kindler* 2004, 151.

[1151] *Niedersächsischer Landtag*, Drs. 16/3056 (Kleine Anfrage mit Antwort v. 7.12.2010).

[1152] Vgl. dazu die Studie von White-IT, *Kleinz,* Zeit online v. 25.11.2010, abrufbar unter: http://www.zeit.de/digital/internet/2010-11/kinderpornografie-whiteIT-schuenemann?page=1.

[1153] Dazu schon oben S. 165.

[1154] *Albrecht/Kilchling* 2011, 94 f.; 97ff.

[1155] BVerfGE 125, 260 (323).

Sabotageakte und Angriffe auf das Internet, die Sicherheitspolitik vor einer neuen Herausforderung steht.[1156]

Schließlich so das *Bundesverfassungsgericht* fehle es „mangels öffentlicher Wahrnehmbarkeit" an einem „gesellschaftlichen Gedächtnis", so dass es nicht möglich sei, wie in anderen Bereichen „zurückliegende Vorgänge auf der Grundlage zufälliger Erinnerung zu rekonstruieren". Daher nimmt das Gericht an, dass die Vorratsdatenspeicherung „für eine effektive Strafverfolgung und Gefahrenabwehr von besonderer Bedeutung" sei.[1157] In Anbetracht einer im Vergleich zur durchschnittlichen Aufklärungsquote sehr hohen Aufklärungsquote für Straftaten, die mit dem Tatmittel Internet begangen wurden, kann diese Feststellung jedoch nicht unhinterfragt bleiben.[1158] Faktisch ist es keineswegs so, dass es ohne Vorratsspeicherung von Telekommunikationsverkehrsdaten an Anknüpfungspunkten für die Aufklärung von Delikten mit einem Bezug zur Telekommunikation fehlt. Es ist zwar richtig, dass es insbesondere bei der Kommunikation über das Internet an einem mit der Offline-Welt vergleichbaren sozialen Gedächtnis fehlt: Es gibt keine Zeugen, die eine bestimmte Person gesehen haben und diese beschreiben können. Allerdings hinterlässt, anders als in der Offline-Welt, jede Handlung im Internet digitale Spuren, die insofern auch die Ermittlungsarbeit erleichtern.[1159] Beispielsweise gibt es bei Betrugsdelikten über das Internet in aller Regel Kontodaten. Auch Stalking, Mobbing oder Verleumdungs- oder Beleidigungsdelikte, die in Foren geschehen, können überwiegend auch ohne Vorratsdatenspeicherung aufgeklärt werden, denn in der Mehrzahl der Fälle handelt es sich um Täter aus dem Bekannten- oder Freundeskreis.[1160] Verkehrsdaten sind insofern nicht der einzig mögliche Ermittlungsansatz. Zudem hat die Polizei, bei Verdacht einer Straftat oder zu Gefahrenabwehrzwecken, auch die Möglichkeiten bei Seitenbetreibern Zugangsdaten und gespeicherte Informationen zu einem Nutzer heraus zu verlangen.[1161] Schließlich gibt es auch ohne eine Speicherung der Telekommunikationsverkehrsdaten auf Vorrat die Möglichkeit, die vorhandenen Daten beim jeweiligen Telekommunikationsdiensteanbieter abzufragen. Diese dürfen allerdings aus datenschutzrechtlichen Gründen die

[1156] Dazu grundlegend oben Kap. 1.2, S. 17 ff.; *Möllers* 2009, 131, 154 f. legt dar, dass in Deutschland etwa 95 Prozent aller Vorgänge in irgendeiner Weise von der Informationstechnik abhängig seien (Warenverkehr, Gesundheitswesen, Dienstleistungssektor, Finanzsystem, etc., bilden insgesamt heute die Grundlage des funktionierenden Zusammenlebens). Dem technischen Fortschritt gegenüber stehen neue Angriffspotentiale wie etwa durch Phising, Pharming, Trojaner, Spam-Mails, virenverseuchte E-Mails. Er legt dar, dass sich die Zahl der Sabotageakte im Internet, bei denen es u.a. zu Stromausfällen und dem Zusammenbruch von Buchungssystemen etc. gekommen sei, sich in den letzten Jahren vervielfacht habe. Ausführlich auch zum Internet als kritische Infrastruktur und den neu entstandenen Sicherheitsrisiken, oben S. 42.

[1157] BVerfGE 125, 260 (323).

[1158] *Albrecht/Kilchling* 2011, 86 ff.

[1159] Zu den digitalen Spuren im Netz, vgl. oben Kap. 1.1.2.3.

[1160] *Albrecht/Kilchling* 2011, 109 ff. legen unter zahlreichen anderen Gesichtspunkten dar, warum Stalking nicht mittels Vorratsdatenspeicherung besser bekämpft werden könnte.

[1161] Ausführlich zu den bestehenden Ermittlungsmöglichkeiten zur Aufdeckung der Identität im Internet, *Brunst* DuD 2011, 618.

Verkehrsdaten nicht unbegrenzt speichern, sondern jeweils nur solange, wie sie für die Vertragsabwicklung und -abrechnung benötigt werden.[1162]

Gemäß § 97 Abs. 3 Satz 2 TKG dürfen Abrechnungsdaten bis sechs Monate nach Absendung der Rechnung gespeichert werden. Dies gilt aber nur soweit die Daten zu Abrechnungszwecken benötigt werden. Soweit keine Daten zu Abrechnungszwecken benötigt werden, also im Fall von Flatrate-Angeboten, bei der E-Mail-Kommunikation sowie bei Prepaid-Angeboten und Anonymisierungsdiensten, entstehen Datenlücken. Denn in diesen Fällen dürfen die Daten nur, jedenfalls soweit keine Einwilligung der Kunden vorliegt, zur Behebung von Fehlern und Störungen und zur Missbrauchsbekämpfung nach § 100 TKG gespeichert werden. Die Rechtsprechung hält für IP-Zugangsdaten bei Flatrate-Tarifen eine Speicherung von sieben Tagen für zulässig.[1163]

Generell variiert die Speicherpraxis der Telekommunikationsdiensteanbieter aber stark von Unternehmen zu Unternehmen. Auch ohne Vorratsdatenspeicherung werden zahlreiche Verkehrsdaten bei vielen Anbietern für sechs Monate und darüber hinaus gespeichert.[1164] Es werden aber nicht flächendeckend alle Verkehrsdaten bei jedem Anbieter für längere Zeit vorgehalten.

Es gibt insoweit nicht zu bestreitende Datenlücken ohne eine Speicherung von Verkehrsdaten auf Vorrat. Die Möglichkeit retrograd Beziehungsmuster aufzudecken, IP-Adressen zu zuordnen oder Bewegungsprofile zu erstellen oder festzustellen, ob sich das Handy eines Verdächtigen zur Tatzeit in der Nähe des Tatorts befand, ist dadurch eingeschränkt. Diese Informationen würden jedoch in einer Vielzahl an Fällen verschiedenste Ermittlungsansätze bieten, die so dann zur Aufklärung von Straftaten beitragen könnten. Ob es deshalb gravierende Ermittlungsdefizite und Einbußen hinsichtlich der Wahrung der inneren Sicherheit gibt, ist dagegen eine andere Frage.

Jedenfalls kann die Vorratsdatenspeicherung mit dem *Bundesverfassungsgericht,* als Reaktion auf das spezifische Gefahrenpotential der Telekommunikation begriffen werden. Allerdings heißt dies noch nicht, dass die Bedeutung der Vorratsdatenspeicherung für die Arbeit der Ermittlungsbehörden tatsächlich so hoch ist, wie es Sicherheitsbehörden und Innenministerien vielfach darstellen – gerade in Anbetracht der zahlreichen digitalen Spuren, die der einzelne Nutzer im Internet auch ohne eine Vorratsspeicherung hinterlässt, ist die tatsächliche Bedeutung einer Vorratsdatenspeicherung für die Ermittlungsarbeit der Polizei kritisch zu hinterfragen.

4.4.2.2 Statistische und kriminologische Untersuchungen

Ob die Vorratsdatenspeicherung jedoch unabhängig von ihrer abstrakten Eignung tatsächlich einen Beitrag zu mehr Sicherheit leistet, ist heftig umstritten. Das Bundeskriminalamt hat im Jahr 2010 verschiedene Fälle zum Beleg der Erforderlichkeit einer

---

[1162] Vgl. genauer §§ 97, 99, 100 und 101 TKG.

[1163] *LG Darmstadt*, Urt v. 06.06.2007 - 10 O 562/03, abgedruckt in CR 2007, 574.

[1164] Im September 2011 veröffentlichte der AK Vorrat ein Dokument der Generalstaatsanwaltschaft *Münch*en, wonach Verkehrsdaten vielfach über 180 Tage gespeichert würden (http://www.heise.de/newsticker/meldung/AK-Vorrat-wirft-Telecom-Unternehmen-verfassungswidrige-Vorratsdatenspeicherung-vor-1338178.html).

Vorratsdatenspeicherung vorgestellt und im darauffolgenden Jahr eine Vollerhebung zur Frage, welche Daten angefragt werden und ob sie verfügbar waren, veröffentlicht. Darüber hinaus dienen Kriminalstatistiken und Aufklärungsquoten immer wieder als Beleg, für einen Beitrag zu mehr Sicherheit der Vorratsdatenspeicherung.[1165] Auch die Europäische Kommission hat sich in ihrem Evaluationsbericht zur Vorratsdatenspeicherungsrichtlinie mit der Frage der Bedeutung der Vorratsdatenspeicherung zur Gewährleistung von Sicherheit auseinandergesetzt. Darüber hinaus liegen zwei Studien des *Max-Planck-Instituts für ausländisches und internationales Strafrecht* in Freiburg aus den Jahren 2008 und aus dem Jahr 2011 vor, die sich mit der Frage der Existenz von Schutzlücken ohne Vorratsdatenspeicherung befassen.[1166]

Sodann wurde 2012 eine Studie der TU Darmstadt vorgelegt, in welcher mittels einer mathematischen Simulation aufgezeigt wurde, dass die Annahme, dass je mehr Daten vorliegen, desto besser die Ermittlungsmöglichkeiten sind, nicht zu treffe. Die Forscher untersuchten diese Annahme anhand der Vorratsdatenspeicherung. Sie werteten die Kommunikationsdaten anhand von auffälligen Kommunikationsstrukturen aus. Hier kamen die Forscher, dass eine kürzere Speicherfrist für entsprechende mathematische Auswertungen besser geeignet sei um Auffälligkeiten zu identifizieren.[1167]

Schließlich wurde 2013 auch eine Studie der dänischen Polizei vorgelegt, welche belegt, dass die Vorratsdatenspeicherung in der Praxis für die Polizeiarbeit nur von geringem Nutzen sei. Die Aufklärungsquote werde durch die Vorratsdatenspeicherung nicht verbessert.[1168]

4.4.2.2.1 Kriminologische Untersuchungen des Max-Planck-Instituts

Die Studien des Max-Planck-Instituts für ausländisches und internationales Strafrecht (Freiburg) zielten darauf die Bedeutung der Verkehrsdatenabfrage zu ermitteln und darauf zu klären, ob nach dem Wegfall der Vorratsdatenspeicherung Schutzlücken bestehen. Diese Untersuchungen haben sich sehr umfassend und aus unabhängiger, kriminologischer Perspektive mit der Frage nach der Erforderlichkeit einer Vorratsdatenspeicherung auseinandergesetzt. Soweit in den Untersuchungen andere vorhandene Datenerhebungen (des Bundeskriminalamts, der Polizeilichen Kriminalstatistik, dem Evaluationsbericht der Kommission) ausgewertet werden, wird jeweils bei der Darstel-

---

[1165] „Die Aufklärung eines Falles gilt als besonders relevanter Indikator für die Effizienz der Strafverfolgungsbehörden und das Ausmaß des Schutzes von zentralen Rechtsgütern durch das Strafrecht, wie eben die fehlende Aufklärung (und niedrige Aufklärungsquoten) als Sicherheitsprobleme indizierend gelten". Wichtig ist insbesondere der Hinweis, dass die Aufklärungsquote vor allem für die Delikte als Indikator für die Ermittlungseffizienz gelten kann, bei denen die Anzeige des Verletzen oder die Kenntnisnahme durch die Strafverfolgungsbehörden die Ermittlungen auslöst, aber nicht gleichzeitig ein Tatverdächtiger genannt wird (wie etwa beim Ladendiebstahl), *Albrecht/Kilchling* 2011, 71.

[1166] *Albrecht/ Grafe/ Kilchling* 2008 – auch abgedruckt in BT Drs. 16/8434 (abrufbar unter: http://dip21.bundestag.de/dip21/btd/16/084/1608434.pdf; dazu auch die Dissertation *Grafe* 2007; *Albrecht/Kilchling* 2011, abrufbar unter http://vds.brauchts.net/MPI_VDS_Studie.pdf.

[1167] *Krempl,* heise online v. 11.9.2012, abrufbar unter: http://heise.de/-1704716; *Hamacher/ Katzenbeisser,* NSPW 2011.

[1168] *Krempl,* heise online v. 31.5.2013, abrufbar unter: http://heise.de/-1874170; die Studie ist im dänischen Original abrufbar unter: http://www.ft.dk/samling/20121/almdel/reu/bilag/125/1200765.pdf.

lung dieser auf die Anmerkungen und Bewertung durch das Max-Planck-Institut eingegangen.

Beide Untersuchungen beruhen auf einem Mehrmethoden-Ansatz. Der im Jahr 2008 veröffentlichten Studie lagen eine umfassende Analyse von Strafverfahrensakten aus den Jahren 2003 und 2004, schriftlichen Befragungen von Staatsanwälten sowie Expertengesprächen mit Praktikern aus allen Bereichen, die mit Maßnahmen nach §§ 100g, 100h konfrontiert waren, zu Grunde.[1169] Die Anschlussuntersuchung aus dem Jahr 2011, erfolgte wiederum im Auftrag des Bundesjustizministeriums, und beruhte auf einer Auswertung statistischer Erhebungen, Sekundäranalysen und Interviews mit Vertretern der Justiz (Staatsanwälte und Richter), der Polizei und Repräsentanten der großen Universalanbieter (Deutsche Telekom, E-Plus, Vodafone, O2).[1170] Als „Kontrastgruppe" wurde schließlich die Situation in verschiedenen Ländern mit und ohne Vorratsdatenspeicherung untersucht.[1171]

Aus der umfassenden Erhebung zog das Max-Planck-Institut im Jahr 2008 folgende, für die Frage der Bedeutung von Verkehrsdaten für die Ermittlungsarbeit der Polizei relevanten, Schlüsse:[1172]

- Es werden zwei Perspektiven diagnostiziert, in denen die Daten eine besondere Bedeutung hätten: Zum einen dienten sie der Identifizierung eines noch unbekannten Täters. Hier stelle die Verkehrsdatenabfrage häufig das erste und einzige Mittel dar, um die Straftat aufzuklären. Zum anderen verhelfe die Verkehrsdatenabfrage dazu, Bandenstrukturen und Kontakte der Tatbeteiligten untereinander offenzulegen.[1173]
- Die Verkehrsdaten seien überwiegend für das Ermittlungsverfahren relevant. Hingegen würden sie für „Anklage, Hauptverhandlung und Urteil (…) relativ selten" verwendet.[1174]
- In 24 Prozent der Fälle wurden die Verkehrsdaten im Rahmen einer Telekommunikationsüberwachung nach § 100a StPO miterhoben.[1175]
- Probleme mit der Speicherungspraxis der Unternehmen spielten in den Akten kaum eine Rolle. Nur bei 63 Beschlüssen, also in etwa zwei Prozent aller untersuchten Fälle, seien die Daten nicht mehr verfügbar gewesen.[1176]

[1169] BT Drs. 16/8434, 57 ff.
[1170] *Albrecht/Kilchling* 2011, 10 hier findet sich eine tabellarische Auflistung nach Funktionen der befragten Interviewpartner.
[1171] *Albrecht/Kilchling* 2011, 11 f.
[1172] Hier ist es wichtig zu berücksichtigen, dass die Studie aus dem Jahr 2008 sich allein mit der Frage der Bedeutung von Verkehrsdaten für die Ermittlungsarbeit befasst hat und nicht etwa mit der Bedeutung von auf Vorrat gespeicherten Verkehrsdaten.
[1173] BT Drs. 16/8434, 235.
[1174] BT Drs. 16/8434, 235.
[1175] *Albrecht/ Grafe/ Kilchling* 2008, 285.
[1176] „Bei 37 Beschlüssen waren die Daten bereits gelöscht und bei 17 Beschlüssen nur teilanonymisiert gespeichert", vgl. BT Drs. 16/8434, 235.

- Insgesamt sei eine Vielzahl von Unbeteiligten bei der Verkehrsdatenabfrage mitbetroffen. Auch wird erläutert, dass in keinem der untersuchten Fälle der Anschluss eines Zeugnisverweigerungsberechtigten erkennbar betroffen war und ein Verwertungsverbot nach sich gezogen hätte. Dies lege die Vermutung nahe, dass tatsächlich „die „Dunkelziffer" der betroffenen sonstigen Zeugnisverweigerungsberechtigten (…) relativ hoch" sei.[1177]
- Empfohlen wird, den Zugriff auf Verkehrsdaten um eine weitere Fallgruppe, nämlich solche der Tatbegehung durch Endgeräte zu ergänzen, „bei denen offensichtlich der Weg über die Verkehrsdaten der einzige Ermittlungsansatz ist".[1178]

Das Gutachten des Max-Planck-Instituts aus dem Jahr 2011 knüpft an diese Untersuchung an, hat aber mit der Frage, ob durch das Urteil des *Bundesverfassungsgerichts* zur Vorratsdatenspeicherung Schutzlücken entstanden sind, einen anderen Schwerpunkt. Die, wesentlichen Schlussfolgerungen im Gutachten des Max-Planck-Instituts sind:

- *Datengrundlage und Diskurse*

- Bislang lägen keine Studien vor, die die Erforderlichkeit der Vorratsdatenspeicherung belegen können, oder die Auswirkungen des Urteils des *Bundesverfassungsgerichts* vom 2. März 2010 quantifizieren können. [1179]
- Die Diskussion sei geprägt durch den Bezug auf Einzelfälle,[1180] wobei diese als typisch dargestellt werden, obwohl dies nicht empirisch belegbar wäre.[1181] Insbesondere lägen in Bezug auf islamistischen Terrorismus keine Erkenntnisse vor, dass Verkehrsdaten zur Verhinderung eines Anschlags geführt hätten.

[1177] *Grafe*, 2007, 349.
[1178] BT Drs. 16/8434, 236.
[1179] *Albrecht/Kilchling* 2011, 218 Die einzelnen Auswertungen und Analysen der Statistiken des *BKA* und zur PKS sowie zum Evaluationsbericht der Kommission finden sich jeweils im Anschluss an die Darstellung der jeweiligen Studien, siehe unten S. 191 ff.
[1180] Die Einzelfallbezogenheit der Argumentation zeigt sich etwa in einem Bericht des Innenministers des Landes Thüringen vom 29.7.2010. Der Innenminister verweist hier auf den Bericht, der zum Zweck der Evaluation der VDS-RL der Kommission zugeleitet worden sei. Gegenstand dessen seien zwei Berichte über Fälle, die belegen würden, dass die Vorratsdatenspeicherung unverzichtbar sei. In einem Fall handelt es sich um eine Raubserie, die von mehreren Tätern gemeinschaftlich begangen wurde, die während der Tatbegehung miteinander mit Mobiltelefonen den Kontakt hielten und die über die durch Verkehrsdaten ermittelten Kontaktmustern, Standortdaten, Bewegungsprofilen und einer darauf gestützten Inhaltsüberwachung der Telekommunikation aufgeklärt werden konnte. Dieser Fall wird als typische Fallkonstellation bezeichnet. Im anderen Fall geht es um Drogenhandel und einen in Verbindung dazu stehenden Auftragsmord. Ermittlungsansatz war hier, durch Verkehrsdaten des Tatverdächtigen den Täter zu identifizieren. Dies sei aber nicht gelungen, da die für sechs Monate gespeicherte Daten für eine „umfassende Analyse" nicht ausgereicht hätten. vgl. dazu *Albrecht/Kilchling* 2011, 79 f. Der Bericht ist abrufbar unter www.jenapolis.de/71302/vorratsdatenspeicherung-bei-schweren-straftaten-oft-unverzichtbar-um-taeter-ermitteln-zu-koennen/.
[1181] *Albrecht/Kilchling* 2011, 219.

- *Aufklärungsquoten: Trends in ausgewählten Deliktsbereichen*

- „Der Zugriff auf Vorratsdaten der Telekommunikation erfolgt lediglich in einer sehr kleinen Zahl von Verfahren." Es sei nicht nachvollziehbar, wie dies die innere Sicherheit beeinflussen soll.[1182]
- Es deute nichts darauf hin, dass sich durch die Zugriffsmöglichkeiten auf Vorratsdaten, die in den Jahren 2008 und 2009 zur Verfügung standen, die Statistiken zur Aufklärung von Straftaten verändert hätten.[1183] Insgesamt zeige die Untersuchung, dass der Wegfall der Vorratsdatenspeicherung nicht ursächlich für Bewegungen in den Aufklärungsquoten sei.[1184]
- Generell entsprächen die Aufklärungsquoten in Deutschland jenen in der Schweiz, in der es eine Vorratsdatenspeicherung gibt.[1185] Auch hier bestünden, trotz Vorratsspeicherung, weiter Ermittlungsprobleme und zwar insbesondere auf Grund der Verbreitung von effizienten Anonymisierungstechniken, der Nutzung öffentlicher WLAN-Netze und dem Cloud Computing.[1186] So führe das Fehlen einer Vorratsdatenspeicherung nicht zu einer unterschiedlichen Sicherheitslage.[1187]
- Insgesamt ergäben sich unter Berücksichtigung sämtlichen verfügbaren Datenmaterials keine belastbaren Hinweise darauf, dass die „Schutzmöglichkeiten durch den Wegfall der Vorratsdatenspeicherung reduziert worden wären"[1188] – wobei nicht ausgeschlossen wird, dass sich in Einzelfällen Ermittlungsansätze aus Vorratsdaten ergeben können. Diese Einzelfälle würden sich aber auf die Gesamttrends nicht auswirken.

- *Ermittlungsmethoden, Ermittlungseffizienz und Aufklärungsquote*

„Verkehrsdaten spielen in der Regel nur mit anderen Daten eine Rolle." Der Fokus auf die auf Vorrat gespeicherten Verkehrsdaten als alleinige Ermittlungsmaßnahme, wie häufig dargestellt, sei im Ergebnis nicht plausibel.[1189]

- *Konsequenzen aus Perspektive der betroffenen Praktiker*

- Praktiker der Polizei[1190] sehen insgesamt einen hohen Bedarf an der Speicherung von Telekommunikationsverkehrsdaten auf Vorrat zu Ermittlungszwecken, da sich aus den Daten zahlreiche weitere Ermittlungsansätze ergäben. Der Zunahme von Flatrate-Tarifen und der daraus resultierenden fehlenden Speicherung einzelner Verbindungen müsse begegnet werden. Besonderes Interesse an Vorratsdaten be-

[1182] *Albrecht/Kilchling* 2011, 120 f.
[1183] *Albrecht/Kilchling* 2011, 121.
[1184] *Albrecht/Kilchling* 2011, 219.
[1185] *Albrecht/Kilchling* 2011, 123.
[1186] *Albrecht/Kilchling* 2011, 124.
[1187] *Albrecht/Kilchling* 2011, 219.
[1188] *Albrecht/Kilchling* 2011, 220.
[1189] *Albrecht/Kilchling* 2011, 221.
[1190] Vgl. zur Auflistung der Befragten, oben Fn. 1170.

kunden die Ermittler für den gesamten Bereich der Internetkriminalität. Hier fehle ohne retrograde Daten jeglicher Ermittlungsansatz. In Bezug auf das IP-Sharing (NAT-Verfahren) bedürfe es zudem bei einer Neuregelung einer Anpassung an die technischen Gegebenheiten. Sie fordern daher die Speicherung der Ports.[1191] Die Ermittler wenden sich zudem gegen die Einführung eines abgeschlossenen Straftatenkatalogs als Zugriffsvoraussetzung.[1192]

- Die Perspektive der Polizeibeamten wird durch die Interviews mit Staatsanwälten bestätigt. Vielfach seien Verkehrsdaten nicht mehr gespeichert, wenn die Ermittlungen zur Staatsanwaltschaft gelangen. Auch sie betonen die besondere Relevanz retrograder Verkehrsdaten für die Aufklärung von mit dem Tatmittel Computer begangener Straftaten. Auch gebe es Einschränkungen bei der Ermittlungsarbeit bei Kapitaldelikten.[1193]
- Lücken werden aktuell auch in Bezug auf die Speicherung von eingehenden Anrufen ausgemacht, die überhaupt nicht mehr gespeichert würden. Zudem sei die Zielwahlsuche derzeit bei der deutschen Telekom nicht möglich. Außerdem blieben viele Fälle aus dem Bereich der IuK-Kriminalität unaufgeklärt, da sich Telekommunikationsanbieter weigern, die nach § 113 TKG gespeicherten Daten nach Bestandsdaten aufzulösen. Darüber hinaus bestünden Lücken bei IMSI und IMEI-Nummern, da diese mangels Rechnungsrelevanz häufig nicht gespeichert würden. Beklagt wird auch die Möglichkeit einer Funkzellenabfrage in Echtzeit, die bei allen Anbietern aktuell nicht möglich sei. Generell seien Echtzeitabfragen derzeit nur über §100a TKG möglich, da Verkehrs- und Inhaltsdaten derzeit nicht getrennt gespeichert würden.[1194]
- Insgesamt, so folgert das Max-Planck-Institut, bestünde derzeit die gravierendste Schutzlücke in Bezug auf Ermittlungen im Bereich der IuK-Kriminalität. Hier kulminieren verschiedene Faktoren: besonders kurze Speicherfristen bei IP-Adressen, unterschiedliche Rechtsauffassungen zwischen Ermittlern und Anbietern über den Rechtscharakter und die erforderlichen Voraussetzungen für die Zusammenführung von IP-Adresse und Bestandsdatum,[1195] sowie technisch bedingte Lücken, bei der Nutzung von Ports an Hotspots oder auch mobilem Internet. Ein Experte aus Baden-Württemberg vergleicht die derzeitige Situation im Internet mit Straßenverkehr ohne Kfz-Kennzeichen.[1196]

[1191] *Albrecht/Kilchling* 2011, 159 f.
[1192] *Albrecht/Kilchling* 2011, 160.
[1193] *Albrecht/Kilchling* 2011, 164.
[1194] *Albrecht/Kilchling* 2011, 243.
[1195] Zu diesem Streit auch oben S. 84; dieser dürfte sich durch den Beschluss des *BVerfG* v. 24.1.2012 - 1 BvR 1299/05 weitgehend gelegt haben. Danach ist höchstrichterlich festgestellt, dass die Zuordnung einer dynamischen IP-Adresse zu einem Bestandsdatum als Eingriff in das Telekommunikationsgeheimnis zu werten ist.
[1196] *Albrecht/Kilchling* 2011, 224.

- Im präventiven Bereich berichten Polizeiexperten von zwei Fällen in denen mangels vorhandener Geo- und Verkehrsdaten die Abwehr einer konkreten Todesgefahr misslungen sei.[1197]
- Die Telekommunikationsanbieter berichten von einem Rückgang der Abfragen seit dem Urteil des *Bundesverfassungsgerichts*.[1198] Bezüglich der Speicherpraxis der Unternehmen, ergebe sich ein sehr unübersichtliches Gesamtbild.[1199] Dabei zeige sich, dass eine Abrechnungsrelevanz von Verkehrsdaten vielfach nach Ansicht der Anbieter auch bei Flatrate-Tarifen[1200] und Prepaid-Karten[1201] bestünde.
- Ein Quick-Freeze-Verfahren bewerten die befragten Praktiker als kein taugliches Äquivalent, da sie keine retrograden Daten erfasse.[1202]

Insgesamt zeigen beide Studien des Max-Planck-Instituts, dass zwar ein großes Interesse an Verkehrsdaten seitens der Ermittlungsbehörden vorhanden ist, aber keine nachweisbaren Schutzlücken ohne eine Vorratsdatenspeicherung bestehen. Allein im Bereich der Zuordnung von IP-Adressen zu Bestandsdaten wird eine Schutzlücke diagnostiziert.

In Bezug auf die Studie aus dem Jahr 2011 wurde der Verdacht geäußert, dass diese nach den Wünschen des Bundesjustizministeriums verfasst worden wäre.[1203] Hintergrund dessen ist, dass eine vorläufige Version des Gutachtens im August 2010 erstmals dem Justizministerium vorgelegt worden war, die zu anderen Ergebnissen kam.

[1197] *Albrecht/Kilchling* 2011, 225.
[1198] *Albrecht/Kilchling* 2011, 195.
[1199] Soweit ein Einzelverbindungsnachweis gewünscht ist werden die Daten bei zwei der großen Anbieter 80 bzw. 90 Tage gespeichert, bei den dritten bis zu 182 Tagen. Sieben Tage werden bei den Internetzentrierten Unternehmen die IP-Adressen gespeichert. Einer der Universalanbieter speichert IP-Adressen über Festnetz 30 Tage speichert. Über Mobilfunk hingegen nur bis zum Verbindungsende. Bei einem anderen werden diese Daten, wie auch E-Mailverbindungsdaten gar nicht mehr gespeichert. Während ein dritter sei wie IMEI und ISEI behandelt. Portnummern und Mac-Adressen werden bei einigen Anbietern tatsächlich überhaupt nicht gespeichert. Uneinheitlich werden auch Geodaten gespeichert. Abrechnungsrelevante Verkehrsdaten werden häufig nach 30 Tagen gelöscht. Bei einem Anbieter werden die Daten bis 80 Tage nach Rechnungsversand vorgehalten (also insgesamt 90 Tage plus den Rechnungsmonat). Eingehende Verbindungen werden zwar von einem Anbieter gespeichert, ein anderer hält sie nur für 3 bis 7 Tage vor (Speicherfrist für das Störungsmanagement (vgl. § 100 TKG)); so *Albrecht/Kilchling* 2011, 196.
[1200] So berichtet etwa ein Anbieter, dass da diese Kommunikationsvorgänge, die zwar im Endkundenverhältnis auf einer Flatrate basieren, im Inter-Carrier-Verhältnis abrechnungsrelevant seien und daher dennoch häufig gespeichert würden. Daher würden auch bei Inlandsgesprächen auf Flatrate-Basis zumindest von einem Anbieter für wenige Tage, die Daten gespeichert (im Mobilfunkbereich würden sowohl aus- wie auch eingehende Verbindungen 30 Tage erfasst). „Vor diesem Hintergrund führt ein Unternehmen aus, dass es Flatrates im Hinblick auf die Abrechnungserfordernisse im Mobilfunk faktisch nicht gebe. Anders sei die Situation im Internet; dort gebe es fast ausschließlich Flatrate-Verträge“, *Albrecht/Kilchling* 2011, 176.
[1201] Hier ist die Praxis sehr unterschiedlich, während ein Anbieter alle Daten speichert, speichert ein anderer überhaupt nicht, dazu ausführlich *Albrecht/Kilchling* 2011, 176 f.
[1202] *Albrecht/Kilchling* 2011, 227.
[1203] *Der Spiegel,* 11/2012 „Gutachten nach Wunsch“.

Grundlage dieses Gutachtens waren allein Interviews mit Praktikern. Eine Verknüpfung der Interviews mit der Auswertung statistischer Erhebungen folgte erst in der zweiten Fassung und führte laut Angaben der Verfasser zu modifizierten Gesamtresultaten.[1204]

4.4.2.2.2 Erhebungen des Bundeskriminalamts

Das Bundeskriminalamt hat im Oktober 2010 der Presse eine Sammlung von Beispielsfällen aus der polizeilichen Praxis vorgestellt, die „die Bedeutung von Mindestspeicherfristen für die Strafverfolgung und Gefahrenabwehr" belegen sollten.[1205]

Für die Erforderlichkeit der Zuordnung einer IP-Adresse zu einem Bestandsdatum, wurde zunächst ein Fall genannt, in dem die Ermittlung des Inhabers einer IP-Adresse gescheitert war. In einem Chatroom hatte ein Nutzer Kindesmissbrauch und die Verbreitung von Kinderpornographie thematisiert. Als zweites wurde dargestellt, das es der Polizei bei einer DDoS-Attacke mangels Zuordenbarkeit der IP-Adressen nicht möglich war, die Internetnutzer davor zu warnen, dass sie Teil eines kriminellen Bot-Netzes waren.[1206] Es wurden sodann Fälle des (Computer-)Betrugs, der Datenveränderung und Computersabotage aufgezählt. Hier hätten mangels Vorratsspeicherung der IP-Zugangsdaten 80 Prozent der Hauptverdächtigen nicht identifiziert werden können.[1207] Es werden dann Suizid- und Amokankündigungen genannt als Fälle, in denen mangels Zuordnungsmöglichkeit der IP-Adresse zu einem Nutzer ein präventives Vorgehen der Polizei scheiterte. Schließlich hätte auch ein Unterstützer einer Terrororganisation (Einstellen eines Videos ins Internet) mangels gespeicherter IP-Daten nicht ermittelt werden können.

Als Beispiele, in denen mangels Zuordnung von Telefonie-Verkehrsdaten zu einem Anschlussinhaber die Aufklärung scheiterte, werden ein Fall einer telefonischen Bombendrohung in einem Krankenhaus, Anschlagsplanungen einer terroristischen Vereinigung und schließlich der Mord an einer Rentnerin und die Ermordung eines Hamas-Funktionärs in Dubai genannt. In sämtlichen Fällen hätten sich aus den telefonischen Kontakten Anknüpfungspunkte zu einem möglichen Täter oder zur Ermittlung organisatorischer Strukturen ergeben können. Mangels Verkehrsdaten hätten jedoch Anknüpfungspunkte für weitere Ermittlungen gefehlt.[1208]

Abschließend werden in der Mitteilung Fälle genannt, in denen die Standortdaten für die Ermittlungsarbeit benötigt wurden, aber mangels Speicherung die Aufklärung fehlschlug.[1209]

[1204] Auch das Max-Planck-Institut wendete sich ausdrücklich gegen die Vorwürfe, http://www.mpicc.de/shared/data/pdf/pm_02_12_vorratsdatenspeicherung.pdf.

[1205] *BKA* Mindestspeicherfristen 2010.

[1206] *BKA* Mindestspeicherfristen 2010.

[1207] Als Beispiel für einen Fall in dem eine IP-Adresse mangels Speicherung durch den Anbieter nicht zugeordnet werden konnte, wird ein Hacking-Angriff auf das Pentagon genannt, *BKA* Mindestspeicherfristen 2010, S. 3.

[1208] *BKA* Mindestspeicherfristen 2010, S. 5 f.

[1209] Genannt wird hier der Mord an einem Polizisten bei dem der flüchtige Täter per Handy ein Taxi anforderte. Sodann werden Ermittlungen wegen Schleuserei genannt. Hier hätten wegen fehlender

Eine solche Auflistung konkreter Fälle hat eine starke Wirkung, da für den Einzelnen nachvollziehbar wird, was für schwerwiegende Straftaten ohne Vorratsdatenspeicherung nicht aufgeklärt und welche Gefahren nicht abgewendet werden konnten. Es wird der Eindruck vermittelt, dass ohne diese Daten der Polizei die Hände gebunden seien.

Eine solche Argumentation ist jedoch kritisch zu hinterfragen. Denn es lässt sich nicht erkennen, ob tatsächlich Verbindungsdaten, wenn sie denn vorhanden gewesen wären, zielführend gewesen wären.[1210]

So ist etwa die Folgerung nicht zwingend, dass sich Anknüpfungspunkte für die Frage hätten ergeben können, ob die Zwickauer Terrorzelle in ein größeres Netz eingebunden war und wer sie unterstützt hat, wenn eine Vorratsdatenspeicherung erfolgt wäre.[1211] Denn ein Umgehungsverhalten durch das tatsächliche Organisationsstrukturen verschleiert werden, liegt gerade bei einer gut organisierten und seit Jahren unentdeckt im Untergrund agierenden terroristischen Vereinigung nahe.[1212]

Gegen die Argumentation mit Einzelfällen spricht sodann, dass selbst wenn diese mit einer Vorratsdatenspeicherung hätten aufgeklärt oder verhindert werden können, sich diese kaum oder gar nicht auf die „Gesamttendenz in der Entwicklung der Aufklärungsquoten“ auswirken.[1213]

Schließlich bringt die Überprüfung der in der Fallsammlung aufgeführten Tötungsdelikte durch das Max-Planck-Institut zu Tage, dass die Darstellung des Bundeskriminalamts zum Teil fehlerhaft ist. Denn tatsächlich seien die Fälle überwiegend aufgeklärt worden und zwar jeweils ohne Verkehrsdaten.[1214] Insgesamt ergebe sich aus der

---

retrograder Verkehrsdaten die Routen, Kontaktmuster, Tatorte, etc. nicht ermittelt werden können. Abschließend wird ein Fall eines mutmaßlichen Mafia-Mordes aufgeführt, der mangels der Möglichkeit auf retrograde Verkehrsdaten zuzugreifen, nicht hätte aufgeklärt werden können, da die Verkehrsdaten für die Beweisführung erforderlich gewesen wären; *BKA* Mindestspeicherfristen 2010, S.S. 6 f.

[1210] *Hoeren* in panorama, Sendung vom 1.4.2010, Überflüssige Gesetze - Wie Politiker Sicherheit vorgaukeln: „Die *BKA* Liste ist das unseriöseste was man sich vorstellen kann. Der Punkt ist hätte, hätte, hätte ist kein wissenschaftliches Argument. Das hängt von vielen Faktoren ab, ob etwas aufgedeckt hätte werden können.“

[1211] So etwa die CDU/CSU-Politiker *Merk, Uhl* und der Bundesinnenminister *Friedrich,* vgl. *Krempl,* heise online v. 16.11.2011, abrufbar unter: http://www.heise.de/-1380400.html; *Huq,* heise online v. 27.11.2011, abrufbar unter: http://www.heise.de/-1385956.html.

[1212] Zudem wäre hier eine Speicherung über zehn Jahre hin weg erforderlich um die Zeit in der die Morde passierten, zu rekonstruieren. Um Unterstützer zu ermitteln und die Organisation der NSU aufzudecken, hätte hingegen - soweit die Mitglieder der NSU überhaupt über eigene Telekommunikationsinstrumente mit ihren Unterstützern kommuniziert haben - eine Speicherung von wenigen Wochen genügt. Schließlich kann gefragt werden, ob nicht, wenn die Verfassungsschutzbehörden sauber gearbeitet hätten, nicht schon längst eine Überwachung der Telekommunikation und eventuell auch der Wohnräume der NSU möglich gewesen wäre, so dass es eines Rückgriffs auf die auf Vorrat gespeicherte Verkehrsdaten gar nicht erst bedurft hätte. Letztlich sind die Ermittlungen um die Zwickauer Terrorzelle von so vielen Pannen geprägt, so dass sich der Verweis auf diese nicht eignet um eine Vorratsdatenspeicherung zu rechtfertigen.

[1213] *Albrecht/Kilchling* 2011, 82.

[1214] Tatsächlich seien die Fälle überwiegend aufgeklärt worden und zwar jeweils ohne Verkehrsdaten, *Albrecht/Kilchling* 2011, 103 f.

Analyse der Fälle kein Indiz dafür, dass die Aufklärung bei schwerster Kriminalität durch die Entscheidung des *Bundesverfassungsgerichts* behindert worden sei.[1215] Auch ergäben „sich keine Anhaltspunkte dafür, dass in den bislang nicht aufgeklärten Tötungsdelikten auf Vorrat gespeicherte Verkehrsdaten in den Ermittlungen hätten weiter führen können".[1216]

Das Bundeskriminalamt hat neben den Einzelfällen als Beleg für die Erforderlichkeit der Vorratsdatenspeicherung, hinaus „Kernaussagen" einer internen statistischen Erhebung des Bundeskriminalamts zu den Auswirkungen des Urteils vom 2. März 2010 veröffentlicht.[1217] Dieser liegt eine interne statistische Vollerhebung zu präventiven und repressiven Auskunftsersuchen sowie in Fällen der Anschlussinhaberfeststellung bei IP-Adressen (in Verbindung mit § 113 TKG) bezogen auf 5.082 Anschlüsse zu Grunde. Dabei hätten insgesamt 4.292 Auskunftsersuchen, also rund 84 Prozent der Anfragen, nicht beauskunftet werden können.[1218]

In Bezug auf die abgerufenen Datenarten ergibt sich aus der Untersuchung, dass überwiegend (in 90 Prozent der Fälle) IP-Daten abgerufen wurden.[1219] 45 Prozent dieser Anfragen zum Inhaber einer IP-Adresse bezogen sich dabei auf den Deliktsbereich des (Computer-)Betrugs und 39 Prozent der Fälle auf die Verbreitung, den Erwerb oder Besitz kinder- und jugendpornographischer Schriften sowie auf Straftaten gegen die sexuelle Selbstbestimmung. Das Bundeskriminalamt ist der Ansicht, dass die Daten „die polizeifachliche Erforderlichkeit der Verkehrsdatenspeicherung für 6 Monate" belegen.[1220]

4.4.2.2.3 Die Polizeiliche Kriminalstatistik

Gegner der Vorratsdatenspeicherung argumentieren hingegen unter Berufung auf die polizeiliche Kriminalstatistik, dass der Beitrag der Vorratsdatenspeicherung zur Gewährleistung von Sicherheit insgesamt nur sehr gering sei.[1221] Diese weist keine verbesserte Aufklärungsquote für die Zeit in der die Regelungen zur Vorratsdatenspeicherung in Deutschland in Kraft waren auf. Dezidiert untersucht dies auch das Max-Planck-Institut in seinem Gutachten für das Bundejustizministerium aus dem Jahr 2011. Dabei wird für Informations- und Kommunikationskriminalität dargestellt, dass hier die Aufklärungsquote seit Ende der 1990er Jahre zurückgegangen sei. Gerade für das Jahr 2010, also nach der endgültigen Suspendierung der Vorratsdatenspeicherung,

---

[1215] *Albrecht/Kilchling* 2011, 105.
[1216] *Albrecht/Kilchling* 2011, 240; vgl. auch S. 105ff.
[1217] *BKA* Mindestspeicherfristen 2010.
[1218] *Maurer* 2011; in 83 Prozent der Fälle einer Negativauskunft hätten die Ermittlungen eingestellt werden müssen; vgl. auch *BKA* Statistische Datenerhebung 2011. Diese Argumentation des *BKA* wird zum Teil in Frage gestellt, das wohl auf Weisung der obersten Behörden vielfach Anfragen gestellt wurden, gerade um die Erforderlichkeit der Vorratsdatenspeicherung zu belegen, obwohl bekannt war, dass die Daten nicht mehr gespeichert waren, http://www.vorratsdatenspeicherung.de/content/view/505/79/lang,de/.
[1219] Vgl. *BKA* Statistische Datenerhebung 2011.
[1220] Fn.; so dann auch auf der SIRA-Conference *Maurer* 2011.
[1221] http://www.vorratsdatenspeicherung.de/content/view/455/79/.

sei ein klarer Anstieg der Aufklärungsquote zu verzeichnen.[1222] Aus der polizeilichen Kriminalstatistik lässt sich letztlich nicht die Notwendigkeit einer Vorratsdatenspeicherung ableiten, da diese durch weit mehr Faktoren geprägt ist.

4.4.2.2.4 Evaluationsbericht der Europäischen Kommission

Auch der Kommissionsbericht zur Vorratsdatenspeicherungsrichtlinie befasst sich mit der Frage der Bedeutung der Vorratsdatenspeicherung für die Sicherheit. Grundlage dieses Berichts bilden Mitteilungen aus den Mitgliedsstaaten. Allerdings haben lediglich neun Mitgliedstaaten vollständige Daten vorgelegt, während 19 Mitgliedsländer nur selektiv Datenmaterial übermittelt haben. Die Daten beruhen jeweils auf den im Mitgliedstaat durchgeführten Verkehrsdatenabfragen. Nachdem der Kommission im Jahr 2010 noch kein umfassendes Datenmaterial zum Beleg der Erforderlichkeit vorlag, hat sie erneut bei den Mitgliedstaaten angefragt.[1223] Daraufhin wurden von zehn Mitgliedstaaten Berichte über Einzelfälle, in denen die Verkehrsdaten notwendig gewesen wären, erstellt.[1224]

Laut Bericht seien insgesamt in den Jahren 2008 und/oder 2009 jährlich über zwei Millionen Mal Verkehrsdaten abgefragt worden.[1225] Allerdings wurde dabei scheinbar nicht zwischen dem Abruf von auf Vorrat gespeicherten Verkehrsdaten und den zu Rechnungszwecken ohnehin gespeicherten Daten differenziert. Dies führt dazu, dass die Aussage letztlich für den Beleg der Erforderlichkeit einer Vorratsdatenspeicherung ungeeignet ist.[1226]

In Bezug auf das Abrufalter der Verkehrsdaten lässt sich dem Kommissionsbericht entnehmen, dass in der Mehrzahl der Fälle die Daten innerhalb der ersten drei Monate abgerufen werden.

Alter	*Telefonfestnetz*	*Mobilfunk*	*Internetdaten*	*Aggregat*
> 3 Monate	61 Prozent	70Prozent	56 Prozent	67 Prozent
3-6 Monate	28 Prozent	18 Prozent	19 Prozent	19 Prozent
6-12 Monate	8 Prozent	11 Prozent	18 Prozent	12 Prozent
< 1 Jahr	3 Prozent	1 Prozent	7 Prozent	2 Prozent

Übersicht über das Alter von gespeicherten Daten, zu denen in neun Mitgliedstaaten, die Statistiken übermittelt haben, Zugang gewährt wurde, aufgeschlüsselt nach Art der Daten[1227]

[1222] *Albrecht/Kilchling* 2011, 88 f.

[1223] Eine ausführliche Darstellung des Entstehungsprozesses des Bewertungsberichts der Kommission findet sich bei *Albrecht/Kilchling* 2011, 77 f.

[1224] KOM (2011) 225, 2.

[1225] KOM (2011) 225, 26. Die Häufigkeit der Anfragen unterscheidet sich stark von Land zu Land. So wurden in Zypern weniger als 100 Mal Daten angefragt, während in Polen über eine Millionen Mal Daten abgefragt wurden. Diese Abweichungen werden mit Verweis auf die Einwohnerzahl, die Trends in der Entwicklung der Kriminalität, Zweckbindungen und Bedingungen für den Zugang sowie die Kosten des Datenerwerbs, erklärt.

[1226] *Albrecht/Kilchling* 2011, 133; auch wird der Evaluationsbericht kritisiert und eine unabhängige Erhebung gefordert, *Schlepper/Leese* NK 2011, 70.

[1227] Tabelle Nr. 5 basierend auf KOM (2011) 225, 26. Der Bericht enthält aber keine Aussagen dazu

Als Funktionen der Verkehrsdatenspeicherung für die Ermittlungsarbeit nennt der Kommissionsbericht, ihren großen Nutzen für die „Entwicklung von Beweisspuren“,[1228] sie sei von großem Wert für die „Einleitung strafrechtlicher Ermittlungen“[1229] und schließlich sei sie ein „wesentlicher Bestandteil von Strafermittlungen“.[1230]

Diese Aussagen bringen letztlich keinen Mehrwert, da die Annahme sich im Wesentlichen auf die Beobachtung stützt, dass die Daten in erheblichem Umfang abgefragt werden.[1231] Dem Bewertungsbericht lässt sich nicht entnehmen, ob und welche Bedeutung Vorratsdaten bei Ermittlungen im Bereich der schweren Kriminalität, insbesondere der Bekämpfung des internationalen Terrorismus, zukommt.[1232]

Die Kommission zieht sodann drei Schlüsse aus den ihr vorgelegten Informationen zum Abfrageverhalten in den Mitgliedstaaten: Zum einen würden Internetdaten häufig später abgefragt als andere Formen von Beweisdaten. Zum anderen sei für die Aufklärung von besonders schweren Straftaten häufig ein Zugriff auf ältere Verkehrsdaten erforderlich, aus denen sich dann ergebe „wie lange Straftaten vorbereitet wurden, um kriminelle Verhaltensmuster und die Beziehungen zwischen Tatbeteiligten zu erkennen und den Tatvorsatz festzustellen“.[1233] Drittens hätten unterschiedliche Zugriffsanforderungen in den verschiedenen Mitgliedstaaten zur Folge, dass grenzübergreifende Datenabfragen im Wege von Rechtshilfeersuchen, häufig sehr lang dauern und so in diesen Fällen Daten mit einem Alter von über sechs Monaten abgerufen wurden.[1234]

---

wie viele der neun Staaten überhaupt eine Speicherfrist von über einem Jahr vorgesehen hatten. Auch ergibt sich aus den Angaben nicht wie der Abruf der Daten innerhalb der ersten drei Monate erfolgt. Wenn ein ebensolcher proportionaler Abfall gegeben ist, wie er zwischen der Speicherung bis 3 Monate und der Speicherung zwischen drei und sechs Monaten besteht, wäre anzunehmen, dass bis zu 80 Prozent der Daten innerhalb der ersten 14 Tage abgefragt werden. Daher wäre eine genaue Aufschlüsselung über die Abfragen von Interesse.

[1228] KOM (2011) 225, 28 f. da sie es ermöglichen Aktivitäten und Verbindungen zwischen Verdächtigen zu erkennen. Insbesondere Standortdaten wären dabei für Strafverfolgungsbehörden, wie auch Angeklagte von großer Bedeutung. Auch für die Aufklärung von Straftaten im Zusammenhang mit der Kommunikation über das Internet, könne eine Untersuchung nur unter Nutzung der Vorratsdaten erfolgen, da etwa Gewaltandrohungen in Chatrooms häufig keine anderen Spuren hinterließen. Es werden dann zum Beleg einzelne Fallbeispiele angeführt.

[1229] KOM (2011) 225, 29 So sei die Vorratsdatenspeicherung für Fälle sexuellen Missbrauchs im Internet „unentbehrlich“. Um dies zu belegen wird etwa darauf hingewiesen, dass die von Europol geführte Operation Rescue zum Schutz von Kindern vor Missbrauch dadurch beeinträchtigt worden wäre, dass die Vorratsdaten nicht in allen Mitgliedstaaten verfügbar gewesen seien. Auch im Bereich der Computerkriminalität seien IP-Adressen oft der erste Anknüpfungspunkt für polizeiliche Ermittlungen.

[1230] KOM (2011) 225, 30 Die auf Vorrat gespeicherten Daten seien häufig von entscheidender Bedeutung für Strafverfahren und Gerichtsentscheidungen. So habe Finnland berichtet, dass 56 Prozent der angefragten Daten wichtig oder wesentlich für die Aufdeckung und/oder Verfolgung von Straftaten gewesen seien.

[1231] *Albrecht/Kilchling* 2011, 132.

[1232] *Albrecht/Kilchling* 2011, 133.

[1233] KOM (2011) 225, 27. Diese zweite Feststellung lässt sich nicht mit den angeführten Statistiken über die Abfragen begründen.

[1234] KOM (2011) 225, 27 Insgesamt bezog sich aber laut Kommissionsbericht weniger als 1 Prozent der Anfragen auf Daten, die in einem anderen Mitgliedstaat gespeichert waren.

4.4.2.2.5 Fazit

Es zeigt sich an allen Berichten, Statistiken und Erhebungen, die zum Beleg der Bedeutung der Vorratsdatenspeicherung erstellt wurden oder sich mit der Frage ihrer Erforderlichkeit auseinandersetzen, dass das Bestehen von Schutzlücken nicht qualifiziert nachgewiesen ist. Auch liegen keine verlässlichen Zahlen darüber vor in wie vielen Fällen tatsächlich mangels Vorratsdatenspeicherung Ermittlungen eingestellt werden mussten.

Allein für den Bereich der IP-Adressen, die für den gesamten Bereich der IuK-Kriminalität von besonderer Bedeutung sind, bestehen nachweislich Datenlücken.[1235] Allerdings ist auch in diesem Bereich zu beachten, dass eine Vorratsdatenspeicherung, das zeigt der Blick in Nachbarstaaten in denen Verkehrsdaten auf Vorrat gespeichert werden, kein Allheilmittel ist: Aufklärungsschwierigkeiten ergeben sich auch aus der Nutzung offener W-LAN-Bereiche, fortgeschrittener Anonymisierungstechniken und anderen Umgehungsstrategien.[1236]

Anders als die Darstellungen von Bundeskriminalamt und Kommission, die (was sich aus ihrer Rolle als Befürworter einer Vorratsdatenspeicherung erklärt) Statistiken und Fälle derart lesen und darstellen, dass die Vorratsdatenspeicherung stets als ein „unentbehrliches" Ermittlungsinstrument erscheint, wird in der Analyse des Max-Planck-Instituts deutlich, dass die Bedeutung von auf Vorrat gespeicherten Verkehrsdaten für die Sicherheit verhältnismäßig gering ist.

4.4.2.3 Tauglich, aber nicht unentbehrlich

Der Blick auf die verschiedenen Untersuchungen macht zunächst einmal deutlich, dass es an überzeugenden Belegen für die zwingende Erforderlichkeit einer Vorratsdatenspeicherung fehlt. Sie ist eben kein „Allheilmittel" für die Schwierigkeiten, die sich Ermittlungsbehörden auf Grund der Digitalisierung stellen.[1237] Auch fehlt es an Statistiken darüber, welche Daten mit welchem Alter abgerufen werden. Es ergibt sich zugleich das Bild, dass für Ermittlungsbehörden, die Speicherung von Verkehrsdaten auf Vorrat vielfältige Ermittlungsansätze verspricht – auch wenn es sich letztlich nicht um das entscheidende Instrument zur Gewährleistung von Sicherheit handelt.

Hier sei zudem darauf verwiesen, dass es zwar voraussichtlich zahlreiche Fälle gibt, in denen sich aus den Verkehrsdaten Ermittlungsansätze ergeben. Es werden aber auch, wenn Täter um eine Vorratsdatenspeicherung wissen, vermehrt Umgehungsmöglichkeiten genutzt werden,[1238] so dass die bestehenden Ermittlungsansätze trotz Vorratsspeicherung ins Leere führen können. Denn auch wenn die Verkehrsdaten auf Vorrat

[1235] So wird etwa im IuK Bericht des LKA *Baden-Württemberg* (2010) ausgeführt: „Der drastische Rückgang von erfolgreichen bestandsdatenanfragen nach dem Wegfall der Vorratsdatenspeicherung belegt eindrücklich die absolute Notwendigkeit der Schaffung einer entsprechenden gesetzlichen Regelung", LKA Baden-Württemberg, 11.

[1236] *Albrecht/Kilchling* 2011, 88.

[1237] Dass die Vorratsdatenspeicherung kein „Allheilmittel" ist, meint auch *Roggenkamp* K&R 2012, Nr. 2, Editorial.

[1238] So etwa *Breyer*, StV 2007, 214 ff., 218, der aus diesem Grund die Geeignetheit der Vorratsdatenspeicherung zu Sicherheitszwecken generell in Frage stellt.

gespeichert werden, bestehen zahlreiche Umgehungsmöglichkeiten, etwa die Nutzung des mobilen Internets[1239], der Einsatz von Anonymisierungsdiensten aus dem nicht-europäischen-Ausland, die Nutzung von Internet-Cafés, Universitäts-Netzwerken[1240] oder offener W-LAN-Zonen.

Das Datenmaterial führt vor allem eine deutliche Diskrepanz zwischen der medialen und politischen Vermittlung der Vorratsdatenspeicherung als „unentbehrliches" Instrument zur Bekämpfung von Terrorismus, schwerer Straftaten und Kinderpornographie und ihrem tatsächlichen Nutzen zu Tage. Auch die Darstellung dass das Internet ohne Vorratsdatenspeicherung ein „rechtsfreier Raum" sei,[1241] entspricht, so zeigen es die Statistiken deutlich, nicht der Realität.

Dennoch wird die Forderung nach einer Vorratsdatenspeicherung politisch immer wieder im Kontext mit Terror und Kinderpornographie, insbesondere bei akuten Verunsicherungen, wie etwa dem Anschlag des Rechtsextremen *Breivik* in Schweden oder der Aufdeckung der Zwickauer Terrorzelle gefordert – und zwar gänzlich unabhängig davon, ob eine Vorratsdatenspeicherung im konkreten Fall tatsächlich etwas genutzt hätte. Dies erklärt, warum die Vorratsdatenspeicherung als zentrales Instrument zur Gewährleistung der Sicherheit im digitalen Zeitalter wahrnehmbar ist, obwohl ein Beitrag der Vorratsdatenspeicherung zur Steigerung der Sicherheit bislang (statistisch) nicht nachgewiesen werden kann.

Fest steht jedoch auch, dass mit der zunehmenden Verbreitung von Flatrate-Tarifen immer weniger Daten ohnehin bei den Telekommunikationsanbietern gespeichert sind. Denn die Verkehrsdaten sind dann auf Grund des datenschutzrechtlichen Erforderlichkeitsgrundsatzes nicht mehr zu vertraglichen Zwecken durch die Anbieter zu speichern.[1242] Es besteht insofern eine begründete Sorge, dass es zukünftig vermehrt für Ermittlungsverfahren erforderliche Daten fehlen könnten.[1243]

4.4.3 Vorratsdatenspeicherung und die Frage: Sicherheit oder Freiheit?

Die Betrachtung der politischen Diskussion um die Vorratsdatenspeicherung hat zu Tage gebracht, dass eine Entscheidung für oder gegen sie als eine Entscheidung generell für Freiheit oder eben für Sicherheit begriffen wird. Gegner und Befürworter der Vorratsdatenspeicherung argumentieren plakativ-populistisch. Die Diskussion um die

---

[1239] Bei dem soweit nicht IPv6 genutzt wird bis heute keine Vorratsspeicherung erfolgt, vgl. zum Zugang über NAT, oben S. 25 ff.

[1240] Diese waren nach der Begründung des deutschen Umsetzungsgesetzes nicht speicherungsverpflichtet (vgl. dazu auch *Hornung,* PVS 2012, 377, 380; kritisch *Wettern* DuD 2009, 343, 345) Auch die Betreiber von Firmennetzwerken waren nach überwiegender Ansicht nicht zur Speicherung verpflichtet, wenn sie private Nutzung von Telefon und Internet gestatten, *Feldmann* NZA 2008, 1398; *Klug/Reif* 2008, RDV 2008, 89, 90; *Polenz* CR 2009, 225 ff. a.A. *Koch* NZA 2008, 911.

[1241] Vgl. Nachw. in Fn. 345.

[1242] In einem Urteil des BGH 2011 kommt zum Ausdruck, dass dieser eine Speicherung nach § 100 Abs. 1 TKG für 7 Tage billigt, soweit diese aus Gründen der Netzsicherheit erforderlich ist, BGH v. 13.1.2011, NJW 2011, 1509.

[1243] Dazu auch: *Hornung,* PVS 2012, 377, 378.

Vorratsdatenspeicherung ist hochgradig emotionalisiert und eine sachliche Diskussion ist kaum möglich.

Richtig ist auf der anderen Seite, dass die Vorratsdatenspeicherung für die Ermittler vielfältige Ermittlungsansätze verspricht. Sie kann in vielen Bereichen, vor allem aber im Rahmen der Verfolgung von Informations- und Kommunikationstechnik spezifischer Kriminalität Anknüpfungspunkte zur Aufklärung von Straftaten oder auch zur Abwehr konkreter Gefahren liefern.

Ebenso zutreffend ist aber die Argumentation der Gegner, die in der Vorratsdatenspeicherung neue Risiken für die informationelle Selbstbestimmung der Bürger und eine infrastrukturelle gesamtgesellschaftliche Überwachung erkennen.

4.5 Vorratsdatenspeicherung als Herausforderung für die Rechtsordnung

Dass der Diskurs um die Vorratsdatenspeicherung so emotionalisiert geführt wird, liegt letztlich auch daran, dass sich in ihr die Bedingungen bündeln, die das Spannungsverhältnis von Freiheit und Sicherheit verschärfen, wie es im ersten Teil dieser Arbeit dargelegt wurde. Digitale Datenverarbeitung, eine globalisierte Gesellschaftsordnung und die Bedrohung durch den internationalen Terrorismus stellen die Gewährleistung von Freiheit und Sicherheit vor neue Herausforderungen. Diese bündeln sich in der Vorratsdatenspeicherung:

- Es handelt sich um ein sicherheitspolitisches Überwachungsinstrument im Vorfeld einer Straftat und einer konkreten Gefahr, die unabhängig von einem Verdacht oder Anlass jeden Nutzer von Telekommunikation trifft. Es handelt sich insofern um eine depersonalisierte Überwachungsmaßnahme, die an einer zentralen Infrastruktur der Informationsgesellschaft anknüpft.
- In dem Konzept einer Vorratsdatenspeicherung zeigt sich die zunehmend präventive Ausrichtung der Polizeiarbeit.[1244] Die Vorratsspeicherung der Telekommunikationsverkehrsdaten ermöglicht es Kommunikations- und Bewegungsprofile (nahezu) von jedem Einzelnen zu erstellen.[1245] Dies ist auch deswegen so problematisch, weil die Nutzung von Telekommunikation heute Voraussetzung für die Ausübung einer Vielzahl an Grundrechten ist.[1246]
- Mit der Vorratsdatenspeicherung soll auf die Schwierigkeit reagiert werden, Handlungen im Internet und mittels Telekommunikation einer Person zuzuordnen, die sich erst unter den Bedingungen digitaler Datenverarbeitung entwickelt hat. Sie ist insofern auch der Versuch, eine aus Perspektive des Datenschutzrechts begrü-

[1244] Dazu oben Kap. 1.4.2.

[1245] Aus den Daten lassen sich Lebensgewohnheiten, Freundschaften, Organisationsstrukturen von Verbänden, Bewegungsprofile und schließlich bis in die „Intimsphäre“ reichende Schlüsse ziehen (etwa der Kontakt zu bestimmten spezialisierten Ärzten, o.ä.), so BVerfGE 125, 260 (319); eine ausführliche Darstellung der Analysemöglichkeiten von Verkehrsdaten findet sich bei *Kurz/Rieger* 2009, 54; vgl. zu Analysemöglichkeiten auch schon oben S. 183 ff.

[1246] Vgl. dazu oben Kap. 1.2; Kap. 2.1.3.4.

ßenswerte Entwicklung, nämlich hin zu datenfreiem Handeln ohne Speicherung sämtlicher Verbindungsdaten, im Namen der Sicherheit umzukehren.[1247]

- In der Vorratsdatenspeicherung spiegelt sich die Tendenz, zunehmend auf private Akteure im Rahmen der Erfüllung originär staatlicher Aufgaben zurückzugreifen.[1248]
- Schließlich ist die Vorratsdatenspeicherung auch deshalb ein prägnantes Beispiel für das Spannungsverhältnis von Freiheit und Sicherheit im digitalen Zeitalter, weil sie auf einer europäischen Richtlinie beruht. Sie wurde in deutsches Recht über den Umweg Europa eingeführt.[1249]

Der Ansatz, der im Rahmen der Vorratsdatenspeicherung verfolgt wird – nämlich mittels einer Überwachungsinfrastruktur dafür Sorge zu tragen, dass bestimmte Daten über jeden verfügbar sind – wird neben der Speicherung von Telekommunikationsverkehrsdaten auf Vorrat auch in Bezug auf andere Daten, wie etwa Suchmaschinen, Konto- oder Fluggastdaten, diskutiert. Wenn entsprechende Konzepte realisiert werden sollten, würde sich die Befürchtung der Gegner der Vorratsdatenspeicherung verwirklichen: die Einführung der Vorratsdatenspeicherung wäre dann tatsächlich ein Dammbruch.

Es bedarf daher der näheren Betrachtung, inwieweit die Verfassung die Einführung immer neuer Vorratsspeicherungen und anderer vorsorgender Sicherheitsmaßnahmen zu verhindern vermag. Kann die Verfassung Schutz vor dem Abdriften in einen Überwachungsstaat zu gewähren? Was bedeutet das vom *Bundesverfassungsgericht* formulierte Verbot einer totalen Erfassung und Registrierung konkret?[1250]

[1247] Dies sieht auch *Simitis*, RDV 2007, 143, 144 f.

[1248] *Grafe*, 2007, 351.

[1249] Dabei liegt die Vermutung nahe liegt, dass die Harmonisierung nur vorgeschoben wurde um sie als Richtlinie verabschieden zu können *Gausling* 2010, 34.

[1250] Bislang gibt es nur wenige Ansätze in der Literatur, die versuchen dieses Verbot zu konkretisieren. Grundlegend dazu *Roßnagel,* NJW 2010, 1238, *Ders.* DUD 2010, 544; dazu auch *Knierim,* ZD 2011, 17; kritisch äußern sich *Hornung/ Schnabel,* DVBl. 2010, 824.

5 Der Schutz der Freiheit vor neuen Herausforderungen

Das *Bundesverfassungsgericht* hat die Vorratsspeicherung der Telekommunikationsverkehrsdaten als nicht schlechthin verfassungswidrig beurteilt.[1251] Es rekurriert in diesem Zusammenhang erstmals auf ein Verbot totaler Erfassung und Registrierung der Freiheitswahrnehmung aller Bürger. Die Vorratsdatenspeicherung dürfe nicht Vorbild für weitere anlasslose Datensammlung sein. Die Identität der Verfassung verbiete, dass die Freiheitswahrnehmung der Bürger total erfasst und registriert wird.[1252] Damit hat das *Bundesverfassungsgericht* auf die Befürchtung reagiert, dass mit der Einführung einer Vorratsdatenspeicherung der Damm auf dem Weg in einen Überwachungsstaat gebrochen werde.

Dieses Verbot mutet absolut an und scheint auch dazu zu dienen die Kritiker, die den Dammbruch mit der Einführung der Vorratsdatenspeicherung fürchten, zu beschwichtigen. Es ist nicht die erste absolute Grenze, die das *Bundesverfassungsgericht* in der Rechtsprechung zum Schutz der Freiheit entwickelt hat.

Die Auseinandersetzung mit diesem Verbot ist geboten, denn im Hinblick auf die Vorratsdatenspeicherung ist in verfassungsrechtlicher Hinsicht ein Paradigmenwechsel erkennbar. Dieser führt dazu, dass in Frage steht, inwiefern klassische Schranken-Schranken im Hinblick darauf noch einen Schutz vor einer weiteren schleichenden Ausdehnung von Sicherheitsbefugnissen bieten können. Die Vorratsdatenspeicherung zeichnet sich aus, durch einen „Paradigmenwechsel der Gestaltung technischer Infrastrukturen".[1253] Es erfolgt keine Orientierung am Normalfall und sachlichen Zielen, sondern am Ausnahmefall. Die für die Informationsgesellschaft so zentrale technische Infrastruktur wird nicht entsprechend einem Schutz der Freiheitsinteressen der Bürger gestaltet – also datenschutzrechtskonform, sondern es erfolgt eine Orientierung am staatlichen Eingriffsinteresse.[1254] Gerechtfertigt wird dies im Hinblick auf neue Bedrohungsszenarien.

Im Folgenden werden die in der Rechtsprechung des Verfassungsgerichts bislang anerkannten absoluten Grenzen zunächst kurz dargestellt (Kap. 5.1). Im Anschluss wird dann erörtert, ob tatsächlich mittels absoluter Verbote Freiheitsräume effektiv geschützt werden können (Kap. 6). Abschließend wird der Frage nachgegangen inwiefern überhaupt ein begründeter Bedarf besteht für die Formulierung einer solch (vermeintlich) scharfen Grenze.

Diese Untersuchung bildet die Grundlage für die Beantwortung der Frage, ob das vom *Bundesverfassungsgericht* formulierte Verbot einer totalen Erfassung und Registrie-

[1251] Zum Urteil des Verfassungsgerichts bereits oben, S. 155 ff.
[1252] BVerfGE 125, 260 (324).
[1253] *Hornung,* PVS 2012, 377, 389.
[1254] *Hornung,* PVS 2012, 377, 389.

A. Moser-Knierim, *Vorratsdatenspeicherung,* DuD-Fachbeiträge,
DOI 10.1007/978-3-658-04156-4_5, © Springer Fachmedien Wiesbaden 2014

rung geeignet ist ein Abdriften in einen Sicherheits- und Überwachungsstaat zu verhindern.[1255]

5.1 Absolute Grenzen in der Rechtsprechung des Bundesverfassungsgerichts

Das *Bundesverfassungsgericht* hat verstärkt in letzten Jahren versucht mittels „absoluter Grenzen" in seiner Rechtsprechung das staatliche Überwachungsstreben zu beschränken.[1256] Es hat in seiner Rechtsprechungstradition einen „unantastbaren Bereich privater Lebensgestaltung" entwickelt, welcher vor staatlichem Zugriff „absolut" geschützt sein soll. Es hat dann ein Verbot der Bildung vollständiger Persönlichkeitsabbilder formuliert und schließlich nunmehr im Urteil zur Vorratsdatenspeicherung das Verbot einer totalen Erfassung und Registrierung formuliert.[1257]

Die „absolut" geschützten Bereiche und „absoluten" Verbote vermitteln den Eindruck, dass das Grundgesetz bestimmte Freiheitsräume vollkommen schützen würde. Es wirkt, als gebe es Sphären in die der Staat niemals eindringen darf und Maßnahmen, die der Staat unter keinen Umständen ergreifen darf. Ob diese Eingriffsschranken tatsächlich so wirkmächtig sind, wie sie klingen, soll untersucht werden, indem sowohl der unantastbare Kernbereich privater Lebensgestaltung (Kap. 5.1.1) als auch das Verbot der Bildung vollumfänglicher Persönlichkeitsprofile (Kap. 5.1.2) im Hinblick auf ihre freiheitssichernde Wirkung untersucht werden.

5.1.1 Der „unantastbare Bereich privater Lebensgestaltung"

Absolut vor dem Zugriff staatlicher Gewalt zu schützen ist nach ständiger Rechtsprechung des *Bundesverfassungsgerichts* ein „unantastbarer Bereich privater Lebensgestaltung".[1258]

Schon im *Elfes*-Urteil im Jahr 1957 stellte das *Bundesverfassungsgericht* fest, dass sich aus den Gewährleistungen der Art. 19 Abs. 2, Art. 1 Abs. 3 und Art. 2 Abs. 1 GG ein „letzter unantastbarer Bereich menschlicher Freiheit" ergebe, der der „Einwirkung der gesamten öffentlichen Gewalt entzogen" sei, da dies der Grundbaustein von Freiheit und Würde sei.[1259]

Ausgehend von dieser These entwickelte das *Bundesverfassungsgericht* in der Rechtsprechung zum Allgemeinen Persönlichkeitsrecht die „Sphärentheorie".

[1255] Dem wird dann in Kap. 5 nachgegangen.

[1256] *Roßnagel* 2011b, 46.

[1257] BVerfGE 125, 69 (324).

[1258] Dabei ist zwischen dem Schutz der Intimsphäre und dem sog. Kernbereich zu differenzieren. Dazu ausführlich *Desoi/Knierim*, DÖV 2011, 398; stRspr zum unantastbaren Bereich privater Lebensgestaltung in Zusammenhang mit der Intimsphäre: BVerfGE 6, 32 (41); 6, 389 (433); 27, 1 (6); 32, 373 (379); 33, 367 (376); 34, 238 (245); 35, 35 (39); 54, 143 (146). In Zusammenhang mit dem Kernbereichsschutz BVerfGE 80, 367 (373); 89; 69 = NJW 1993, 2365 (2366); seitdem bezeichnet das Gericht diesen Bereich als „Kernbereich privater Lebensgestaltung", so BVerfGE 90, 145 (171); 109, 279 (LS 4); 113, 348 (391); 120, 274 (335).

[1259] BVerfGE 6, 32 (41). Die Ausführungen im Folgenden entsprechen vielfach bzw. beruhen im Wesentlichen auf dem Aufsatz *Desoi/Knierim*, DÖV 2011, 398; ausführlich zum Kernbereich privater Lebensgestaltung, vgl. auch *Dammann* 2011.

Ein solches Modell verschieden intensiv zu schützender Schichten geht auf eine zivilrechtliche Theorie zum Allgemeinen Persönlichkeitsrecht von *Hubmann* zurück,[1260] die zunächst Eingang in die Rechtsprechung des *Bundesgerichtshof*[1261] fand und schließlich vom *Bundesverfassungsgericht* verfassungsdogmatisch ausgebaut wurde. Das Gericht nimmt an, dass das Allgemeine Persönlichkeitsrecht in verschieden schutzwürdige Sphären unterteilt werden könne. Diese seien nach dem Grad ihres Sozialbezugs voneinander zu unterscheiden.[1262] Absolut geschützt und damit abwägungsfest[1263] sei die im Kern des Persönlichkeitsrechts liegende Intimsphäre.[1264] Das Gericht definiert dabei die Intimsphäre nicht positiv,[1265] sondern grenzt sie über ein Negativkriterium von der weiteren Privatsphäre ab. Die Intimsphäre würde verlassen, wenn ein Verhalten des Menschen in der „Außenwelt" anknüpfe.[1266]

Dass jedenfalls der unantastbar geschützte Bereich nicht berührt sei, wenn ein „Sozialbezug" bestünde, hatte das Gericht schon im Urteil *Homosexuelle I* festgestellt.[1267] Indizien für einen Sozialbezug sind nach Rechtsprechung des Verfassungsgerichts die Kommunikation mit anderen,[1268] die Abgeschlossenheit oder Öffentlichkeit der Situation,[1269] die örtlichen Bedingungen[1270] oder auch der Wille des Einzelnen.[1271]

Da es unter den Bedingungen moderner Datenverarbeitung – auf Grund der vielfältigen Verknüpfungs- und Verwendungsmöglichkeiten – kein belangloses Datum mehr gibt, hat das *Bundesverfassungsgericht* im Volkszählungsurteil das Recht auf informationelle Selbstbestimmung anerkannt.[1272] Dies wurde als Abkehr von der Sphärentheorie gewertet.[1273] Denn anders als die Konzeption der Privatsphäre ist das Recht auf informationelle Selbstbestimmung nicht daten- sondern verarbeitungsorientiert.[1274] Dies

[1260] *Hubmann*, 1953, 216 ff.
[1261] BGHZ 13, 334 (338).
[1262] Im Zentrum liegt die absolut geschützte Intimsphäre um die sich die Sozialsphäre und die Öffentlichkeitsphäre legen. Je nachdem auf welcher Stufe ein Eingriff in die Privatsphäre einzuordnen ist, eine ausführliche Darstellung findet sich bei *Desoi/Knierim*, DÖV 2011, 398
[1263] Das Gericht betont wiederholt, dass innerhalb dieser Intimsphäre „kein Raum für eine Abwägung mit anderen Interessen" bestünde und sie unantastbar sei. So etwa BVerfGE 34, 238 (248); 35, 35 (39); 35, 202 (220).
[1264] Dilemmatisch an dieser Konzeption war jedoch, dass das Gericht diese Sphäre anhand des Merkmals „Sozialbezug" von der weiteren Privatsphäre, in die Eingriffe gerechtfertigt werden können, abgrenzte, da insofern dieser Konzeption das Menschenbild eines vollkommen isolierten Individuums zu Grunde gelegt wurde.
[1265] Lediglich eine Schwangerschaft sowie die sexuelle Identität wurden von der Rechtsprechung des *BVerfG* positiv der Intimsphäre zugeordnet BVerfGE 39, 1 (42); 49, 286 (301).
[1266] BVerfGE 27, 1 (7).
[1267] BVerfGE 6, 389 (433).
[1268] BVerfGE 6, 389 (433).
[1269] BVerfGE 27, 1 (8).
[1270] BVerfGE 34, 238 (247); 54, 143.
[1271] BVerfGE 32, 373 (380).
[1272] Zum Volkszählungsurteil bereits oben, S. 81 ff.
[1273] *Benda*, DUD 1984, 86, 88; *Simitis*, NJW 1984, 394 ff., 402; *Tinnefeld*, NJW 1993, 1118; *Denninger* 1990, 380 f.
[1274] *Simitis*, NJW 1984, 394, 402.

ist folgerichtig, da das Recht auf informationelle Selbstbestimmung von seiner Konzeption her quer zu allen drei Sphären liegt.[1275]

In der Entscheidung zur Verwertbarkeit von Tagebucheintragungen im Strafverfahren aus dem Jahr 1989 hat das *Bundesverfassungsgericht* den unantastbaren Bereich privater Lebensgestaltung wieder aufgegriffen.[1276] Anders als zuvor führt das Gericht aus, dass zur Bestimmung des Kernbereichs sowohl auf formale als auch auf inhaltliche Komponenten abzustellen sei. Entscheidend seien der Wille des Betroffenen (Geheimhaltungsinteresse), der Inhalt (höchstpersönlich) und ob und wie intensiv ein Sachverhalt die Sphäre anderer oder die Belange der Gemeinschaft berührt.[1277] Die Tagebuchaufzeichnungen seien aufgrund ihres Inhalts[1278] für die Wahrheitsfindung im Strafverfahren erforderlich, daher berühren sie nach Ansicht der das Urteil tragenden Richter[1279] die Belange der Gemeinschaft und seien dementsprechend nicht absolut geschützt.[1280] Letztlich wird durch die Betonung des Einzelfalls und die Abgrenzung anhand von Maß- und Wertbegriffen wie „Intensität" der Kernbereich einer Abwägung geöffnet.

Erstmals außerhalb des Allgemeinen Persönlichkeitsrechts hat das *Bundesverfassungsgericht* in der Entscheidung zum großen Lauschangriff im Jahr 2004 einen unantastbaren Kernbereich privater Lebensgestaltung anerkannt.[1281] Diesen hat es innerhalb des Schutzbereichs von Art. 13 GG entwickelt.

Das Gericht leitet die Gewähr des Kernbereichs nicht mehr aus der Wesensgehaltsgarantie ab, sondern allein aus der Garantie der Menschenwürde.[1282] Den Kernbereich

---

[1275] *Lang*, BeckOK-GG, Art. 2, Rn. 3; *Kunig*, in: *Münch*/*Kunig*, GG 2012, Art. 2 Rn. 38; *Hornung*, MMR 2004, 3, Rn. 3.

[1276] BVerfGE 80, 367 (374).

[1277] BVerfGE 80, 367 (374).

[1278] Es handelte sich dabei um Aufzeichnungen, die über ein halbes Jahr vor der dem Beschwerdeführer zur Last gelegten Tat verfasst worden waren. Dieser hatte in einem schriftlichen inneren Monolog seine Angst vor einem gewaltsamen sexuellen Übergriff auf eine Frau Ausdruck verliehen. Dazu *Amelung*, NJW 1990, 1753. Die Tagebuchaufzeichnungen wurden für die gutachterliche Beurteilung der Schuldfähigkeit des Angeklagten in das Verfahren eingeführt.

[1279] Die Entscheidung erging mit 4:4 Stimmen, nach der abweichenden Meinung wären die Tagebuchaufzeichnungen dem unantastbaren Bereich zuzuordnen gewesen, BVerfGE 80, 367 (376).

[1280] BVerfGE 80, 367 (378); In der Literatur wurde die Argumentation des Gerichts als „zumindest partielle Wiederbelebung der Sphärentheorie" bewertet, *Amelung*, NJW 1990, 1753, Rn. 1755, Fn. 20. „Daran ist richtig, dass das im Rahmen der Sphärentheorie zur Bestimmung des unantastbaren Bereichs entwickelte Abgrenzungskriterium des Sozialbezugs auch weiterhin vom Gericht verwendet wurde. Mit der Tagebuchentscheidung hat das *BVerfG* zwar seine ständige Rechtsprechung zum Schutz eines unantastbaren Bereichs fortgesetzt, nicht jedoch an der ursprünglichen Konzeption der Sphärentheorie festgehalten. Es hat sich nämlich nicht auf das im Rahmen der Sphärentheorie verwendete Abgrenzungskriterium des Sozialbezugs zur Bestimmung des Schutzbereichs beschränkt, sondern dieses weiterentwickelt, indem es nun auf den Willen des Einzelnen, der nicht mehr nur Indiz für den Sozialbezug ist, und auf den Inhalt einer Information abstellt, worin die Anerkennung des Menschen als sozialen Wesens zum Ausdruck kommt", so *Desoi/Knierim*, DÖV 2011, 398, 400.

[1281] BVerfGE 109, 279.

[1282] BVerfGE 109, 279 (LS 4); Dies ist wohl auch den Besonderheiten des Falls geschuldet. Gegenstand des Verfahrens war eine Verfassungsänderung und das Gericht prüfte daher allein anhand

selbst, bestimmt das Gericht, auch hier nicht abstrakt, sondern betont, dass die Besonderheiten des Einzelfalls maßgeblich seien. Als typische Fälle für einen Kernbereichsbezug nennt das Gericht Äußerungen innerster Gefühle oder Ausdrucksformen der Sexualität.[1283]

Das *Bundesverfassungsgericht* betont im Urteil, dass der Kernbereich privater Lebensgestaltung absolut geschützt sei. Es sieht ihn aber nicht durch ein räumliches Substrat geschützt. Stattdessen entwickelt das Gericht ein zweistufiges Schutzkonzept, dass es aus der Garantie der Unantastbarkeit des Kernbereichs privater Lebensgestaltung ableitet. Demnach ist zwischen Erhebung und Verwertung zu unterscheiden.

Auf der ersten Stufe der Erhebung der Daten, müsse gewährleistet werden, dass soweit als möglich die Erhebung von Kernbereichsdaten unterbleibe. Dazu bedürfe es „besonderer gesetzlicher Vorkehrungen, die den Kernbereich der privaten Lebensgestaltung schützen".[1284] Wegen des hohen Eingriffsgewichts einer Ermächtigungsnorm, in deren Rahmen die Erhebung von kernbereichsrelevanten Daten wahrscheinlich ist, müsse der Eingriff zum einen unter Richtervorbehalt gestellt werden. Zum anderen müsse durch weitere verfahrensrechtliche Regeln Sorge getragen werden, dass, sobald die Erhebung von Daten mit Kernbereichsbezug erkannt wird, die Erhebung abgebrochen wird.

Auf der zweiten Stufe, der Auswertung der Daten, müssten dann Verwendungs- und Verwertungsverbote greifen. Denn in Fällen, in denen die Erhebung von kernbereichsrelevanten Daten unvermeidbar sei, etwa wenn erst Informationen zur Kenntnis genommen werden, bevor sich ihr Kernbereichsbezug herausstellt, müssten die aufgefundenen und erhobenen kernbereichsrelevanten Daten unverzüglich gelöscht und ihre Verwertung ausgeschlossen werden.[1285]

Auch wenn es an einer klaren und abstrakten Definition des absolut geschützten Kernbereichs privater Lebensgestaltung fehlt und die Bestimmung durch die Einzelfallbezogenheit letztlich einer Abwägung gleichkommt, hat der Kernbereichsschutz zumindest durch die verfahrensrechtliche Ausgestaltung einen starken Einfluss auf die Ausgestaltung konkreter Gesetzgebungsverfahren entwickelt.[1286] Das *Bundesverfassungsgericht* hat insbesondere in den Urteilen zum Großen Lauschangriff und zur Online-Durchsuchung aus der Garantie des unantastbaren Kernbereichs umfassende Verfahrensvorschriften abgeleitet.[1287] Der Topos eines unantastbaren Kernbereichs ist hier eine wichtige Argumentationsfigur zur Begrenzung staatlicher Eingriffe.[1288]

---

der Maßstäbe aus Art. 79 Abs. 3 GG, - also Art. 1 Abs. 1 und Art. 20 Abs. 3 GG. Das Gericht hat jedoch auch später an dieser verfassungsrechtlichen Begründung des Kernbereichs allein aus Art. 1 Abs. 1 GG festgehalten, vgl. etwa BVerfGE 120, 274 (335).

[1283] BVerfGE 109, 279 (314).

[1284] BVerfGE 109, 279 (318); so dann auch BVerfGE 113, 348 (399); 120, 274 (328).

[1285] BVerfGE 120, 274 (338); unter Verweis auf BVerfGE 109, 279 (313); 113, 348 (391).

[1286] Dies führen etwa die Entscheidungen zum Großen Lauschangriff oder zur Onlinedurchsuchung vor Augen, BVerfGE 109, 279; 120, 274.

[1287] BVerfGE 109, 279; 120, 274.

[1288] „Ungeachtet der Kritikpunkte bleibt aber festzuhalten, dass das Gericht seine Linie der Begrenzung staatlicher Überwachungsmaßnahmen insgesamt konsequent fortsetzt. Dazu gehört auch der

5.1.2 Verbot der Bildung von Persönlichkeitsprofilen

Absolut verboten, ist nach Ansicht des *Bundesverfassungsgerichts* auch die Erstellung umfassender Persönlichkeitsprofile. Es sei „mit der Menschenwürde (…) nicht zu vereinbaren, wenn der Staat das Recht für sich in Anspruch nehmen könnte, den Menschen zwangsweise in seiner ganzen Persönlichkeit zu registrieren und zu katalogisieren (…) und ihn damit wie eine Sache zu behandeln, die einer Bestandsaufnahme in jeder Beziehung zugänglich ist", so das Gericht in der Mikrozensus-Entscheidung.[1289] Konkretisiert hat das Gericht dies im Volkszählungsurteil: „Eine umfassende Registrierung und Katalogisierung der Persönlichkeit durch die Zusammenführung einzelner Lebensdaten und Personaldaten zur Erstellung von Persönlichkeitsprofilen" sei „unzulässig".[1290] Das Gericht führt weiter aus, dass im Fall der Volkszählung keine Persönlichkeitsprofile erstellt würden, da „die Zusammenführung von im Rahmen der Volkszählung 1983 erhobenen Daten oder deren Verbindung mit bei den Statistischen Ämtern bereits vorhandenen Informationen" es nicht ermögliche, „Teilabbilder der Persönlichkeit anzufertigen, die mit der Würde des Menschen nicht vereinbar sind".[1291] Das Gericht betont auch später, dass die Erstellung eines Persönlichkeitsprofils oder eines umfassenden Bewegungsbildes unzulässig sei.[1292]

Die Verfassungswidrigkeit eines solchen Persönlichkeitsprofils folgert das Gericht aus der Menschenwürdegarantie. Gerade auch unter den Bedingungen digitaler Datenverarbeitung müsse der Mensch in seiner Würde geachtet werden. Dabei darf er auch nicht im Rahmen der Datenverarbeitung zum Objekt staatlichen Handelns werden.

Dieses Verbot wurde allerdings nie weiter konkretisiert. Kritisiert wird daher, dass es sich bei dieser absolut anmutenden Eingriffsschranke, letztlich nur um ein theoretisches Konstrukt handele. Denn egal wie umfassend Profile erstellt werden, wurde ein Verstoß bislang nie festgestellt.[1293] Grundsätzlich wurde kritisiert, dass der Begriff ungenau und für eine Abgrenzung ungeeignet sei.[1294] *Bull* betont, dass die Herstellung von Persönlichkeitsprofilen vielmehr häufig sozialadäquat sei.[1295]

Lediglich im Jahr 2006 erkannte das *Bundesverfassungsgericht* an, dass mit der Zugriffsbefugnis des § 31 PolG NW „angesichts der Menge und Vielfalt der personenbezogenen Daten, die heute − bei allen öffentlichen oder privaten Stellen zusammengenommen − über nahezu jede Person vorhanden sind, der von der Verfassung nicht zugelassenen Möglichkeit zumindest" angenähert werde, „dass Daten mit anderen Datensammlungen zu einem teilweise oder weitgehend vollständigen Persönlichkeitsbild zusammengefügt werden". Dies gelte insbesondere, da „auch sämtliche Datenbestände privater Stellen („Stellen außerhalb des öffentlichen Bereichs") betroffen" sind, „in denen sich ein ganz wesentlicher Anteil aller gespeicherten personenbezogenen Daten befindet". Das Gericht verweist beispiel-

---

im Ergebnis überzeugende Schutz des Kernbereichs privater Lebensgestaltung." *Eifert*, NVwZ 2008, 521.

[1289] BVerfGE 27, 1 (6).

[1290] BVerfGE 65, 1, 42 (53).

[1291] BVerfGE 65, 1 (54).

[1292] BVerfGE 112, 304 (319). Im Sinne des Verbots der Erstellung eines Bewegungsabbildes BVerfGE 120, 378 (418 ff.).

[1293] *Simitis* in *Simitis,* BDSG Komm 2011, § 1, Rn. 95.

[1294] *Vogelsang,* 1987, 165.

[1295] *Bull* 2011, 128.

haft auf Kundenkartensystemen von Kaufhäusern, mit denen „Informationen über das private Einkaufsverhalten“ erhoben werden. Verfassungskonform müsse § 31 PolG NW so ausgelegt werden, dass er zu keiner „umfassenden Registrierung und Katalogisierung der Persönlichkeit“ ermächtige. Er erlaube daher auch nicht „die Zusammenführung einzelner Lebens- und Personaldaten zur Erstellung von Persönlichkeitsprofilen der Bürger“.[1296]

Über den konkreten Fall hinaus ist neben der Tatsache, dass das *Bundesverfassungsgericht* hier auch privat gespeicherte Daten berücksichtigt, die Feststellung des Gerichts von Bedeutung, dass soweit „die Erhebung und Verknüpfung entsprechender Daten der Erstellung eines Persönlichkeitsprofils nahe“ komme, dies einen „besonders intensiven Grundrechtseingriff“ ermögliche.[1297]

Erstaunlich in Anbetracht dieser Feststellung ist, dass das *Bundesverfassungsgericht* im Urteil zur Vorratsdatenspeicherung mit keinem Wort auf das Verbot der Erstellung umfassender Persönlichkeitsprofile eingeht. Dies hätte in Anbetracht der umfassenden Analysemöglichkeiten nahegelegen. Daran zeigt sich letztlich die Schwäche des Verbots der Profilbildung, denn einschlägig ist das Verbot der Profilbildung in der Praxis nie.

5.1.3 Absolut und unantastbar?

Die Formeln von einem „unantastbaren Kernbereich privater Lebensgestaltung“ und einer mit der Menschenwürdegarantie unvereinbaren Profilbildung klingen nach einer absoluten und wirkungsstarken Begrenzung. Sie muten an wie strikte Verbote, die eindeutig und kraftvoll staatliche Eingriffe beschränken. Sie vermitteln den Eindruck den staatlichen Wissensdurst umfassend, eben absolut, und vor jeglichem Zugriff zu schützen. Allerdings ist im Hinblick auf den Kernbereich privater Lebensführung, das Verbot von Persönlichkeitsprofilen und dem Verbot totaler Erfassung und Registrierung fraglich, ob diese vermeintlich absoluten Grenzen, tatsächlich so absolut und unantastbar – also keiner Abwägung zugänglich[1298] – sind, wie sie klingen oder ob diese Formulierungen nicht mehr rhetorisch als normativ wirken.

[1296] BVerfGE 115, 320 (351).
[1297] BVerfGE 115, 320 (350 f.).
[1298] Zum Auslegung des Begriffs „unantastbar“, vgl. oben S. 75

6 Das Dilemma absoluter Grenzen

Zum Teil wird mit Verweis auf die Tagebuch-Entscheidung angenommen, dass das *Bundesverfassungsgericht* gar keine absoluten Verbote aus der Menschenwürdegarantie ableite.[1299] Es zeigt sich an der Tagebuchentscheidung ein Dilemma, das immer wieder zu Tage tritt. Es werden absolute Verbote formuliert, die dann tatsächlich nie einschlägig sind. Die Gründe für das Versagen absoluter Grenzen sollen im Folgenden erörtert werden.

6.1.1 Relativität absoluter Begriffe

Zwar gibt es absolute Begriffe, wie „unantastbar" oder „total", diese sind aber tatsächlich nur die Beschreibung eines utopischen Zustands. Absolute Verbote klingen total, sind tatsächlich aber relativ. Es gibt insofern keine absoluten Eingriffssperren.[1300]

Dies fördert sowohl eine weitergehende Analyse der Sphärentheorie und des Konzepts eines „unantastbaren Kernbereichs privater Lebensgestaltung" zu Tage, als auch eine Analyse der Rhetorik im Urteil zur Vorratsdatenspeicherung.

6.1.1.1 (Un-)Antastbar

In der Rezeption der verfassungsgerichtlichen Rechtsprechung zum Schutz der Intimsphäre wurde kritisiert, dass das Gericht zwar den „unantastbaren Bereich privater Lebensgestaltung" gebetsmühlenartig wiederholt, aber die Intimsphäre selbst nicht definiert. Die Kritik wird unter dem Stichwort „Relativität der Sphären" zusammengefasst.[1301]

Argumentiert wird, dass die Schwierigkeit, eine Situation einer der drei Sphären zuzuordnen, bestünde und dass jeder Mensch die Situationen, die er persönlich als intime, private oder öffentliche Angelegenheiten behandelt wissen will, anders einordnet.[1302] Darüber hinaus sei das Abgrenzungskriterium des Sozialbezugs ungeeignet und führe ins Leere. Deutlich zeigt sich dies am Beispiel Sexualität. Denn einerseits wird diese im Alltagsverständnis der Intimsphäre zugeordnet, obwohl sie stets einen Sozialbezug voraussetzt und so nach der sphärenorientierten Betrachtung des Verfassungsgerichts aus der Intimsphäre heraustritt.[1303]

[1299] *Isensee* 2003, 32. Er erkennt aber dennoch die Würde des Menschen als Grenze staatlicher Schutzpflichten an. In der Tagebuch-Entscheidung hatte das BVerfG argumentiert hier, dass die Verwertung des Tagebuchs nicht den Kernbereich privater Lebensgestaltung betreffen würde, da es darauf ankäme, ob die Inhalte höchstpersönlichen Charakter hätten. Hier bestünde ein Bezug auf eine Straftat, so dass die Tagebuchaufzeichnungen nicht dem Kernbereich zuzuordnen seien, BVerfGE 80, 367 (374).

[1300] *Simitis,* in: *Simitis,* BDSG Komm 2011, § 1 Rn. 97.

[1301] *Rohlf* 1980, 80 ff.; *Mückenberger*, KJ 1984, 1; *Podlech*, in: AK-GG, 1984, Art. 2, Rn. 35; *Mangoldt/ Klein/ Starck*, 3. Aufl. 1985, Art. 2 Rn. 11; *Isensee*/ *Kirchof*, HdStR Bd. VI, 1. Aufl. 1989, § 152 Rn. 38; s. auch *Albers* 2005, 211.

[1302] *Albers* 2005, 211; *Hufen*, JuS 2010, 1, 9. Die Ausführungen sind zum Teil bereits in *Desoi/Knierim*, DÖV 2011, 398 veröffentlicht worden.

[1303] *Rohlf* 1980, 79.

A. Moser-Knierim, *Vorratsdatenspeicherung,* DuD-Fachbeiträge,
DOI 10.1007/978-3-658-04156-4_6, © Springer Fachmedien Wiesbaden 2014

Die Wurzel dieser Relativität der Sphären liegt darin, dass der Sphärentheorie das Menschenbild eines sozial ungebundenen Individuums zu Grunde liegt. Daher verkennt die Sphärentheorie, dass der Mensch als gesellschaftsbezogenes und gesellschaftsgebundenes Wesen Schutz der Privatheit gerade auch im sozialen Kontakt benötigt.[1304] Für die freie Entwicklung der Persönlichkeit als Kind wie als Erwachsener wird Kommunikation und Informationsaustausch benötigt.[1305] Die Intimsphäre in der Konzeption des Verfassungsgerichts beschränkt sich jedoch aufgrund der Abgrenzung über den Sozialbezug auf einen Bereich der Nichtkommunikation, in dem der Einzelne als äußerlich vollständig isoliertes Individuum im stillen Kämmerlein handelt und dessen Auswirkungen auch keinerlei Auswirkungen auf die Umwelt haben.[1306]

Zudem wurde an der Konzeption der Intimsphäre kritisiert, dass sie dogmatisch unklar ist und davon ausgegangen werden könne, dass im Einzelfall immer dann der Intimbereich als nicht berührt angesehen wird, wenn seine Einschränkung für notwendig erachtet wird.[1307] Der absolut geschützte Bereich der Intimsphäre würde so praktisch auf null reduziert.[1308] Dies bestätigt schließlich die Entscheidung zur Verwertung von Tagebucheinträgen im Strafverfahren.[1309] Eben weil die Tagebuchstellen für das Verfahren relevant waren, wurde in ihrer Verwertung keine Verletzung des Kernbereichs privater Lebensgestaltung gesehen – obwohl doch gerade Tagebücher dazu dienen den inneren Monolog zu verschriftlichen und insofern im Allgemeinen als höchst intim einzuordnen sind.

Mit dem Schutz einer über den Sozialbezug abgrenzbaren unantastbaren Intimsphäre beschwört das *Bundesverfassungsgericht* zwar die rechtsstaatlich absolut garantierte Menschenwürde, im Ergebnis bleibt es jedoch bei einer Beschwichtigungsfloskel, da der Mensch ja gerade als soziales Wesen existiert und so ein Eingriff in die Intimsphäre nie anzunehmen sein wird. Denn letztlich gibt es kein menschliches Verhalten, bei dem kein Sozialbezug vorliegt.

Aber auch der von einem Sozialbezug unabhängige Schutz über eine inhaltliche Bestimmung des absolut geschützten Kernbereichs privater Lebensgestaltung zeigt sich realiter als relativ. Entsprechend ist auch die Konzeption des „unantastbaren Kernbereichs" des *Bundesverfassungsgerichts* auf heftige Kritik in der Literatur gestoßen.[1310] Denn schon die Bestimmung des Kernbereichs anhand des Inhalts zeigt, dass diese Methode „dilemmatisch" ist:[1311] Wenn nur anhand des Inhalts im Einzelfall festgestellt werden kann, ob eine Information bzw. ein Datum höchstpersönlich ist, muss diese Information zunächst bekannt sein. Schließlich kann sie nur dann auf ihren materiellen Gehalt hin untersucht werden. Das Dilemma besteht also darin, dass stets zunächst der

[1304] *Rohlf* 1980, 79.
[1305] *Luhmann* 1999, 68; *Hofmann*, AöR 1993; *Gröschner/Wiehart-Howaldt* 1995; *Habermas* 2001, 62; Kritisch zu sämtlichen Würdekonzeptionen *Will* 2006, 33.
[1306] *Rohlf* 1980, 87; *Podlech*, Leviathan 1984, 85 ff.
[1307] *Mangoldt/Klein/Starck*, GG-Kommentar, 3. Aufl. 1985, Art. 2, Rn. 11.
[1308] *Rohlf* 1980, 81.
[1309] BVerfGE 80, 367.
[1310] Zum Kernbereich privater Lebensgestaltung, vgl. oben Kap. 5.1.1.
[1311] So *Gurlit*, NJW 2010, 1035, 1036.

unantastbare Kernbereich, der als Ausfluss der Menschenwürdegarantie verstanden wird, erfasst werden muss, um später festzustellen, dass es sich dabei um kernbereichsrelevante und so unantastbare Informationen handelt. Zu Recht wird daher kritisiert, dass so eine Unantastbarkeit nicht gewährleistet werden kann und ein Verstoß gegen die Menschenwürdegarantie vorprogrammiert sei.[1312] Deutlich zeigt sich die daraus resultierende Problematik am Beispiel von Online-Durchsuchungen: Wenn sich hier bei der Auswertung zeigt, dass es sich um kernbereichsrelevante Daten handelt, ist die geforderte Unantastbarkeit bereits verletzt.

Letztlich sei so der Schutz des unantastbaren Kernbereichs im Wesentlichen auf die Forderung nach möglichst schneller Beseitigung der „Antastung" reduziert. Diese Konstruktion ist allerdings in Anbetracht des grundsätzlich auf Eingriffsabwehr zielenden Grundrechtsschutzes befremdlich.[1313]

Dieses Dilemma kann nur vermieden werden, soweit es einen Kontext gibt, aus dem auf die Art des Inhalts der Information geschlossen werden kann, ohne dass sie zur Kenntnis genommen werden muss.[1314]

Andere betonen, dass die Garantie eines unantastbaren Kernbereichs nicht bedeute, dass der Staat jegliches Handeln zu unterlassen habe, das in diesen Kernbereich eindringen könnte.[1315] Dies wäre nur der Fall, wenn der Staat sicher sein könnte, dass „in die als unantastbar ausgewiesene Sphäre des Höchstpersönlichen" eingedrungen wird.[1316] Diese Argumentation fördert jedoch nur zu Tage, was auch Gegenstand der Kritik ist – unantastbar klingt zwar absolut, ist es aber nicht.

Zum Teil wird argumentiert, dass, um der Absolutheitsgarantie zu entsprechen, also um tatsächlich Unantastbarkeit zu gewähren, sämtliche Datenerhebungen unterbleiben müssten, bei denen die Verletzung des Kernbereichs privater Lebensgestaltung mit einer gewissen Zwangsläufigkeit zu befürchten sei.[1317]

Die Kritik, dass der Kernbereichsschutz in der Konzeption des *Bundesverfassungsgerichts* leerlaufe, trifft zu, soweit man den Kernbereich räumlich begreift und die Menschenwürdegarantie des Art. 1 Abs. 1 GG auch als subjektives Recht versteht, dessen absolut zu schützendes Gut der Kernbereich ist.

Wenn man aber die Menschenwürdegarantie als „Achtungsanspruch" versteht und insofern nicht bereits jede Kenntnisnahme kernbereichsrelevanter Informationen als Ver-

---

[1312] *Wolter* 2007, 707, 719; *Kutscha,* LKV 2008, 481.
[1313] *Eifert,* NVwZ 2008, 521, 523.
[1314] *Eifert* NVwZ 2008, 521, 523.
[1315] *Baldus* JZ 2008, 218, 220.
[1316] *Baldus* JZ 2008, 218, 220; Eine solche wäre beispielsweise bei einer zeitlichen und räumlichen „Rundumüberwachung" in der Regel zu bejahen.
[1317] *Kutscha*, LKV 2008, 481; Demnach wäre etwa jede Information aus dem Schlafzimmer unantastbar. Andere begreifen die Figur des Kernbereichs als ideellen Raum, der vor jedem Eindringen zu schützen sei. So etwa die abweichende Meinung der Richterinnen *Jaeger* und *Hohmann-Dennhardt* in der Entscheidung zum Großen Lauschangriff BVerfGE 109, 382, 383f.; siehe dazu *Poscher*, JZ 2009, 269, 272.

letzung des unantastbaren Kernbereichs begreift, sondern eine solche erst annimmt, wenn zu der Kenntnisnahme eine Missachtung tritt, kann mit *Poscher* der Widerspruch aufgelöst werden.[1318] Diese Sichtweise ist zudem konsequent in Anbetracht dessen, dass eine Verletzung von Art. 1 Abs. 1 GG in ständiger Rechtsprechung des *Bundesverfassungsgerichts* nur dann angenommen wird, wenn „der Achtungsanspruch der sich aus ihr ergibt"[1319] verletzt wurde. Das Gericht geht eben nicht von einem starren Raum aus, der nicht betreten werden darf.[1320]

Poscher meint, dass der Kernbereich nicht auch schon dann verletzt, wenn kernbereichsrelevante Informationen lediglich zur Kenntnis genommen werden − es sich um „nicht intendierte" Eingriffe in den Kernbereich handle.[1321] Der verfahrensrechtliche Schutz des Kernbereichs bilde daher „einen konsistenten Baustein im Rahmen einer insgesamt beachtlichen dogmatischen Leistung des Gerichts, die dazu beiträgt, grundrechtliche Freiheit und rechtsstaatliche Kontrolle in einem für die verfassungsrechtliche Dogmatik schwierigen Umfeld zu sichern". [1322]

Der Sache nach ist diese Betrachtungsweise zutreffend. Im Hinblick auf die Praxis, ist sie jedoch nicht weniger dilemmatisch. Denn tatsächlich ist es so, dass Informationen, wenn sie einmal bekannt geworden sind, selbst wenn sie abstrakt als kernbereichsrelevant oder intim bewertet würden, im konkreten Fall, wenn sie unbedingt benötigt werden, dennoch genutzt werden. Insofern ändert auch die Perspektive, dass eine Verletzung des Kernbereichs privater Lebensgestaltung erst dann vorliegt, wenn der Achtungsanspruch verletzt würde, nichts an der Feststellung, dass der absolut klingende Begriff eines unantastbaren Kernbereichs letztlich relativ ist.[1323]

6.1.1.2 Totale Begriffe – total unmöglich

Das im Urteil zur Vorratsdatenspeicherung genannte Verbot einer totalen Erfassung und Registrierung führt ein weiteres Dilemma der vermeintlich absoluten Verbote zu Tage. Mit der Feststellung „die Freiheitswahrnehmung der Bürger" dürfe nicht „total erfasst und registriert" werden,[1324] bezeichnet das Gericht etwas als absolut verboten, das total unmöglich ist.[1325]

Die Problematik besteht darin, dass es eine totale Überwachung nie geben kann. „Totale Überwachung bedeutet Identifizierbarkeit jeder Person jeder Zeit und an jedem Ort."[1326]

[1318] *Poscher*, JZ 2009, 269, 275.
[1319] BVerfGE 87, 209 (228); 96, 375 (399).
[1320] Vgl. Nachw. in Fn. 1317.
[1321] *Poscher*, JZ 2009, 269, 275.
[1322] *Poscher*, JZ 2009, 269, 277.
[1323] *Baldus* JZ 2008. 218, 227 „Die Idee eines unantastbaren Bereiches menschlicher Freiheit wird gewiss niemals in aller Reinheit einlösbar sein. Sie muss in Ausnahmefällen eine wertende Einschränkung um des Schutzes der Freiheit anderer Willen erfahren, ob man dies nun Abwägung nennen mag oder nicht." Er betont, dass ihr dennoch eine hohe freiheitssichernde Funktion zukommt.
[1324] BVerfGE 125, 260 (324)
[1325] Die Ausführungen sind einem bereits veröffentlichten Text, Abschnitt 2 entlehnt: *Knierim*, ZD 2011, 17.
[1326] *Saeltzer*, DUD 2004, 218, 224.

Total meint also eine tatsächlich allumfassende, absolute, vollständige, komplette, lückenlose, unbegrenzte Überwachung. Total heißt auch ganz und gar, in jeder Beziehung und damit restlos und ausschließlich. Total wäre eine Überwachung nur dann, wenn auch wirklich kein überwachungsfreier Raum verbleibt. Und das ist etwas, was nie erreicht werden kann. Eine Überwachung, die keine Lücken lässt, die nicht noch steigerungsfähig ist, ist letztlich nicht vorstellbar. Insofern wird diese Grenze, wenn man den Begriff „total" ernst nimmt, nie erreicht werden. Totale Überwachung als verfassungsrechtliche Grenze ist daher total unmöglich.

Absolute Grenzen können, solange sie an ideellen Begriffen anknüpfen, nie überschritten werden. Dies gilt auch für die Erfassung und Katalogisierung der gesamten Persönlichkeit, also das Verbot vollumfängliche Persönlichkeitsprofile zu erstellen. In der gesamten Persönlichkeit wird ein Profil nie eine Person erfassen können. „Vollständig", „absolut", „total" sind Begriffe, die vermeintlich Schutz versprechen, aber die realiter nie erfüllt werden können. Gerade in Bezug auf die Erfassung und Registrierung muss es um Anteile gehen und nicht um eine hundertprozentige Überwachung.

6.1.2 Dynamische Entwicklung des Grundgesetzes

Nicht nur wegen ihrer faktischen Relativität sind absolute Grenzen schwächer als sie klingen, sondern auch weil sie vom zeitlichen Wandel des Verfassungsrechts und zwar nicht durch Textänderung, sondern auf Grund von Bedeutungsänderungen, erfasst sind. Das Verfassungsrecht, verändert sich nicht nur durch konkrete Änderungen des Verfassungstextes, sondern ebenso durch den allmählichen Bedeutungswandel auf Grund zeitgeschichtlicher Veränderungen.[1327]

Erst durch diesen Verfassungswandel wird, so *Hesse,* Stabilität und Konstanz einer Verfassung ermöglicht. Denn „will die Verfassung ihren Geltungsanspruch auch hinsichtlich der Vielzahl geschichtlich sich wandelnder Problemlagen durchsetzen, so muss „ihr Inhalt notwendig ‚in die Zeit hinein offen' bleiben".[1328]

Das heißt aber auch, dass die Offenheit und Dehnbarkeit, die für die Auslegung der Grundrechte gilt, auch für deren Grenzen gilt. „Auch die Eingriffsmöglichkeiten zur Verwirklichung des Gemeinwohls können nicht ‚zeitlos' bestimmt werden, sondern sind von sich wandelnden Problemlagen abhängig."[1329] Nicht ausgenommen von dem Bedeutungswandel sind auch die in der Rechtsprechung des *Bundesverfassungsgerichts* als absolut anerkannten Schranken-Schranken.

Das heißt auch diese scheinbar harten und starren Grenzen, sind nicht statisch auszulegen. Vielmehr handelt es sich auch bei diesen um entwicklungsoffene Begriffe, die jeweils im Lichte der gesellschaftlichen Rahmenbedingungen interpretiert werden müssen. Insofern das *Bundesverfassungsgericht* dynamische gesellschaftliche Entwicklungen bei der Auslegung der Verfassung berücksichtigt, bezieht es in seine Ein-

[1327] „Von den streng geregelten (…) Verfahren der Textänderung abgesehen, wandelt sich (…) das Verfassungsrecht still und unbemerkt durch eine allmähliche und permanente Bedeutungsänderung", *Roßnagel* 1984, 19.
[1328] *Hesse* 1959, 16.
[1329] *Roßnagel* 1984, 22.

schätzung technische und soziokulturelle Entwicklungen und Veränderungen mit ein. Dies ist auch bei der Auslegung der absoluten Verbote zu berücksichtigen.

6.2 Leerlauf klassischer Eingriffsschranken

Es stellt sich die Frage, gerade in Anbetracht der Feststellung, dass absolute Verbote nie so stark sind wie sie klingen, warum überhaupt so vermeintlich starke Schranken genutzt werden. Warum leitet das *Bundesverfassungsgericht* im Urteil zur Vorratsdatenspeicherung ein Verbot totaler Erfassung und Registrierung aus der Identität der Verfassung ab und beschränkt sich nicht auf die Prüfung der klassischen Eingriffsschranken? Genügen diese denn nicht, um auch in Anbetracht veränderter Verwirklichungsbedingungen von Freiheit und Sicherheit im digitalen Zeitalter diese beiden Werte in einen verfassungskonformen Ausgleich zu bringen?

In Bezug auf die Verarbeitung personenbezogener Daten werden Eingriffe insbesondere durch Zweckbindung (Kap. 6.2.1) und den Grundsatz der Verhältnismäßigkeit (Kap. 6.2.2) beschränkt. Es wurde im ersten Teil der Arbeit[1330] dargelegt, dass die veränderten gesellschaftlichen Rahmenbedingungen die Gewährleistungsfähigkeit von Freiheit und Sicherheit vor neue Herausforderungen stellen. Die Digitalisierung der Kommunikation, die Ausdehnung des Sicherheitsbegriffs und die Einschränkung staatlicher Souveränität innerhalb der Europäischen Union (Kap. 6.2.3) sind insofern auch die Anknüpfungspunkte, um eine Antwort auf die Frage zu suchen, ob Freiheit nicht mehr ausreichend durch klassische Eingriffsschranken geschützt wird (Kap. 6.2.4).

6.2.1 Aushöhlung des Zweckbindungsgrundsatz

Einen Schutz, gerade in Bezug auf staatliche Informationserhebungen, verspricht zunächst der datenschutzrechtliche Zweckbindungsgrundsatz.[1331] Schließlich besagt dieser, dass keine Daten zu unbestimmten Zwecken erhoben werden dürfen.

Nach Ansicht des *Bundesverfassungsgerichts* verletzt eine verdachtsunabhängige Speicherung sämtlicher Telekommunikationsverkehrsdaten auf Vorrat weder den Zweckbindungsgrundsatz noch das Verbot einer Vorratsspeicherung, wenn die Zweckbindung der Daten in der Ermächtigungsgrundlage zur Datenspeicherung abschließend bestimmt wird.[1332] Der Zweckbindungsgrundsatz wird also nach höchstrichterlicher Rechtsprechung als gewahrt beurteilt, wenn personenbezogene Daten nur für den Zweck gespeichert werden, damit für diesen, sollte er sich realisieren, auf sie zugegriffen werden kann − selbst wenn der weit überwiegende Anteil der Daten wieder unmittelbar oder nach einer bestimmten Zeit ungenutzt gelöscht wird.

In dieser Auslegung des Verbots einer zweckfreien Datensammlung auf Vorrat, kommt eine neue Leseart des Verbots einer Vorratsspeicherung, wie es das *Bundesverfassungsgericht* im Volkszählungsurteil festgestellt hat, sowie ein gewandeltes Verständnis des Zweckbindungsgrundsatzes zum Ausdruck: Ein personenbezogenes Datum dient auch dann einem bestimmten Zweck, wenn es lediglich für den eventualen

[1330] S. 9 ff.
[1331] Ausführlich zu diesem oben S. 87.
[1332] Dazu schon oben Kap. 2.1.3.1.

Eintritt eines von vorneherein bestimmten Zwecks vorgehalten wird. Insofern steht der Zweckbindungsgrundsatz einer umfassenden Erfassung und Registrierung nicht entgegen.

Der Zweckbindungsgrundsatz verliert dadurch an Wirkungskraft. Denn zukünftig können Daten gesammelt werden, allein wenn die Möglichkeit besteht, dass diese für einen bestimmten Zweck gebraucht werden, sie also nur zur Vorratshaltung für den Eintritt eines eventuellen Zwecks benötigt werden.

6.2.2 Verhältnismäßigkeit – eine (zu) weiche Grenze

Verfassungsrechtlich steht im Zentrum der Begrenzung von staatlichen Sicherheitsmaßnahmen der Verhältnismäßigkeitsgrundsatz. Ein staatlicher Eingriff in Grundrechte, kann nur dann gerechtfertigt sein, wenn er verhältnismäßig ist.[1333] Das heißt, er muss geeignet, erforderlich und verhältnismäßig i.e.S (angemessen) sein. In jüngerer Zeit kam der Verhältnismäßigkeitsprüfung bei der verfassungsgerichtlichen Prüfung neu eingeführter Sicherheitsinstrumenten herausragende Bedeutung zu. Dabei wohlgemerkt nur der Prüfung der Verhältnismäßigkeit i.e.S.[1334]

Das Gericht hat aus dem Verhältnismäßigkeitsgrundsatz heraus spezifische Anforderungen an die verfahrensmäßige und technische Ausgestaltung verschiedener Maßnahmen entwickelt.[1335] Trotzdem kann die Verhältnismäßigkeitsprüfung das Abdriften in einen Überwachungsstaat nicht verhindern: Denn so wird zwar eine konkrete Ausgestaltung unter Umständen verfassungswidrig sein, eine verfassungskonforme Gestaltung kann aber stets erzielt werden. Diese Annahme belegt der Blick auf die neuere Rechtsprechung des *Bundesverfassungsgerichts.* Dieses hat zwar immer wieder die konkrete Ausgestaltung von sicherheitspolitischen Instrumenten als unverhältnismäßig erachtet, aber diese nie als generell verfassungswidrig beurteilt.[1336] Dies hat seinen Grund darin, dass die Verhältnismäßigkeitsprüfung – wie der Name sagt – keine scharfe Grenze bildet, sondern eine weiche.

Sodann besteht das Dilemma, dass die Verhältnismäßigkeitsprüfung bei staatlichen Informationserhebungen regelmäßig auf den ersten beiden Stufen leer läuft:[1337] So wird das Sammeln von personenbezogenen Informationen immer geeignet sein, den legitimen Zweck, Sicherheit zu gewährleisten, zu fördern. Schließlich sind keine persönlichen Informationen denkbar, die nicht für polizeiliche Ermittlungsarbeit genutzt werden könnten.[1338] Letztlich kann jede Information einen Beitrag zur Wahrheitsfindung leisten. Mehr ist für die Geeignetheit nicht nötig.[1339] Und die Maßnahme wird in aller

---

[1333] Zum Verhältnismäßigkeitsgrundsatz, oben S. 105.

[1334] Ausführlich dazu *Roßnagel* 2011b; deutlich wird dies wenn man wie Hornung den Umfang der Textpassagen in den Urteilen gegenüberstellt, *Hornung* PVS 2012, 377, 393.

[1335] So etwa BVerfGE 125, 260 (321 ff.); vgl. zur Kritik an der Ableitung umfassender organisatorischer und technischer Anforderungen aus dem Verhältnismäßigkeitsgrundsatz, oben S. 158 f.

[1336] Vgl. Nachw. in Fn. 814.

[1337] So auch *Hornung,* PVS 2012, 377, 392.

[1338] Zur Informationsvorsorge als wesentlicher Bestandteil moderner Polizeiarbeit, vgl. oben Kap. 1.4.2.2, S. 63.

[1339] Ausführlich dazu auch *Hornung,* PVS 2012, 377, 391.

Regel auch erforderlich sein. Denn je umfassender eine Datenerhebung erfolgt, desto geringer ist die Wahrscheinlichkeit, eine gleich geeignete Maßnahme zu finden. Insofern sind Maßnahmen mit großer Streubreite in aller Regel erforderlich.[1340]

Dieses Phänomen beschreibt *Hornung* treffend „Je mehr Informationen man zu unbestimmten Zwecken sammelt, desto weniger lässt sich argumentieren, die Maßnahme sei zu diesem Zweck nicht geeignet, weil sich in der Masse der Informationen immer zumindest potentiell nützliche Angaben befinden werden. Zugleich wird es zwar sehr einfach, mildere Mittel zur Sammlung immer größerer Datenmengen eines Lebensbereiches zu finden, aber es lässt sich nicht mehr argumentieren, diese Mittel – die ja notwendigerweise weniger Informationen für die Sicherheitsbehörden bereitstellen – seien gegenüber der weitreichenderen Speicherung (im Extremfall: aller) Daten eines Lebensbereiches gleich geeignet.[1341]

Daher verlagert sich die verfassungsrechtliche Prüfung auf die Prüfung der dritten Stufe, der Verhältnismäßigkeit i.e.S. – der Angemessenheit. Die Prüfung der Angemessenheit vermag aber ebenfalls kein Abdriften hin zu einem immer mehr an Sicherheit und weniger an Freiheit zu verhindern, da sie eben im Kern eine Abwägung ist und diese bei der Kollision zweier verfassungsrechtlich schützenswerter Rechtspositionen, nie absolut in eine Richtung ausschlagen wird. Mit anderen Worten: Bei einem Eingriff in die Freiheitsgrundrechte der Bürger wird nie ein Sicherheitsinstrument generell unverhältnismäßig sein, sondern immer nur die bestehende Gestaltung (jedenfalls soweit nicht absolut geschützte Güter verletzt werden).[1342]

In diesem Sinne hat *Petri* schon im Jahr 2003 diagnostiziert, dass sich das „Verhältnismäßigkeitsprinzip in der Realität als untaugliches Instrument zur Begrenzung von Grundrechtseingriffen erwiesen“ habe. „Wenn in Ermangelung konkreter Maßstäbe nur gemessen wird, ob eine Maßnahme „außer Verhältnis“ zu einem Eingriff in Freiheitsreche steht, führt dies faktisch zu einer Umkehrung der Argumentationslast auf Kosten der Freiheit.“[1343]

Die Verhältnismäßigkeitsprüfung kann darüber hinaus eine umfassende Überwachung der gesamten Gesellschaft nicht verhindern, da hier immer nur geprüft wird, ob *ein* bestimmter Eingriff oder *eine* gesetzliche Regelung verhältnismäßig ist, nicht aber ob auf Grund der Kumulation verschiedener Eingriffe und Sicherheitsgesetze *insgesamt* eine umfassende Überwachung und damit die Umkehr des Verhältnisses von Freiheit und Sicherheit, wie es im Grundgesetz vorgesehen ist, erreicht wird.

Eine begrenzte Ausnahme stellt in dieser Hinsicht die Entscheidung zum verdeckten Einsatz eines GPS-Peilsenders dar. Hier stellt das *Bundesverfassungsgericht* fest, dass „beim Einsatz moderner, insbesondere dem Betroffenen verborgener, Ermittlungsmethoden“ die Strafverfolgungsbehörden mit Rücksicht auf „das dem ‚additiven‘ Grundrechtseingriff

[1340] So etwa bei der Beurteilung des Großen Lauschangriffs, BVerfGE 109, 279 (336 f.) 115, 320 (345); 120, 274 (320); 120, 378 (428); 125, 260 (317); ausführlich dazu auch *Hornung,* PVS 2012, 377, 392.
[1341] *Hornung* PVS 2012, 377, 392.
[1342] Vgl. zu diesem Gedanken bereits *Roßnagel* 1984, 64 ff.
[1343] *Petri*, RDV 2003, 16, 20.

innewohnende Gefährdungspotential besondere Anforderungen an das Verfahren beachten" müssten.[1344] Das Gericht betrachtet hier also auch die Maßnahme in ihrem Zusammenwirken mit anderen im Einsatz befindlichen Überwachungsinstrumenten. Allerdings wird nicht der gesamtgesellschaftliche Grad an Überwachung betrachtet, sondern das Zusammentreffen verschiedener Ermittlungsmaßnahmen im Einzelfall. Es geht insofern um die Totalüberwachung eines einzelnen Bürgers.

Das Gericht verlangt hier, dass die „Staatsanwaltschaft als primär verantwortlicher Entscheidungsträger über alle Ermittlungseingriffe informiert" sein müsse, da ansonsten die „Feststellung übermäßiger Belastung" nicht möglich wäre. Der Gesetzgeber habe aber davon ausgehen dürfen, dass die von „Verfassungs wegen stets unzulässige ‚Rundumüberwachung' mit der ein umfassendes Persönlichkeitsprofil eines Beteiligten erstellt werden könnte, durch allgemeine verfahrensrechtliche Sicherungen auch ohne spezifische gesetzliche Regelung grundsätzlich ausgeschlossen"[1345] sei. Letztlich handelt es sich auch insoweit um eine stark begrenzte Ausnahme.

Deutlich macht jedoch die Entscheidung aus dem Jahr 2005, dass das Gericht schon damals erkannt hatte, dass der Fokus auf Einzelmaßnahmen in Anbetracht des informationstechnischen Wandels für den Grundrechtsschutz generell riskant ist.[1346]

Letztlich kann festgestellt werden, dass die Verhältnismäßigkeitsprüfung zur Eindämmung staatlicher Informationsvorsorge durch Datenerfassungsmaßnahmen zu Sicherheitszwecken nur eingeschränkt wirkungsfähig ist. Ihre Schwäche liegt zum einen darin begründet, dass „Geeignetheit" und „Erforderlichkeit", in ihrer Ausformung durch das *Bundesverfassungsgericht* als Eingriffsschranken zum Schutz der Freiheit faktisch leer laufen. Zudem wohnt der Verhältnismäßigkeit i.e.S. die Schwierigkeit inne, dass diese Abwägungsformel in Anbetracht massiver Bedrohungsszenarien, nie absolut in eine Richtung ausschlagen wird. Und schließlich scheitert sie, da im ihrem Rahmen

---

[1344] Es führt weiter aus, dass „wegen des schnellen und für den Grundrechtsschutz riskanten informationstechnischen Wandels (…) der Gesetzgeber die technischen Entwicklungen aufmerksam beobachten und notfalls durch ergänzende Rechtssetzung korrigierend eingreifen" müsse, BVerfGE 112, 304 (LS 2, 3; S. 319f.). Hintergrund der Entscheidung war ein strafrechtliches Ermittlungsverfahren. Der Tatverdächtige wendete sich gegen den Einsatz eines GPS-Systems zur Ermittlung seines Aufenthaltsortes. Er beanstandete, dass es für den Einsatz dieser Maßnahme auf Grund des Zusammenwirkens mit zahlreichen anderen Überwachungsinstrumenten, die eingesetzt wurden, einer eigenen Ermächtigungsgrundlage bedurft hätte. Der Fall wurde auch dem *EGMR* vorgelegt. Dieser stellte in der daraufhin ergehenden Entscheidung *Uzun./.*Deutschland 2010 fest, dass ein „ausreichender Schutz vor Missbrauch insbesondere" voraussetze, „dass unkoordinierte Ermittlungsmaßnahmen verschiedener Behörden verhindert werden müssen und die Staatsanwaltschaft vor der Anordnung der GPS-Überwachung eines Beschuldigten daher sicherstellen muss, dass sie über bereits getroffene weitere Observationsmaßnahmen unterrichtet ist. Mit Blick auf die Ausführungen des Bundesverfassungsgerichts in dieser Frage stellt er jedoch fest, dass die zur Verhütung der Totalüberwachung einer Person im maßgeblichen Zeitraum bestehenden Schutzvorkehrungen, einschließlich des Verhältnismäßigkeitsgrundsatzes, ausreichten, um einem Missbrauch vorzubeugen", *EGMR* Urt. v. 2.9.2010 – Beschw. Nr. 35623/05, EuGRZ 2011, 115. Auch der *EGMR* erkennt also an, dass eine Totalüberwachung des Einzelnen nicht mit Art. 8 EMRK vereinbar wäre.

[1345] BVerfGE 112, 304 (319) unter Bezugnahme auf BVerfGE 65, 1 (43); 109, 279 (323).

[1346] BVerfGE 112, 304 (320).

immer nur ein konkreten Einzelfall geprüft und nicht die kumulative Wirkung eines Instruments in Verbindung mit bereits vorhandenen staatlichen und privaten Datensammlungen und Überwachungsmaßnahmen betrachtet wird.

6.2.3 Hilflosigkeit deutschen Rechts gegenüber Europäischer Rechtsakten

Nicht nur im Hinblick auf verfassungsrechtliche Schranken-Schranken, die leer laufen, stellt sich die Frage, ob die verfassungsrechtlich garantierte Freiheit unter den heute aktuellen Bedingungen noch angemessen geschützt ist. Diese Frage stellt sich auch in Anbetracht der immer stärkeren Determination und Überlagerung nationalen Rechts durch europäisches Recht.

Denn Europäisches Sekundärrecht wird nicht an den Maßstäben des Grundgesetzes geprüft. Nach der Solange II-Rechtsprechung prüft das *Bundesverfassungsgericht* dies solange nicht, solange auf europäischer Ebene ein adäquater Grundrechtsschutz gewährleistet wird.[1347] Nur in wenigen Ausnahmefällen hat sich das Bundesverfassungsgericht die Verwerfungskompetenz vorbehalten und zwar dann, wenn es die Identität der Verfassung verletzt würde[1348] oder bei einem Ultra-Vires-Handeln von Unionsorganen.[1349] Das heißt, dass zahlreiche Gesetze, die Überwachungsmöglichkeiten bieten, gar nicht erst unter den soeben aufgeführten Gesichtspunkten verfassungsrechtlicher Schranken-Schranken überprüft werden. Im Urteil zur Vorratsdatenspeicherung hat das Bundesverfassungsgericht nun zwar die Vereinbarkeit der Europäischen Richtlinie mit den Grundrechten überprüft – allerdings hat es damit keineswegs eine eigene Verwerfungskompetenz hinsichtlich sekundärem Unionsrechts angenommen.[1350]

6.2.4 Kein Schutz vor totaler Überwachung durch klassische Schranken-Schranken

Es konnte gezeigt werden, dass klassische Schranken-Schranken es nicht vermögen das Abdriften in einen Überwachungsstaat effektiv zu begrenzen: neue technische Möglichkeiten, eine gewandelte Ausrichtung von individueller Observation hin zu gesamtgesellschaftlicher-Erfassung sowie die Überlagerung nationalen Rechts durch internationale Regime führen dazu, dass die Grundsätze der Zweckbindung und der Verhältnismäßigkeit Freiheit nicht mehr gegen ein wachsendes Sicherheitsstreben schützen können. Gegen einen schleichenden Prozess, in dem Freiheitsräume immer weiter beschnitten werden, besteht insofern kein ausreichender Schutz allein durch die klassischen Schranken-Schranken.

6.3 Notwendigkeit der Konkretisierung

Im Angesicht dieser Entwicklungen wird zu Recht gefragt, ob das Grundgesetz noch geeignet ist Freiheit in Sicherheit unter den Bedingungen moderner Datenverarbeitung zu gewähren. Kann diese Aufgabe das Verbot totaler Erfassung und Registrierung erfüllen, welches das *Bundesverfassungsgericht* im Urteil zur Vorratsdatenspeicherung formuliert hat?

[1347] Dazu schon oben S. 177 f.
[1348] BVerfGE 123, 267 (340).
[1349] BVerfG 2 BvR 2661/06 - Beschluss v. 6.7.2010, Rn. 62 (*Mangold).*
[1350] Vgl. dazu oben S. 1085.

Es wurde bereits aufgezeigt, dass absolute Grenzen, vielfach drohen leer zu laufen. Doch da klassische Schranken-Schranken im Angesicht der Digitalisierung und einer zunehmenden Sicherheitsvorsorge leerlaufen, bedarf es neuer Konzepte, um das Abdriften in einen Überwachungsstaat und eine Sicherheitsgesellschaft zu verhindern. Diese Funktion könnte dem absoluten Verbot einer totalen Erfassung und Registrierung zukommen.

Das bestehende und in Kap. 6 dargestellte Dilemma absoluter Grenzen hat jedoch gezeigt, dass auch absolute Grenzen letztlich relativ sind. Sie sind immer auch Verhältnismäßigkeitsprüfung, allerdings in anderem Gewandt. Es lässt sich in Anbetracht der aufgezeigten Relativität absoluter Grenzen durchaus fragen, ob sich die Funktion dieser Postulate darauf beschränkt, die jeweils unterlegene Seite zu beschwichtigen: Die Gegner von Wohnraumüberwachung, von Online-Durchsuchung und Vorratsdatenspeicherung sollen befriedet werden, obwohl sie in der Sache verloren haben – da jeweils die Maßnahme als grundsätzlich zulässig bewertet wurde (obwohl die konkrete Umsetzung als verfassungswidrig beurteilt wurde).[1351] Es soll ihnen vermittelt werden, dass sie in einem Staat leben, in dem absolute Kontrolle absolut verboten ist.

Allerdings muss sich die Funktion absoluter Verbote nicht darin erschöpfen beschwichtigend zu wirken. Dafür erforderlich ist aber, dass sie konkretisiert werden. Das Konzept eines unantastbaren Kernbereichs hat nur auf Grund der Konkretisierung als zweistufiges Verfahren effektive Wirkungskraft entfaltet.

Wenn absolute Grenzen wirkungsvoll Freiheit schützen sollen und nicht wie das Verbot der Profilbildung leerlaufen, ist es Aufgabe des Juristen diese Grenzen zu konkretisieren und Konzepte zu entwickeln, wie die vermeintlich absoluten Schranken tatsächlich Wirkungskraft entfalten können. In Anbetracht eines sich kontinuierlich ausdehnenden Sicherheitsstrebens und dem nicht zu stillenden Informationshunger der Sicherheitsbehörden, ist es eine der zentralen Aufgaben des Verfassungsjuristen, das zur Wahrung des Gleichgewichts von Freiheit und Sicherheit zentrale Verbot einer totalen Erfassung und Registrierung der Bürger weiterzuentwickeln.

[1351] Vgl. dazu die Nachw. in Fn. 814.

7 Das Verbot umfassender gesamtgesellschaftlicher Überwachung

„Die Speicherung der Telekommunikationsverkehrsdaten" darf „nicht als Schritt hin zu einer Gesetzgebung verstanden werden, die auf eine möglichst flächendeckende vorsorgliche Speicherung aller für die Strafverfolgung oder Gefahrenprävention nützlichen Daten zielte. Eine solche Gesetzgebung wäre, unabhängig von der Gestaltung der Verwendungsregelungen, von vornherein mit der Verfassung unvereinbar. Die verfassungsrechtliche Unbedenklichkeit einer vorsorglich anlasslosen Speicherung der Telekommunikationsverkehrsdaten setzt vielmehr voraus, dass diese eine Ausnahme bleibt. Sie darf auch nicht im Zusammenspiel mit anderen vorhandenen Dateien zur Rekonstruierbarkeit praktisch aller Aktivitäten der Bürger führen. Maßgeblich für die Rechtfertigungsfähigkeit einer solchen Speicherung ist deshalb insbesondere, dass sie nicht direkt durch staatliche Stellen erfolgt, dass sie nicht auch die Kommunikationsinhalte erfasst und dass auch die Speicherung der von ihren Kunden aufgerufenen Internetseiten durch kommerzielle Dienstanbieter grundsätzlich untersagt ist. Die Einführung der Telekommunikationsverkehrsdatenspeicherung kann damit nicht als Vorbild für die Schaffung weiterer vorsorglich anlassloser Datensammlungen dienen, sondern zwingt den Gesetzgeber bei der Erwägung neuer Speicherungspflichten oder -berechtigungen in Blick auf die Gesamtheit der verschiedenen schon vorhandenen Datensammlungen zu größerer Zurückhaltung. Dass die Freiheitswahrnehmung der Bürger nicht total erfasst und registriert werden darf, gehört zur verfassungsrechtlichen Identität der Bundesrepublik Deutschland".[1352] Fraglich ist jedoch, ob dieses Verbot es vermag, ein Abdriften in eine Überwachungsgesellschaft tatsächlich effektiv zu begrenzen.[1353]

Mit dem Ziel einer Konkretisierung des Verbots totaler Erfassung und Registrierung fordert *Roßnagel* zutreffend die Durchführung einer „Überwachungs-Gesamtrechnung".[1354] Doch was bedeutet dies konkret für die Einführung neuer Überwachungsinstrumente? Und vor allem: Wann wäre denn die Grenze totaler Erfassung und Registrierung überschritten? Mittels einer verfassungsrechtlichen Analyse des Urteils sollen im Folgenden, Grundlagen, Inhalt und Folgen des Verbots totaler Erfassung und Registrierung ermittelt werden. [1355]

7.1 Verfassungsrechtliche Grundlage

Das Verbot totaler Erfassung und Registrierung der Freiheitswahrnehmung aller Bürger sieht das *Bundesverfassungsgericht* als Teil der Identität der Verfassung.[1356] Darüber hinaus begründet das Gericht diese Feststellung jedoch nicht weiter.[1357] Insofern ist zunächst zu untersuchen, welche verfassungsrechtliche Grundlage das Verbot totaler Erfassung und Registrierung hat.

[1352] BVerfGE 125, 260 (324).

[1353] Damit setzen sich auch auseinander: *Roßnagel,* NJW 2010, 1238, *Ders.,* DUD 2010, 544; dazu auch *Knierim,* ZD 2011, 17; kritisch äußern sich *Hornung/ Schnabel,* DVBl. 2010, 824.

[1354] *Roßnagel*, NJW 2010, 1238, 1240, *Roßnagel*, DUD 2010, 544 dazu auch *Hornung/Schnabel*, DVBl. 2010, 824; *Knierim*, ZD 2011, 17.

[1355] Die Ausführungen des folgenden Kapitels sind zum Teil bereits in *Knierim*, ZD 2011, 17, veröffentlicht.

[1356] BVerfGE 125, 260 (324).

[1357] So auch *Pagenkopf*, in *Sachs,* GG 2011, Art. 10, Rn. 8, der kritisiert, dass darin eine Verfassungsdramatik ausgedrückt würde, die mit der technischen Lebenswirklichkeit nicht übereinstimme.

A. Moser-Knierim, *Vorratsdatenspeicherung,* DuD-Fachbeiträge,
DOI 10.1007/978-3-658-04156-4_7, © Springer Fachmedien Wiesbaden 2014

Im Lissabon-Urteil vom 30. Juni 2009 hat das *Bundesverfassungsgericht* festgestellt, dass die europäische Integration auf Basis des Grundgesetzes nur soweit voranschreiten kann, als die Identität der Verfassung gewahrt bleibt. Die Ewigkeitsklausel des Art. 79 Abs. 3 GG gebe einen integrationsfesten und unantastbaren Kerngehalt der Verfassung vor.[1358] Auf diesen Urteilssatz rekurriert nun der *Erste Senat* im Urteil zur Vorratsdatenspeicherung, als er das Verbot, die Freiheitswahrnehmung der Bürger total zu erfassen und zu rekonstruieren, formuliert. Daraus folgt, dass die durch die Ewigkeitsgarantie geschützten Art. 1 und Art. 20 GG die verfassungsrechtliche Grundlage des Verbots bilden.

Art. 1 Abs. 1 GG dient primär dem Schutz der Würde des einzelnen Rechtssubjekts.[1359] Die Würde des Einzelnen soll unantastbar und damit jeder Abwägung unzugänglich sein.[1360] Allgemein anerkannt ist, dass ein enger Bezug zwischen Menschenwürdegarantie und Freiheit besteht.[1361] Verlangt wird die Anerkennung und Achtung des Individuums in seiner Eigenständigkeit und in seinem Eigenwert sowie dessen Selbstbestimmung und -verantwortung, wie auch seiner Selbstentfaltung.[1362] Die Menschenwürdegarantie verpflichtet insofern dazu, „geistige Freiheit" zu gewähren.[1363]

Entsprechend ist ein spezifischer Bezug zwischen Menschenwürdegarantie und Demokratieprinzip anerkannt. So wird der Anspruch des Einzelnen auf „freie und gleiche Teilhabe" an der öffentlichen Gewalt als in der Würde verankert angesehen.[1364]

Auch ist anerkannt, dass der Menschenwürdegarantie ein objektiv-rechtlicher Gehalt entnommen werden kann. Die Objektformel[1365] lässt sich in ihrer gesamtgesellschaftlichen Dimension formulieren: Mit der Menschenwürde ist eine Gesellschaftsordnung nicht vereinbar, in welcher die Bürger zum bloßen (Daten-)Objekt staatlichen Handelns herabgewürdigt werden. Die Menschenwürdegarantie verlangt,

---

[1358] „Der unübertragbaren und insoweit integrationsfesten Identität der Verfassung (Art. 79 Abs. 3 GG)" BVerfGE 123, 267 (350). Was im Einzelnen der Identität der Verfassung zugeordnet werden kann, ist noch offen. Ausführlich zur Identität der Verfassung, *Kirchof,* in: *Isensee/Kirchof* HStR II, § 21; kritisch zum Identitätsvorbehalt unter europarechtlichen Gesichtspunkten *v. Bogdandy/Schill,* ZaöRV 2010, 701 ff.

[1359] Zur Menschenwürdegarantie, vgl. auch oben Kap. 2.1.1, S. 74 ff.

[1360] Der Menschenwürdegarantie kommt vorwiegend eine abwehrrechtliche Bedeutung zu. Negatorisch wird die Menschenwürdegarantie an Hand der Objektformel konkretisiert: „Die Menschenwürde ist getroffen, wenn der konkrete Mensch zum Objekt, zu einem bloßen Mittel, zur vertretbaren Größe herabgewürdigt wird", Dürig, AöR 1956, 117, 117, 127ff.; zahlreiche Nachweise aus der Rspr vgl. oben Fn. 432; Umstritten ist auch wie der Gehalt der Menschenwürde positiv bestimmt werden kann, vgl. dazu oben, S. 74 ff.

[1361] Vgl. dazu oben S. 74 f.

[1362] *Merten, in:* HGR I, 2006, § 27 Rn. 11; vgl. dazu oben S. 74 ff.

[1363] *Hofmann*, in :*Schmidt-Bleibtreu/Klein*, GG 2011, Art. 1, Rn. 5; vgl. oben S. 77.

[1364] Vgl. BVerfGE 123, 267 (341); Zur Konnexität von Freiheit des Individuums und Demokratie, schon oben S. 103. Das BVerfG betont, dass „ohne freie und gleiche Wahl desjenigen Organs, das einen bestimmenden Einfluss auf die Regierung und Gesetzgebung des Bundes hat, das konstitutive Prinzip personaler Freiheit unvollständig" bliebe, BVerfGE 123, 267, 340; vgl. dazu auch *Hillgruber* in: BeckOK GG, Art. 1 Rn. 14a; „In der freiheitlichen Demokratie ist die Würde des Menschen der oberste Wert." BVerfGE 5, 85 (204).

[1365] Vgl. Nachw. in Fn. 1360.

dass der Einzelne bei einer staatlichen Datenerhebung, -sammlung und -verwertung, als Individuum wahrgenommen wird. Ihm muss stets die Möglichkeit der freien Entfaltung erhalten bleiben. Das heißt, dass kein abschließendes Bild jedes Einzelnen erstellt werden darf, denn ein solches würde den Einzelnen zum bloßen Datenobjekt degradieren.

Zum anderen – und hier kommt die gesellschaftliche Dimension, also die objektivrechtliche Wirkung der Menschenwürdegarantie zu Tragen – muss ein Umfeld gewährleistet werden, in dem Freiheit des Geistes bestehen kann. Voraussetzung dafür ist nicht nur Meinungs- und Informationsfreiheit, sondern ganz wesentlich dafür ist neben der Handlungsfreiheit auch die (Tele-)Kommunikationsfreiheit.[1366]

Alle Grundrechte weisen einen Menschenwürdekern auf – sie unterscheiden sich jedoch nach Nähe zu diesem. Wesentlich ist jedenfalls, dass die für die Würde des Menschen wichtigen Grundrechtsgarantien nicht vollständig aufgezehrt werden. Dies droht aber, wenn jegliche Freiheitswahrnehmung sämtlicher Bürger erfasst würde. Insofern verbietet die Menschenwürdegarantie eine totale Erfassung und Registrierung der Freiheitswahrnehmung jedes Einzelnen.

Neben der objektiv-rechtlichen Wirkung der Menschenwürdegarantie, wurzelt das Verbot in den in Art. 20 GG normierten Grundsätzen. Dieser garantiert Demokratie, (horizontale und vertikale) Gewaltenteilung sowie die Bindung aller Gewalten an das Grundgesetz.[1367] Das Grundgesetz wurde konstituiert mit dem Ziel, die grundsätzliche Freiheit des Einzelnen vor Willkür zu garantieren.[1368] Daraus ergibt sich in Zusammenschau mit Art. 1 GG die grundsätzliche Garantie einer freiheitlichen, demokratischen und rechtsstaatlichen Ordnung, die der Menschenwürde zu dienen verpflichtet ist.

Wesentlich für die Achtung der Menschenwürdegarantie, ist sowohl, dass Verletzungen durch eine Objektivierung vermieden werden, als auch eine freie Entfaltung, insbesondere die Freiheit des Geistes, gesichert ist. Insofern stehen Art. 20 in Verbindung mit Art. 1 GG nicht nur jeglicher Willkürherrschaft entgegen, sondern statuieren auch eine freiheitliche Grundordnung, die als solche Bestandteil der Identität der Verfassung ist.[1369]

Einer solchen freiheitlichen, der Würde des Einzelnen verpflichteten Grundordnung widerspräche eine Gesellschaftsordnung, in der die Freiheitswahrnehmung aller Bürger registriert wird. Dies gilt selbst dann, wenn sie nicht unmittelbar ausgewertet und in diesem Sinne direkt überwacht würden. Denn der Einzelne wäre dann zwar noch frei, doch seine Freiheitswahrnehmung wäre für den Staat jederzeit nachvollziehbar und rekonstruierbar. Die Möglichkeit, unbeobachtet seine garantierten Freiheiten leben

[1366] Ausführlich zur Bedeutung der Telekommunikationsfreiheit im digitalen Zeitalter, vgl. oben S. 95 ff.; 101 f.
[1367] Ausführlich zur Gewaltenteilung oben S. 107; zum Rechtsstaatsprinzip, oben Kap. 104.
[1368] Vgl. dazu oben S. 74 ff.
[1369] *Benda* 1974, S. 23.

zu können, ist aber vielfach Voraussetzung für die Freiheitswahrnehmung.[1370] Soweit das Verhalten umfassend registriert wird, wird Freiheitswahrnehmung der Bürger für den Staat zu Nullen und Einsen und steht so als Datenfundus zur Verfügung, der kategorisiert und analysiert werden kann. Selbst wenn keine unmittelbare Auswertung der Daten erfolgt, ist davon auszugehen, dass von einer solchen umfassenden Datensammlung ein hoher Überwachungsdruck ausgeht.[1371] Schon durch die Möglichkeit permanenter Überwachung wird die Wirkung einer kontinuierlichen Überwachung erzielt. Das Gefühl des Beobachtetseins kann beim Einzelnen dazu führen, dass er sein Verhalten anpasst.[1372]

Insofern verbieten es die Menschenwürdegarantie und die Konstitution einer freiheitlich demokratischen Grundordnung durch Art. 20 GG, wie es auch das *Bundesverfassungsgericht* im Urteil zur Vorratsdatenspeicherung vom 2.3.2010 formuliert hat, die Freiheitswahrnehmung sämtlicher Bürger total zu erfassen und zu registrieren.

7.2 Verbot einer umfassenden gesamtgesellschaftlichen Überwachung

Das Verbot die Freiheitswahrnehmung der Bürger total zu erfassen und zu registrieren ist, wie dargelegt wurde, verfassungsrechtlich fundiert. Aber worauf zielt dieses Verbot genau? Schützt es wirklich nur vor einer totalen, also vollumfänglichen, ausnahmslosen Überwachung, wie die Bezeichnung totale Erfassung und Registrierung vermuten lässt?

Letztlich ergibt eine solche Auslegung, die ausschließlich am Wortlaut anknüpft, keinen Sinn. Denn eine tatsächlich alles erfassende, totale, vollumfängliche Erfassung und Registrierung jeglicher Freiheitswahrnehmung jedes Bürgers ist weder technisch noch tatsächlich möglich.[1373] Geboten ist daher unter teleologischen Gesichtspunkten eine einschränkende Auslegung des Begriffs totaler Erfassung. Für eine einschränkende Auslegung spricht auch, dass das Gericht betont, dass die Vorratsdatenspeicherung nicht dazu führen dürfe, dass diese „im Zusammenspiel mit anderen vorhandenen Dateien zur Rekonstruierbarkeit praktisch aller Aktivitäten der Bürger“ führe. Indem das Gericht hier relativiert und keine Rekonstruktion aller, sondern lediglich „praktisch aller Aktivitäten“ verlangt, macht es deutlich, dass das Verbot einer totalen, vollumfänglichen Überwachung nicht so absolut ist, wie die Wortwahl auf den ersten Blick erscheint.

Der Begriff einer totalen Erfassung und Registrierung muss so relativiert werden, dass die Formel das Schutzziel adäquat umsetzt. Das Schutzziel des Verbots totaler Erfassung und Registrierung ist es zu verhindern, dass die freiheitliche Grundordnung durch

---

[1370] *Tinnefeld* führt aus dass Voraussetzung der Gedankenfreiheit sei, dass „sich der Einzelne in seinem näheren (privaten) Lebensbereich unbeobachtet und in diesem Sinn sicher fühlen kann.“ MMR 2007, 137; dazu auch *Foucault*, vgl. oben Fn. 202.

[1371] Dazu ausführlich oben S. 86.

[1372] Dass *BVerfG* geht davon aus, dass von einem „Gefühl des unkontrollierbaren Beobachtetwerdens“ nachhaltige Einschüchterungseffekte auf die Freiheitswahrnehmung ausgingen, BVerfGE 125, 260 (332).

[1373] Vgl. dazu schon oben Kap. 6.1.1.2, S. 218.

eine umfassende Überwachung konterkariert wird.[1374] Es soll verhindert werden, dass die Freiheit auf Grund umfassender Überwachungsmaßnahmen eingeschränkt wird.

Nahe liegt es, im Ergebnis statt von einer „totalen" Erfassung und Registrierung der Freiheitswahrnehmung sämtlicher Bürger von einer „umfassenden gesamtgesellschaftlichen Überwachung" zu sprechen. So betont das *Bundesverfassungsgericht* etwa im Urteil zur Vorratsdatenspeicherung, dass sich nicht feststellen ließe, dass die „Regelung im Zusammenwirken mit anderen Vorschriften darauf zielt oder hinausläuft, eine allgemein umfassende Datensammlung zur *weitest möglichen* Rekonstruierbarkeit jedweder Aktivitäten der Bürger zu schaffen".[1375]

Die Formel „Verbot einer umfassenden gesamtgesellschaftlichen Überwachung" scheint treffend, da sie den Begriff „total" relativiert ohne ihn ins uferlose auszudehnen. Es wird deutlich, dass die Grenze nicht erst überschritten ist, wenn tatsächlich allumfassend jeder und alles erfasst ist. Verlangt wird eine umfassende, also weitgehende Erfassung und Registrierung. Passend ist diese Auslegung darüber hinaus, weil die Formulierung deutlich macht, dass nicht primär die Rundumüberwachung eines Einzelnen verhindert werden soll, sondern nicht umfassend die Aktivitäten vieler Bürger erfasst werden dürfen. Denn Schutzgut ist die freiheitliche Grundordnung, und damit nur mittelbar die freie Entfaltung des Einzelnen.[1376]

Das Gericht konkretisiert den Schutzgehalt des Verbots einer umfassenden gesamtgesellschaftlichen Überwachung näher. In der Aussage, dass die „Unbedenklichkeit einer vorsorglich anlasslosen" Datenerhebung voraussetze, „dass diese eine Ausnahme bleibt" und sie nicht als Vorbild für weitere „vorsorglich anlasslose(r) Datensammlungen" dienen könne,[1377] wird deutlich, dass anlasslose Vorratsspeicherungen nur als Ausnahme zulässig sind. Das Verbot beschränkt sich jedoch nicht nur darauf, sondern verbietet generell die Freiheitswahrnehmung der Bürger umfassend zu überwachen.

Im Folgenden werden diese beiden Aspekte des Verbots umfassender gesamtgesellschaftlicher Erfassung und Registrierung im Einzelnen näher untersucht (Kap. 7.2.1 u. 7.2.2).

7.2.1 Vorratsspeicherung − nur ausnahmsweise und nur in engen Grenzen

In einer ersten Interpretation könnte man annehmen, dass generell verdachtsunabhängige Datenerhebungen nur als einzelne Ausnahme zulässig sind. Führt das *Bundesverfassungsgericht* doch aus, dass die Unbedenklichkeit einer Vorratsspeicherung voraussetzt, dass diese „eine Ausnahme bleibt" und sie nicht Vorbild für andere vorsorglich anlasslose Datensammlung sein könne.[1378] Damit kann aber nicht ein grundsätzliches Verbot jeglicher vorsorglicher Datenerhebung gemeint sein. Schließlich werden immer

[1374] Vgl. dazu schon oben S. 227 ff.
[1375] BVerfGE 125, 260 (348); *Hervorhebung durch die Autorin*.
[1376] Dass dem so ist, wird auch belegt dadurch, dass das Gericht das Verbot als Bestandteil der Identität der Verfassung begreift und es somit nicht allein aus der Menschenwürdegarantie ableitet sondern auch aus der Garantie eines freiheitlich demokratischen Rechtsstaats; vgl. zum Rechtsstaatsprinzip, S. 104f.; zur freiheitlich demokratischen Grundordnung oben, S. 108 ff.
[1377] BVerfGE 125, 260 (324) ; *Hervorhebungen durch die Autorin*.
[1378] BVerfGE 125, 260 (324).

wieder Daten vorsorglich erhoben, insbesondere durch die Nachrichtendienste, aber auch durch die Polizei. Auch das *Bundesverfassungsgericht* hat vorsorgliche Datenerhebungen schon in der Vergangenheit als legitim beurteilt − allerdings nur dann und soweit es sich um Maßnahmen handelt, die, auch wenn sie vorsorglich sind, in ihrem Umfang beschränkt bleiben:

So hat das Gericht etwa in Bezug auf die strategische Telekommunikationsüberwachung durch die Nachrichtendienste wiederholt festgestellt, dass der mit ihr verbundene Eingriff in das Fernmeldegeheimnis verhältnismäßig und auch verfassungsgemäß sei.[1379] Zwar wiegen die Grundrechtseingriffe namentlich mit Blick auf ihre Verdachtslosigkeit schwer. Andererseits ist zu berücksichtigen, dass die Grundrechtsbeschränkungen dem Schutz hochrangiger Gemeinschaftsgüter dienen. Soweit der Gesetzgeber auf Eingriffsvoraussetzungen und Begrenzungen nicht verzichte, sondern bestimmte Kriterien und verfahrensrechtliche Sicherungen normiere, sei die Ermächtigung verhältnismäßig.[1380]

In Bezug auf die vorbeugende Telekommunikationsüberwachung hat das *Bundesverfassungsgericht* im Urteil aus dem Jahr 2005 zunächst in Bezug auf Bestimmtheitsanforderungen generell klargestellt, dass zwar nicht verlangt wird, „dass die konkrete Maßnahme vorhersehbar ist, wohl aber, dass die betroffene Person grundsätzlich erkennen kann, bei welchen Anlässen und unter welchen Voraussetzungen ein Verhalten mit dem Risiko der Überwachung verbunden ist".[1381] Es führt sodann aus, dass soweit eine Maßnahme auf die „Vorsorge für die Verfolgung künftiger Straftaten oder bei ihrer Verhütung" zielt, kann nicht „an dieselben Kriterien angeknüpft werden, die für die Gefahrenabwehr oder die Verfolgung begangener Straftaten entwickelt worden sind. Maßnahmen der Gefahrenabwehr, die in die Freiheitsrechte der Bürger eingreifen, setzen eine konkrete Gefahrenlage voraus. Die Strafverfolgung knüpft an den Verdacht einer schon verwirklichten Straftat an. Solche Bezüge fehlen, soweit die Aufgabe darin besteht, im Vorfeld der Gefahrenabwehr und Strafverfolgung Vorsorge im Hinblick auf in der Zukunft eventuell zu erwartende Straftaten zu treffen". Deshalb mussten hier die Bestimmtheitsanforderungen spezifisch an dieser Vorfeldsituation ausgerichtet werden.[1382] So muss die Ermächtigungsnorm zur vorbeugenden Telefonüberwachung „handlungsbegrenzende Tatbestandselemente enthalten, die einen Standard an Vorhersehbarkeit und Kontrollierbarkeit vergleichbar dem schaffen, der für die überkommenen Aufgaben der Gefahrenabwehr und der Strafverfolgung rechtsstaatlich geboten ist".[1383]

An diesen Beispielen wird deutlich, dass das *Bundesverfassungsgericht* durchaus vorsorgliche Erhebungen als verfassungsrechtlich zulässig erachtet, allerdings nur, solange sie beschränkt sind. Soweit es festgestellt hat, dass die Vorratsdatenspeicherung nur als Ausnahme zulässig ist, ist dies auszulegen als Verbot vorsorglich anlassloser Datensammlungen.

[1379] BVerfGE 100, 313 (375 ff.).
[1380] BVerfGE 100, 313 (375 ff.).
[1381] BVerfGE 113, 348 (376).
[1382] BVerfGE 113, 348 (377).
[1383] BVerfGE 113, 348 (378).

Die Anlasslosigkeit ist deswegen relevant, weil nach ständiger Rechtsprechung des *Bundesverfassungsgerichts* Datenerfassungen, die der Betroffene durch sein Verhalten nicht veranlasst hat, ein grundsätzlich höheres Eingriffsgewicht beizumessen ist.[1384] Begründet wird dies damit, dass von einer anlassunabhängigen Erhebung verstärkt allgemeine Einschüchterungseffekte ausgehen können, die zur Beeinträchtigung der Grundrechtsausübung insgesamt führen können.[1385] „Die Unbefangenheit des Verhaltens wird insbesondere gefährdet, wenn die Streubreite von Ermittlungsmaßnahmen dazu beiträgt, dass Risiken des Missbrauchs und ein Gefühl des Überwachtwerdens entstehen."[1386]

Wichtig ist in diesem Kontext zwischen den Begriffen „verdachtsunabhängig" und „anlasslos" zu differenzieren: Verdachtsunabhängig ist etwa auch eine Videoüberwachung an einem gefährlichen Ort oder die vorbeugende Telekommunikationsüberwachung. So hat das *Bundesverfassungsgericht* etwa die Videoüberwachung des Verkehrs im Rahmen des Kfz-Kennzeichenscannings trotz ihrer Verdachtslosigkeit als zulässig erachtet.[1387] Das Gericht betont im Urteil zum Kfz-Kennzeichenscanning jedoch, dass die Maßnahme nicht anlasslos und flächendeckend durchgeführt werden dürfe.[1388] Eine Maßnahme die unterschiedslos eingesetzt wird, vermittelt das Gefühl ständiger Kontrolle – daher muss ihr Einsatz auf die Abwehr konkreter Gefahren begrenzt werden.

Insofern ist „anlasslos" noch stärker von einem Verdachts- und Gefahrenmoment entkoppelt als die Begriffe „verdachtsunabhängig" und „verdachtslos".[1389] Diese besagen allein, dass die Maßnahme unabhängig von einem konkreten Verdacht gegen eine bestimmte Person erfolgt. Auch eine Rasterfahndung, die zwar unabhängig von einem konkreten Verdacht gegen eine Person erfolgt, ist, so das *Bundesverfassungsgericht,* nur zulässig, wenn sie allein in bestimmten Gefahrensituationen durchgeführt wird.[1390] Eine generell anlassunabhängige Durchführung von Rasterfahndungen wäre hingegen nicht mit der Verfassung vereinbar.

[1384] BVerfGE 120, 378 (402) unter Verweis auf BVerfGE 100, 313 (376, 392); 107, 299 (320 f.); 109, 279 (353); 113, 29 (53); 113, 348 (383); 115, 320 (354).

[1385] BVerfGE 120, 378 (402) unter Bezugnahme auf BVerfGE 65, 1 (42); 113, 29 (46). „Grundrechtseingriffe, die sowohl durch Verdachtslosigkeit als auch durch eine große Streubreite gekennzeichnet sind -- bei denen also zahlreiche Personen in den Wirkungsbereich einer Maßnahme einbezogen werden, die in keiner Beziehung zu einem konkreten Fehlverhalten stehen und den Eingriff durch ihr Verhalten nicht veranlasst haben -- weisen grundsätzlich eine hohe Eingriffsintensität auf. Denn der Einzelne ist in seiner grundrechtlichen Freiheit umso intensiver betroffen, je weniger er selbst für einen staatlichen Eingriff Anlass gegeben hat. Von solchen Eingriffen können ferner Einschüchterungseffekte ausgehen, die zu Beeinträchtigungen bei der Ausübung von Grundrechten führen können." BVerfGE 120, 320 (354).

[1386] BVerfGE 120, 378 (402).

[1387] BVerfGE 120, 378.

[1388] BVerfGE 120, 378 (LS 2).

[1389] A. A.: *Gusy* 2011, 404 f. meint, dass das Gericht gerade auch in den Entscheidungen Rasterfahndung II, Kfz-Kennzeichenscanning und Vorratsdatenspeicherung anlassunabhängige Datenerhebungen für zulässig erachtet habe. *Gusy* differenziert hier jedoch nicht zwischen Verdachtslosigkeit und Anlassunabhängigkeit, entgegen der Argumentation des Verfassungsgerichts.

[1390] BVerfGE 115, 320.

Die Vorratsdatenspeicherung wird durch die hohe Aussagekraft der Daten, ihren flächendeckenden Einsatz (von dem tatsächlich nahezu jeder Bürger betroffen ist) und ihre Anlasslosigkeit geprägt und ist auch aus diesen Gründen und nur insoweit als Ausnahme in der Rechtsordnung der Bundesrepublik Deutschland zu charakterisieren. Eben nicht allein, weil sie verdachtsunabhängig durchgeführt wird, sondern weil bei ihr anlasslos und flächendeckend Daten auf Vorrat gespeichert werden, handelt es sich bei ihr um eine neue Stufe staatlicher Sicherheitspolitik. Sie schafft eine gesamtgesellschaftliche Überwachungsinfrastruktur, die am Ausnahmefall orientiert ist und von der jeder betroffen ist.

Laut dem Dictum des Gerichts muss die Vorratsspeicherung der Telekommunikationsverkehrsdaten genau in dieser Hinsicht eine Ausnahme bleiben. Weitere anlasslose, infrastrukturelle Überwachungsinstrumente würden die Identität der Verfassung verletzen. Grundsätzlich hat sich die Gesetzgebung aber bezüglich der Verarbeitung personenbezogener Daten am Regelfall und nicht am Ausnahmefall zu orientieren.

7.2.2 Keine umfassende gesamtgesellschaftliche Überwachung

Ob eine umfassende gesamtgesellschaftliche Überwachung realisiert wird, ist nicht nur davon abhängig, ob die Vorratsdatenspeicherung eine Ausnahme und damit das einzige infrastrukturelle Überwachungsinstrument bleibt, sondern es kommt genauso darauf an, dass insgesamt keine umfassende gesamtgesellschaftliche Überwachung realisiert wird. Soweit diese schon durch die Vorratsdatenspeicherung selbst realisiert würde, wäre die Grenze ebenso überschritten. Sodann gilt es auch für die Gesamtheit staatlicher Datenerhebungen.

Darin, dass das *Bundesverfassungsgericht* im Urteil zur Vorratsdatenspeicherung zwar die Notwendigkeit sah auf das Verbot einer umfassenden gesamtgesellschaftlichen Überwachungen hinzuweisen und aus dem Verhältnismäßigkeitsgrundsatz heraus hohe Anforderungen an die Ausgestaltung der Vorratsdatenspeicherung ableitet, kommt zum Ausdruck, dass das Gericht die Grenze totaler Erfassung und Registrierung als nahezu erreicht sieht. Aus dem Verbot einer umfassenden gesamtgesellschaftliche Überwachung folgt insofern zukünftig die Pflicht bei der Einführung neuer Überwachungsinstrumente zu fragen, ob mit ihnen diese Grenze überschritten wird. Erforderlich ist insofern, wie *Roßnagel* fordert, die Durchführung einer doppelten Verhältnismäßigkeitsprüfung.[1391]

„Die verfassungsrechtlich geforderte zivilisatorische Leistung ist es, im Interesse der Freiheit darauf zu verzichten“ alle Aktivitäten aller Bürger umfassend und vollständig zu überwachen. „Daher ist künftig eine doppelte Verhältnismäßigkeitsprüfung notwendig: Zum einen ist auf der Grundlage der Wirkungen eines Überwachungsinstruments dessen verhältnismäßiger Einsatz zu bewerten. Zum anderen ist aber zusätzlich auf der Basis einer Gesamtbetrachtung aller verfügbaren staatlichen Überwachungsmaßnahmen die Verhältnismäßigkeit der Gesamtbetrachtung aller verfügbaren staatlichen Überwachungsmaßnahmen die Verhältnismäßigkeit der Gesamtbelastungen bürgerlicher Freiheiten zu prüfen“.[1392]

[1391] *Roßnagel*, NJW 2010, 1238, 1240.
[1392] *Roßnagel*, NJW 2010, 1238, 1240.

Da mit einer Vorratsdatenspeicherung diese Grenze beinahe erreicht ist, ist es möglich, um zu ermitteln, wann die Grenze überschritten wäre, zunächst zu untersuchen, wie hoch der gesamtgesellschaftliche Grad an Überwachung zum Zeitpunkt des Urteils war. Um diesen Stand zu ermitteln, sollte geprüft werden welche verdachtsunabhängigen Maßnahmen der Strafverfolgungsbehörden und Nachrichtendienste es gibt, welche Ermittlungsinstrumente in welchem Umfang eingesetzt werden und auf welche Datenbanken der Staat zugreifen kann. Auch ist von Bedeutung unter welchen Sicherheitsstandards die Daten verarbeitet werden.

Ein Vielfaches dieses Überwachungsgrades würde unweigerlich gegen das Verbot einer umfassenden gesamtgesellschaftlichen Erfassung und Registrierung verstoßen. Da das Grundgesetz dynamischen Entwicklungen offen steht,[1393] können solche Bewertungen allerdings immer nur für die aktuelle geschichtliche Situation gelten.

Der gesamtgesellschaftliche Überwachungsgrad wäre evident um ein Vielfaches gesteigert, wenn regelmäßig Rasterfahndungen durchgeführt würden, die Verdachtsschwelle für die inhaltsbezogene Telekommunikationsüberwachung nivelliert würde, Kontostammdatenabfragen flächendeckend erfolgen würden oder sich generell feststellen ließe, dass sich das Verhältnis von Betroffenen von Ermittlungsmaßnahmen zum Anteil an Straftaten grundlegend verschoben hat. Ein weiteres Beispiel wäre auch eine signifikante Ausweitung der Videoüberwachung, etwa wenn diese, ob in privater oder staatlicher Hand, so breit eingesetzt wird, dass letzten Endes nahezu die Gesamtfläche der Bundesrepublik Deutschland mit Videokameras überwacht wird.

Für das Verbot umfassender gesamtgesellschaftlicher Überwachung ist also im Rahmen einer doppelten Verhältnismäßigkeit eine Gesamtbetrachtung des Überwachungsgrads durchzuführen. Dabei sind auch Datenerhebungen und -speicherungen durch Private miteinzubeziehen, denn auf diese können, soweit ein begründeter Verdacht einer Straftat oder eine konkrete Gefahr besteht, staatliche Behörden zugreifen.[1394]

7.2.3 Offene Fragen

Diese ersten Ansätze zur Konkretisierung des Schutzgehalts des Verbots umfassender gesamtgesellschaftlicher Überwachung sind noch sehr vage und lassen viele Fragen offen, etwa: Wie kann denn genau der Grad gesamtgesellschaftlicher Überwachung bestimmt werden? Was folgt aus ihm? Und was bedeutet die Forderung nach einer Überwachungs-Gesamtrechnung für Exekutive, Legislative und Judikative? Was folgt daraus, wenn ein Instrument eingeführt wird und damit die Grenze überschritten wird?[1395] Diese Fragen gilt es zu erörtern, denn das Verbot umfassender Überwachung

[1393] Vgl. oben S. 219 f.

[1394] Die §§ 102 ff. StPO ermächtigen zur Durchsuchung von Speichermedien, ausführlich dazu *Herrmann/Soiné,* NJW 2011, 2922, 2923. Erforderlich ist hierfür im Regelfall eine richterliche Anordnung, § 105 StPO;

[1395] *Hornung/Schnabel*, DVBl. 2010, 824, 827 werfen die Fragen auf: „Welche der beiden müsste im Zweifel zurücktreten? Die letzte, weil sie unter Verstoß gegen die Maßgaben des *Bundesverfassungsgericht* verabschiedet wurde oder in Anwendung der lex-posterior Regel die erste? Was geschieht, wenn beide oder nur eine Maßnahme auf europarechtlichen Vorgaben beruht? Sind parallele landesrechtliche Überwachungsmaßnahmen mit einzubeziehen (mit der potentiellen Folge,

und Registrierung wird nur dann Wirkungskraft entfalten können, wenn auch diese Fragen beantwortet werden.

7.3 Die Überwachungs-Gesamtrechnung

Zunächst ist zu untersuchen, wie genau der aktuelle Grad gesamtgesellschaftliche Überwachung ermittelt werden kann – was also die Grundlage und den Maßstab für eine künftig durchzuführende Gesamtrechnung bildet (Kap. 7.3.1). In einem zweiten Schritt soll aus den verfassungsrechtlichen Vorgaben heraus entwickelt werden, was das Erfordernis einer doppelten Verhältnismäßigkeitsprüfung für Exekutive, Legislative und Judikative im Einzelnen bedeutet (Kap. 7.3.2). Abschließend soll dann konkret am Beispiel der Kumulation von Vorratsdatenspeicherung und Speicherung von Fluggastdaten auf Vorrat erörtert werden, ob diese das Verbot umfassender gesamtgesellschaftlicher Überwachung verletzen würde (Kap. 7.3.3).

7.3.1 Aktueller Grad gesamtgesellschaftlicher Überwachung

Die Bewegungs- und Persönlichkeitsanalyse, wie sie durch die Vorratsdatenspeicherung ermöglicht wird, führt nach Ansicht des *Bundesverfassungsgerichts* noch nicht zu einer strikt verfassungswidrigen umfassenden gesamtgesellschaftlichen Überwachung. Aber wann wäre das der Fall? Wenn sich das Handy im Sekundentakt in eine neue Funkzelle einwählen würde? Die Funkzellen deutlich kleiner wären? Wenn auch Inhalte besuchter Web-Seiten gespeichert würden? Wenn hinzu noch von jedem öffentlichen Platz Videoaufnahmen existierten, die dann mit den Bewegungsdaten der Vorratsdatenspeicherung kombiniert werden könnten? Wenn Internet-Passwörter auf Vorrat gespeichert würden, um so auch die Aktivitäten in sozialen Netzwerken kontrollieren zu können?[1396] Kommt es darauf an, wie technophil der Einzelne oder die Gesellschaft insgesamt ist?

Entscheidend kann letztlich nicht sein, wie exakt das Leben jedes einzelnen Bürgers nachvollzogen werden kann. Denn dies ist immer primär eine Frage der persönlichen Lebensweise (also wie oft jemand kommuniziert und was er an persönlichen Informationen – etwa im Internet aber auch in geschlossen Netzwerken – Preis gibt) und der Lebensbedingungen (so werden etwa Asylbewerber oder Empfänger von Sozialleistungen stärker als andere überwacht). Das Verbot umfassender gesamtgesellschaftlicher Überwachung zielt nicht darauf, den Einzelnen vor einer umfassenden Erfassung und Registrierung zu bewahren – hier ist das Verbot einer Rundumüberwachung und

---

dass eine Maßnahme des Bundes in einem Land verfassungswidrig, in einem anderen verfassungsgemäß sein könnte), und wie wäre der resultierende Kompetenzkonflikt zu bewältigen? Wie soll mit dem Problem umgegangen werden, dass bestimmte Berufsgeheimnisträger von einigen Überwachungsmaßnahmen ausgenommen sind, und umgekehrt andere Gruppen wie Asylbewerber oder Empfänger von Sozialleistungen zusätzlichen Datenerhebungen unterliegen)? Soll schließlich auch die Kontrollpraxis mit berücksichtigt werden mit der Folge, dass etwa die kontinuierlich steigende Zahl der Telekommunikationsüberwachungen durch Ermittlungsbehörden den Spielraum des Gesetzgebers einengen würde, obwohl sich die gesetzliche Lage nicht geändert hat?“ Mit ersten Antworten *Roßnagel*, DuD 2010, 544, 546 f.

[1396] Bspw. werden in Frankreich nach einer neuen Verordnung auch Internetpasswörter auf Vorrat gespeichert http://www.zeit.de/digital/datenschutz/2011-03/Passwoerter-Frankreich-speichern.

der Bildung von Persönlichkeitsprofilen einschlägig[1397] –, vielmehr kommt es darauf an, die freiheitliche Grundordnung zu erhalten, um dem Einzelnen eine freie Entfaltung seiner Persönlichkeit, durch die Gewährleistung einer grundsätzlichen Freiheit, zu ermöglichen.[1398] Insofern geht es um eine Betrachtung der Gesellschaft insgesamt. Daher ist es erforderlich, generell den Grad gesamtgesellschaftlicher Überwachung zu ermitteln und nicht bezüglich einer konkreten Person. Es bedarf daher einer typisierenden Betrachtung unterschiedlicher Lebensweisen und -bedingungen ohne diese zu generalisieren.

Insgesamt kann der Grad gesamtgesellschaftlicher Überwachung nicht exakt in einer bestimmten Einheit angegeben werden. Es handelt sich vielmehr um einen auslegungsbedürftigen Begriff. Es kann daher hier auch nur aufgezeigt werden, was bei der Beurteilung des Grades gesamtgesellschaftlicher Überwachung zu berücksichtigen ist und nicht dieser in einer exakten Zahl bemessen werden. Es geht nicht um eine exakte zahlenmäßige Kategorisierung, sondern darum eine wertungsmäßige Betrachtung vorzunehmen um das Bewusstsein für den Umfang der gesellschaftlichen Überwachung zu schärfen.

Die Elemente, die insgesamt den Grad gesamtgesellschaftlicher Überwachung beeinflussen, können Indizien dafür sein, dass das Verbot einer umfassenden Erfassung und Registrierung verletzt wird, sollten sie sich grundlegend in Richtung eines Mehr an Erfassung entwickeln. Auf diese Art und Weise soll die im Rahmen der Überwachungs-Gesamtrechnung erforderliche wertende Betrachtung konkretisiert werden – die Abwägung entfällt dadurch aber keineswegs. Das Verbot umfassender gesamtgesellschaftlicher Überwachung ist und bleibt im Kern eine Abwägungsfrage. Damit sie aber nicht endlos ausgedehnt wird, ist es erforderlich, die Elemente, die den Grad gesamtgesellschaftlicher Überwachung prägen, so weit wie möglich zu konkretisieren.[1399]

- Welche Daten erhebt, erfasst und verarbeitet der Staat? Wie hoch ist die staatliche Überwachungsdichte?

Relevant ist für den Grad an gesamtgesellschaftlicher Überwachung zunächst, inwieweit der Staat selbst die Freiheitswahrnehmung der Bürger erfasst und registriert. Zentral wird die Überwachungsdichte durch infrastrukturelle Überwachungsmaßnahmen, wie die Vorratsdatenspeicherung, geprägt. Diese sind jedoch, wie dargelegt wurde, nur als Ausnahme zulässig.[1400] Das heißt es dürfen nicht systematisch immer mehr Vorratsspeicherungen eingeführt werden. Mehrere infrastrukturelle Überwachungsmaßnahmen wären strikt verfassungswidrig. In Bezug auf Vorratsspeicherungen ist im Rahmen der Gesamtbetrachtung zu berücksichtigen, welche Daten, in welchem Umfang und unter welchen Bedingungen auf Vorrat gespeichert werden.

[1397] Vgl. zu diesem oben Kap. 5.1.2.
[1398] Ausführlich zur verfassungsrechtlichen Grundlage und dem Schutzziel, vgl. oben Kap. 7.1; Kap. 7.2.
[1399] Zum Problem des Leerlaufs, wenn keine Konkretisierung erfolgt, oben Kap. 5.1.2, 6.3.
[1400] Dazu schon oben S. 231.

Auch sind Verwaltungsdaten miteinzubeziehen: Einmal jene, die dem Staat bezüglich jeden Bürgers zur Verfügung stehen, wie etwa Steuerdaten, sowie jene, die nur bezüglich einzelner in Verwaltungsverfahren erhoben werden, etwa betreffend Arbeitslosengeld, Wohngeld, Hartz IV, im Asylverfahren oder aus Baugenehmigungsverfahren. Soweit nur Einzelne oder bestimmte Gruppen betroffen sind, müssen diese Datenerhebungen dennoch in die Gesamtbetrachtung miteinbezogen werden, da sie das Gesamtbild beeinflussen. Durch die Erhebung und Speicherung biometrischer Daten in Ausweisdokumenten oder die Durchführung einer Volkszählung, steigen die Daten die beim Staat vorhanden sind. Auch wenn diese grundsätzlich dem Zweckbindungsgrundsatz unterliegen, können diese Daten objektiv auch für Strafverfolgung und Gefahrenabwehr abgerufen werden. Sie sind insofern für staatliche Sicherheitsbehörden quasi „Vorratsdaten", wenn sie ursprünglich für andere Zwecke gespeichert wurden ein Zugriff auf diese Daten aber unter bestimmten Umständen möglich ist.

Sodann spielen die Daten eine Rolle, die der Staat zu Strafverfolgungszwecken erhebt und verarbeitet. Es ist insofern für die Gesamtbetrachtung genau zu untersuchen: Was dürfen Polizei, Nachrichtendienste und der Verfassungsschutz? Wie oft wird welches verdachtsabhängige Überwachungsinstrument eingesetzt? Eine Rolle spielt hier wie die Eingriffs- und Zugriffsschwellen jeweils definiert sind ebenso wie die polizeiliche und nachrichtendienstliche Praxis. Hier ermöglichen es Statistiken über ihren Einsatz festzustellen, wie hoch der Anteil der Gesamtbevölkerung ist, der von solchen Maßnahmen betroffen ist. Dabei gilt es zu berücksichtigen, dass die absoluten Zahlen nicht automatisch Aufschluss darüber geben wie viele Personen betroffen waren. So sind die Anordnungen zur Telefonüberwachung gem. § 100a StPO in den letzten Jahren rasant angestiegen.[1401] Dies ist aber nicht nur dem geschuldet, dass wirklich häufiger auf das Instrument zurückgegriffen wird, sondern dass oft mehrere Anschlüsse zu einer Person überwacht werden.

Auch die Zusammenarbeit von Polizei- und Nachrichtendiensten und ihre Ausstattung mit Befugnissen sind für die Bemessung des Grads gesamtgesellschaftlicher Überwachung von Bedeutung.[1402]

Wesentlich ist es schließlich, zu ermitteln wie hoch der Anteil der Gesamtbevölkerung ist, der ins Zentrum polizeilicher Ermittlungen gerät. Diese Zahl ist ins Verhältnis zur Gesamtzahl an Straftaten zu stellen. Wenn sich dieses Verhältnis grundsätzlich verändert und zwar so, dass immer mehr Personen im Zentrum polizeilicher Ermittlungsarbeit stehen, deutet dies darauf hin, dass die Grenze umfassender Erfassung und Registrierung überschritten wurde.

[1401] Allein in Hessen stiegen die Zahlen im Jahr 2010 im Vergleich zu 2009 um 10 Prozent, http://www.gulli.com/news/17793-hessen-2010-zehn-prozent-mehr-telekommunikationsueberwachung-2012-01-03; Im Jahr 2000 wurden gem. §§ 100a, 100g StPO in 3353 Verfahren angeordnet (7512 Betroffene), im Jahr 2010 wurden in 5493 Verfahren Anordnungen gem. § 100a StPO erlassen; abrufbar sind die Statistiken über die Anordnung von TKÜ-Maßnahmen über http://www.bundesjustizamt.de/nn_2037064/DE/Themen/Buergerdienste/Justizstatistik/Telekommunikation/Telekommunikationsueberwachung__node.html?__nnn=true.

[1402] Zur Ausweitung polizeilicher Befugnisse der Geheimdienste und nachrichtendienstlicher Befugnisse der Polizei, vgl. oben Kap. 1.4.2.

Sodann sind auch all jene Daten miteinzubeziehen, die im Rahmen der Gefahrenabwehr erhoben werden. Hier sind etwa die Informationen zu berücksichtigen, die in Anti-Terrordatei und der Rechtsextremismus-Datei gespeichert werden.[1403] Es ist im Rahmen der Gesamtbetrachtung zu beachten, wie viele personenbezogene Daten hier jeweils gespeichert sind und unter welchen Voraussetzungen deren Erfassung erfolgt ist.[1404]

All diese Instrumente liefern dem Staat Informationen über die Freiheitswahrnehmung der Bürger. Sie bedingen insofern den Grad gesamtgesellschaftlicher Überwachung. Ganz generell ist bei der Ermittlung des Grads gesamtgesellschaftlicher Erfassung und Registrierung zu fragen, welche Freiheiten werden erfasst? Wie viel unbeobachtbares Leben findet noch statt? Welche Möglichkeiten gibt es am gesellschaftlichen Leben teilzunehmen ohne überwacht zu werden?

Fraglich ist, wie mit Unterschieden zwischen einzelnen Bundesländern umzugehen ist. So bestehen etwa unterschiedliche Anforderungen an die Videoüberwachung öffentlicher Räume oder es ist nicht überall eine Ermächtigung zur Durchführung von Online-Durchsuchungen normiert. Entscheidend ist im Ergebnis das Gesamtbild. Hier ist eine wertende Betrachtung unverzichtbar. Letztlich kann es für diese aber nicht darauf ankommen, ob nun x Kameras mehr in Bayern als in Niedersachsen hängen – schließlich ist gerade was den Grad gesamtgesellschaftlicher Überwachung angeht eine rein an den Ländergrenzen orientierte Betrachtung nicht zielführend: viele Bundesbürger überschreiten sehr häufig Landesgrenzen. Für die einzelnen Prüfverfahren und die auch in den Ländern vorzunehmende Gesamtbetrachtung, sind zwar landesspezifische Besonderheiten zu berücksichtigen, generell gilt es aber im Rahmen einer wertenden Gesamtbetrachtung den Gesamtgrad zu bemessen. Letztlich kommt es gerade in Bezug auf die Bedeutung der Unterschiede zwischen verschiedenen Bundesländern darauf an, was konkret der Prüfungsgegenstand ist und sodann auf die Sicht des jeweils betroffenen Grundrechtsträgers.

- Welche personenbezogenen Daten sind ansonsten vorhanden, auf die der Staat sich Zugriff verschaffen kann?

Miteinzubeziehen in die Überwachungs-Gesamtrechnung ist auch die Überwachung durch Private, denn zum einen kann der Staat im Verdachtsfall und in Gefahrensituationen auf diese Daten zugreifen.[1405] Zum anderen zielt das Verbot umfassender gesamtgesellschaftlicher Überwachung darauf die Freiheit der Gesellschaft und die freie Entfaltung des Einzelnen zu schützen. Es ist insofern unbeachtlich, ob eine umfassende gesamtgesellschaftliche Überwachung durch Staat oder durch Private ermöglicht wird, denn der Staat ist verpflichtet eine solche zu verhindern.
Zu berücksichtigen ist daher in welchem Umfang durch Private die Freiheitswahrnehmung der Bürger erfasst wird. Zu fragen ist etwa, wie die Speicherpraxis von Telekommunikationsunternehmen und Inhalte-Anbietern im Internet aktuell ist? Oder

[1403] Zu diesen schon oben, S. 64.
[1404] Dabei ist auch zu beachten, dass auch eine Rundumüberwachung nur einzelner Personenkreise wäre strikt verfassungswidrig wäre, BVerfGE 112, 304 (319).
[1405] Dazu *Herrmann/Soiné,* NJW 2011, 2922 ff.

auch: Wie hoch ist die Dichte privater Videokameras? Gerade Video-Überwachung wird heute immer häufiger von Privaten eingesetzt. Strikt verfassungswidrig, wäre eine Überwachungsdichte bei der man sich nicht mehr ohne erfasst zu werden bewegen kann, auch wenn vorrangig Private dazu beitragen.

Gleiches gilt für eine umfassende Speicherung der Bewegung im digitalen Raum: Wenn hier nicht nur die Bewegungen sondern auch die Inhalte, also was genau der Einzelne im Internet macht, nachvollzogen werden können, wäre eine verfassungswidrige umfassende Überwachung gegeben. So betont auch das *Bundesverfassungsgericht,* dass es „maßgeblich für die Rechtfertigungsfähigkeit einer solchen Speicherung" sei, „dass auch die Speicherung der von ihren Kunden aufgerufenen Internetseiten durch kommerzielle Dienstanbieter grundsätzlich untersagt ist".[1406] Wenn allerdings auf Grund von technischen Veränderungen oder veränderten Nutzungen, eine Speicherung durch kommerzielle Anbieter zur Regel wird, selbst wenn sie an sich grundsätzlich verboten ist, könnte dadurch eine umfassende Erfassung realisiert werden.

Derartige Tendenzen sind aktuell zu verzeichnen: So ist zwar an sich die Speicherung von IP-Adressen durch Seitenbetreiber verboten. Nutzungsdaten dürfen vielmehr gemäß § 15 Abs. 1 S. 1 TMG nur gespeichert werden, „soweit dies erforderlich ist, um die Inanspruchnahme von Telemedien zu ermöglichen und abzurechnen". Dennoch werden immer mehr IP-Adressen gespeichert, da immer mehr Angebote darauf beruhen, dass Informationen über die Nutzer zur Verfügung stehen.[1407] Auch zahlreiche staatliche Internetseiten speichern die Adressen der Nutzer.[1408] Sollte sich tatsächlich der Grundsatz umkehren, dass trotz des generellen Verbots der Speicherung von IP-Adressen der Seitenbesucher, diese überwiegend gespeichert werden, wäre die Frage, ob das Verbot umfassender gesamtgesellschaftlicher Überwachung nicht schon allein mit einer Vorratsspeicherung der Telekommunikationsverkehrsdaten verletzt wird, neu zu stellen.

- Welche technischen und gesellschaftlichen Veränderungen gibt es?

Geprägt wird der Grad gesamtgesellschaftlicher Erfassung und Registrierung auch durch das Maß, wie häufig und wie umfassend digitale Technik und Telekommunikation genutzt wird. Eine Veränderung hin zu einer immer stärkeren umfassenden Vernetzung, hin zu einem Internet der Dinge,[1409] wirft die Frage neu auf, ob damit nicht das Verbot einer umfassenden gesamtgesellschaftlichen Überwachung verletzt wird. Wenn etwa Waage und Kühlschrank, Brille, Foto und Fernseher auch über das Internet kommunizieren und diese Daten von einer Vorratsspeicherung erfasst werden, wird das Bild, das sich mittels auf Vorrat gespeicherter Telekommunikationsverkehrsdaten von jedem einzelnen erstellen ließe, noch viel exakter.
Auch durch die Umstellung auf IPv6 verändert sich die Aussagekraft der auf Vorrat gespeicherten Verkehrsdaten. Wenn nunmehr jedes privat genutzte Gerät über eine eigene, statische IP-Adresse verfügt, steigern sich die Analysemöglichkeiten bei einer

[1406] BVerfGE 125, 260 (321).
[1407] *Freund/Schnabel*, MMR 2011, 495, 497 f.
[1408] http://www.heise.de/newsticker/meldung/Mehrzahl-der-Bundesministerien-speichert-IP-Adressen-184012.html.
[1409] Dazu grundlegend oben S. 31.

Vorratsdatenspeicherung erheblich. In Bezug auf die Umstellung auf IPv6 ist insofern relevant, wie tatsächlich die Umstellung erfolgt: Sollte nunmehr exakt der Aufenthaltsort und die Aktivitäten im Netz zu jedem einzelnen Gerät nachvollzogen werden können, grenzt dies bereits an eine umfassende Überwachung der gesamten Freiheitswahrnehmung aller Bürger im Netz.

Aber nicht nur Veränderungen in der Telekommunikations- und Informationstechnik, sondern auch im Nutzungsverhalten gilt es zu berücksichtigen: Wie viele Informationen gibt der Einzelne bei der Ausübung seiner Grundrechte frei? Relevant ist hier etwa die Nutzung sozialer Netzwerke. Wenn jeder hier seinen Aufenthaltsort, sein Konsumverhalten und seine gesamten persönlichen Beziehungen preisgibt, ist darüber hinaus keine staatliche Überwachung mehr erforderlich. Es genügt insoweit der Zugriff auf den jeweiligen Account.[1410] Der Unterschied zu einer unmittelbaren Speicherung bei der Polizei besteht hier allerdings darin, dass es sich zum einen um eine Datensammlung handelt in die der Einzelne eingewilligt hat. Von der Vorratsdatenspeicherung ist sie sodann insofern abzugrenzen, als hier Daten bei Privaten für deren Zwecke gespeichert sind und dem Staat nur in einem konkreten Verdachtsfall oder in einer Gefahrensituation auf Grund einer richterlichen Erlaubnis übermittelt werden.

Die dort gespeicherten Informationen können zwar auf der einen Seite vielfach einen Anhaltspunkt für die Verfolgung und Aufklärung von Straftaten bzw. auch zum Schutz von Rechtsgütern liefern. Es ist allerdings Aufgabe des Staates sicherzustellen, dass auch nicht durch Private eine umfassende gesamtgesellschaftliche Überwachung realisiert wird und dass die informationelle Selbstbestimmung gewahrt bleibt. Wobei zu berücksichtigen ist, dass informationelle Selbstbestimmung durchaus auch das Recht auf Preisgabe seiner Daten beinhaltet. Allerdings bestehen insoweit staatliche Schutzpflichten zugunsten der informationellen Selbstbestimmung, als sichergestellt werden muss, dass der Einzelne auch tatsächlich frei über die Preisgabe seiner Daten entscheiden kann. In dieser Hinsicht werden staatliche Schutzpflichten aktiviert. Drohen etwa Internet-Riesen wie Facebook oder Google, durch spezifische Anwendungen eine nahezu lückenlose Dokumentation des Lebens aller Nutzer zu erstellen, ist es Aufgabe des Staates dafür Sorge zu tragen, dass diese Daten tatsächlich nur für die Zwecke, für die sie der Nutzer einstellt, genutzt werden. Es zeigt sich, dass mit wachsender Datenverarbeitung durch den Einzelnen auch die Pflicht des Staates wächst, aktiv für Datenschutz und Datensicherheit Sorge zu tragen. Kommt er dem nicht nach, droht das Verbot umfassender Überwachungen auf diesem Umweg verletzt zu werden.

[1410] Ein Zugriff auf diese Daten ist nach aktueller Rechtsprechung allerdings nur mit richterlicher Genehmigung möglich. Schwierigkeiten bestehen hier soweit Provider im Ausland stehen. Hier bedarf es dann der Rechtshilfe, dazu etwa http://*Beck*-aktuell.*Beck*.de/news/ag-reutlingen-beschlagnahmt-facebook-account-eines-angeklagten; *Meinicke* StV 2012, 463, der eine „Überforderung" der bestehenden strafprozessualen Instrumente im Kontext aktueller Entwicklungen im Bereich der IT diagnostiziert; *Neuhöfer* ZD 2012, 178, 179 betont, dass es dem Gesetzgeber obliege eine Klarstellung bzgl. der TKÜ-Überwachung von Nutzerkonten in sozialen Netzwerken zu schaffen; zur Beschlagnahme von Daten auch: *Klesczewski,* ZStW 2011 (123), 737 ff.

7.3.2 Auswirkungen der Überwachungs-Gesamtrechnung

Im Ergebnis sieht das *Bundesverfassungsgericht* den Spielraum für die Einführung zukünftiger Maßnahmen, wenn die Vorratsdatenspeicherungsrichtlinie umgesetzt wird, als „erheblich geringer" an, da bereits die aktuelle Überwachungsdichte sehr hoch ist. Um in Zukunft nicht gegen das Verbot umfassender gesamtgesellschaftlicher Überwachung zu verstoßen, ist der Gesetzgeber verpflichtet in Zukunft eine Überwachungs-Gesamtrechnung durchzuführen. Adressat dieser Verpflichtung ist primär der Gesetzgeber.[1411] Aber auch Exekutive und Judikative müssen sorgsam prüfen, ob eine die Identität der Verfassung verletzende umfassende gesamtgesellschaftliche Erfassung und Registrierung vorliegt. Denn alle drei Gewalten sind gem. Art. 1 Abs. 3 und Art. 20 Abs. 3 GG an die Verfassung gebunden und insofern auch berufen, die Identität, mithin ihren freiheitlichen Kern, zu schützen.

Zu untersuchen bleibt, welche Pflichten daraus konkret für die drei Gewalten folgen. Denn auch wenn es sich zwar um keine scharfe Grenze handelt, handelt es sich doch um ein verfassungsrechtlichen Grundsatz, der auch im Hinblick auf eine fortschreitende Digitalisierung, die Bedrohung durch den internationalen Terrorismus und die immer enger werdende internationale Zusammenarbeit bei der Bekämpfung dieses beachtet werden muss. Nur wenn eine systematische Einbindung der doppelten Verhältnismäßigkeitsprüfung gelingt, kann sichergestellt werden, dass diese Formel des *Bundesverfassungsgerichts* nicht nur von rechtswissenschaftlichem Interesse ist, sondern in der Praxis Wirkungskraft entfaltet. Die Verfassung verbietet eine umfassende gesamtgesellschaftliche Überwachung. Eine solche kann sowohl durch ein Hineinwachsen als auch durch die Verabschiedung neuer Gesetze erreicht werden.[1412]

Die Überwachungs-Gesamtrechnung ist auf Grund ihres Charakters als doppelter Verhältnismäßigkeitsprüfung vornehmlich unter zwei Gesichtspunkten zu betrachten: Einmal ist aus der Perspektive des Gesetzgebungsprozesses zu fragen, welche Anforderungen aus dem Verbot umfassender gesamtgesellschaftlicher Überwachung für eben dieses erwachsen. Zum anderen ist der Frage nachzugehen, wie das Verbot umfassender gesamtgesellschaftlicher Überwachung rechtlich durchgesetzt werden kann. Hier ist insbesondere das Augenmerk auf die Veränderungen durch das Mehrebenensystem Europa zu legen. Schließlich ist zu fragen, ob sich das Verbot einer umfassenden gesamtgesellschaftlichen Überwachung nicht auch auf die Exekutive auswirkt.

7.3.2.1 Beobachtungs-, Prüfungs- und Abstimmungspflichten

Der Gesetzgeber ist gemäß Art. 1 Abs. 3 GG an die Verfassung gebunden. Eine umfassende gesamtgesellschaftliche Überwachung verletzt die Identität der Verfassung – daraus folgt, die Verpflichtung der Legislative zu prüfen, ob diese Grenze überschritten wurde. Künftig ist es daher erforderlich im Gesetzgebungsverfahren eine doppelte Verhältnismäßigkeitsprüfung durchzuführen.[1413] Der Gesetzgeber muss sicherstellen,

---

[1411] *Hornung* sieht darin vorwiegend einen Appell an den Gesetzgeber, *Hornung,* PVS 2012, 377, 390.
[1412] So auch *Roßnagel,* NJW 2010, 1238, 1240.
[1413] *Roßnagel*, NJW 2010, 1238, 1240.

dass sich keine umfassende gesamtgesellschaftliche Überwachung realisiert: ihn treffen insofern Beobachtungs-, Prüfungs- und Abstimmungspflichten.

- Prüf-, und Beobachtungspflicht

Zunächst ist es die Pflicht der legislativen Gewalt im Gesetzgebungsverfahren zu prüfen, ob sich durch die Neueinführung eine umfassende gesamtgesellschaftliche Überwachung realisiert. Dies gilt auf nationaler wie auf supranationaler Ebene: Die Bundesregierung muss insoweit auch bevor sie sich in europäischen und internationalen Zusammenhängen zur Vereinbarung neuer Beschlüsse und Abkommen entschließt eine solche Gesamtrechnung durchführen.[1414]
Damit der Gesetzgeber überhaupt eine solche Gesamtrechnung durchführen kann, ist er verpflichtet, dafür vorzusorgen, dass das Wissen, welches er benötigt um den Grad gesamtgesellschaftlicher Überwachung bemessen zu können, vorhanden ist. Ihn trifft insofern eine Beobachtungspflicht. Was im Einzelnen dabei zu berücksichtigen ist, wurde im vorangegangen Abschnitt dargelegt.[1415] Ein Verfahren zu implementieren, wie genau die erforderliche Überwachungs-Gesamtrechnung nachvollziehbar gestaltet werden kann, ist Aufgabe des Gesetzgebers. Er muss die notwendige Infrastruktur für die Beobachtung schaffen. Das heißt er muss sicher stellen, dass mit Hilfe von statistischen Erhebungen, durch Meldepflichten und Verfahrensvorschriften für Behörden, die Überwachungsmaßnahmen durchführen, eine Situation geschaffen wird, mittels derer die von der Überwachungs-Gesamtrechnung vorausgesetzten Daten erhoben werden. Neben dieser kontinuierlichen Beobachtungspflicht trifft den Gesetzgeber auch vor der Verabschiedung neuer Gesetzesvorhaben eine Prüfpflicht.

Auch die Vertreter Deutschlands im Europäischen Rat sind dazu verpflichtet, soweit auf europäischer Ebene Richtlinien oder Verordnungen verabschiedet werden sollen, die zu einem Anwachsen des gesamtgesellschaftlichen Überwachungsgrades führen würden, sorgsam zu hinterfragen, ob damit eine Verletzung der Identität der Verfassung droht. Das *Bundesverfassungsgericht* hat ausdrücklich klargestellt, dass die Bundesrepublik sich in europäischen und internationalen Zusammenhängen für die Wahrung der Identität der Verfassung „einsetzen muss".[1416] Es kann insofern nicht genügen, dass sich die Vertreter der Bundesrepublik im Europäischen Rat bei der Verabschiedung neuer umfassender Datensammlung einfach nur vornehm enthalten und überstimmen lassen. Es ist Aufgabe der Vertreter sich für die Beachtung des verfassungsrechtlichen Verbots einer umfassenden gesamtgesellschaftlichen Erfassung und Registrierung „einzusetzen". Erst dann, wenn ein gegen den Widerstand Deutschlands wegen drohender Verletzung der Identität der Verfassung verabschiedetes Gesetz, in einem Verfahren mit Beteiligung Deutschlands als europarechtskonform anerkannt worden sein, droht ein Konflikt zwischen nationalem Verfassungsrecht und europäischem Unionsrecht.

[1414] Denn auch über den Umweg Europa darf keine Totalüberwachung eingeführt werden, so BVerfGE 125, 260 (324).
[1415] Kap. 7.3.1, S. 236 ff.
[1416] BVerfGE 125, 260 (324).

Grundsätzlich zuständig für die Kontrolle des Grads gesamtgesellschaftlicher Überwachung zuständig. Es liegt aber nahe, dass eine solch umfassende Evaluation kaum unmittelbar durch den Bundestag gestemmt werden kann. Soweit er dies nicht selbst schafft, ist der Gesetzgeber aber verpflichtet sicherzustellen, dass die benötigten Informationen zur Verfügung stehen. Er muss also sicherstellen, dass durch eine geeignete Stelle die Überwachungs-Gesamtrechnung durchgeführt wird.

Üblich ist, dass derartige Spezialfragen in einem Ausschuss geklärt werden. Ein solcher müsste eingerichtet werden. In Frage käme die Einrichtung eines ständigen Ausschusses. Dieser müsste auch ermächtigt sein, Aufträge an dritte Stellen vergeben zu können, die alle für die Evaluation erforderlichen Informationen zusammenträgt.

Gegen die Durchführung der Überwachungs-Gesamtrechnung unmittelbar in einem Ausschuss, spricht, dass die Arbeit dort politisch geprägt ist. Die Evaluation sollte aber möglichst unabhängig erfolgen. In Betracht kommt insofern eine Beauftragung des Bundesbeauftragten für Datenschutz und Informationsfreiheit. Dafür spricht neben der Tatsache, dass er nicht politisch involviert ist, dass er in Bezug auf den Gewährleistungsgehalt des Rechts auf informationelle Selbstbestimmung geschult ist und schließlich bei ihm schon jetzt zahlreiche Informationen über staatliche wie private Datenverarbeitung zusammengetragen werden.

Sollte der Bundesbeauftragte für Datenschutz und Informationsfreiheit mit der Erstellung eines regelmäßigen Berichts zum Grad gesamtgesellschaftlicher Überwachung beauftragt werden, müsste er zunächst die gesamten Informationen, die auch bei Bundeskriminalamt, Landeskriminalämtern, Bundesnachrichtendienst, Länder- und Bundespolizeien erhoben werden, auswerten. Sodann müsste er ermächtigt werden, Aufträge zu verteilen, um technische und gesellschaftliche Veränderungen zu erfassen. Ansprechpartner für die Erstellung von Gutachten in Bezug auf technische und gesellschaftliche Veränderungen wäre etwa das Büro für Technikfolgen-Abschätzung[1417]. In Bezug auf Fragen der empirischen Sozialforschung könnten sodann unabhängige Forschungsinstitute beauftragt werden.

Für die Einbindung unabhängiger Forschungseinrichtungen in die Evaluation des gesamtgesellschaftlichen Überwachungsgrades spricht zunächst die Unabhängigkeit dieser Institute. Die Überwachungs-Gesamtrechnung ist in einem politisch hoch brisanten Feld durchzuführen. Von Bedeutung ist gerade deshalb, dass zu den einzelnen Elementen möglichst unabhängige Untersuchungen als Basis der wertenden Betrachtung zur Verfügung stehen.

Der Bundesbeauftragte für Datenschutz und Informationsfreiheit könnte im Rahmen seiner regelmäßigen Berichtspflichten[1418] auch zur gesamtgesellschaftlichen Überwachungsdichte Stellung nehmen. Damit könnte der Gesetzgeber seiner aus dem Verbot umfassender gesamtgesellschaftlicher Überwachung erwachsenden Beobachtungspflicht nachkommen.

[1417] http://www.tab-beim-bundestag.de/de/.

[1418] Der *BfDI* informiert in einem zweijährig erscheinenden Tätigkeitsbericht über seine Arbeit; http://www.bfdi.bund.de/DE/Oeffentlichkeitsarbeit/Taetigkeitsberichte/TB_node.html.

Insofern durch technische Veränderungen, veränderte Lebensbedingungen und Lebensweisen oder das Aufweichung der Eingriffsschwellen in der polizeilichen Praxis eine umfassende gesamtgesellschaftliche Überwachung in der Praxis realisiert wird – also nicht durch ein neues Gesetz, sondern durch ein „Hineinwachsen“,[1419] müsste der Gesetzgeber dafür Sorge tragen, dass dieses Ergebnis der Überwachungs-Gesamtrechnung bei allen drei Gewalten Gehör findet und diese in der Folge effektiv dazu beitragen den Überwachungsgrad zu minimieren.

Sodann trifft die Legislative die Pflicht in konkreten Gesetzgebungsverfahren, die auf die Einführung neuer Datenerhebungen oder anderer Überwachungsinstrumente zielen, eine Stellungnahme einzuholen, da der Gesetzgeber verpflichtet ist nicht nur die Verhältnismäßigkeit der Maßnahme an sich, sondern auch insgesamt zu überprüfen. Diese Verpflichtung gilt sowohl für den Landes- als auch für den Bundesgesetzgeber. Das heißt auch der Landesgesetzgeber muss vor der Verabschiedung neuer Sicherheitsgesetze eine doppelte Verhältnismäßigkeitsprüfung durchführen. Daraus folgt, dass auch die Landesdatenschutzbeauftragten über die erforderlichen Informationen verfügen müssen.

- Abstimmungspflicht im Rat der Europäischen Union

Auf Ebene der Europäischen Union können sich die Beobachtungs- und Prüfungspflichten bis hin zu einer Abstimmungspflicht verdichten. Durch die Übertragung von Hoheitsrechten auf die Europäische Union, insbesondere durch die erweiterten Kompetenzen durch den Lissabon Vertrag, werden zunehmend Datensammlungen, Überwachungsmaßnahmen und Regelungen über die Datenverarbeitung in den Mitgliedstaaten durch Europäische Rechtssetzungsakte bestimmt.[1420]
Im Rat der Europäischen Union ist die Bundesregierung vertreten. Hier sind somit nicht einzelne Volksvertreter abstimmungsberechtigt. Stimmberechtigt ist hier die Bundesregierung und damit das oberste Bundesorgan. Dieses ist an die Verfassung gebunden und auch verpflichtet, sich für die Wahrung der Identität der Verfassung in europäischen und internationalen Zusammenhängen einzusetzen.[1421] Woraus auch die Verpflichtung erwächst im Fall einer drohenden Verletzung der Identität der Verfassung durch ausufernde Datensammlungen gegen diese zu stimmen. Auch wenn das *Bundesverfassungsgericht* nicht explizit die Bundesregierung nennt, ist diese erster Adressat dieser Verpflichtung. Denn diese ist es, die primär die Interessen der Bundesrepublik in Europa und international vertritt.[1422] So handelt es sich eindeutig, um eine Pflicht der deutschen Vertreter im Rat diese Grenzen zu beachten.[1423]

[1419] Siehe hierzu *Roßnagel* DuD 2010, 544, NJW 2010, 1238.
[1420] Vgl. dazu oben S. 67 f; Die Europäischen Rechtsakte werden überwiegend im ordentlichen Gesetzgebungsverfahren gem. Art. 294 AEUV erlassen. Danach müssen Rechtsakte sowohl vom Rat der *Europäischen Union* als auch vom *Europäischen Parlament* angenommen werden.
[1421] BVerfGE 125, 260 (324).
[1422] Das *BVerfG* führt aus, dass sich die „Bundesrepublik in europäischen und internationalen Zusammenhängen“ für die Wahrung der Identität einsetzen, müsse, BVerfGE 125, 260 (324).
[1423] So auch *Bäcker*, EuR 2011, 103, 117.

Anderes gilt für die deutschen Vertreter im Europäischen Parlament. Diese verfügen über ein freies Mandat und sind daher auch nicht in ihrem Abstimmungsverhalten in Folge einer drohenden umfassenden gesamtgesellschaftlichen Überwachung beschränkt.

7.3.2.2 Eingeschränkter Gestaltungsspielraum des Gesetzgebers

Wichtig ist, dass bereits dann, wenn der aktuelle Grad gesamtgesellschaftlicher Überwachung merklich gesteigert würde, ein verfassungswidriger Zustand entstünde. Es wurde aufgezeigt, dass schon heute der Spielraum für die Einführung weiterer überwachungsintensiver Maßnahmen nur noch „gering" ist.[1424] Sollte die Überwachungs-Gesamtrechnung zu dem Ergebnis kommen, dass das Verbot einer umfassenden gesamtgesellschaftlichen Überwachung verletzt wurde, ist der Gesetzgeber gezwungen, zwischen den schon vorhandenen Instrumenten und dem neu-einzuführenden abzuwägen. Denn das neue Vorhaben kann nur realisiert werden, wenn er sich zugleich dafür entscheidet, in anderen Bereichen die Überwachung zu reduzieren.[1425] Die auszutauschenden Instrumente müssten von ihrer Überwachungsintensität her in etwa gleich sein. Um dies zu bemessen, sind die aufgezeigten Maßstäbe heranzuziehen mit welchen auch der Grad gesamtgesellschaftlicher Überwachung zu bestimmen ist.[1426]

Die Schwierigkeit besteht in praktischer Hinsicht darin, dass es kaum möglich ist zwei gleich stark eingreifende Überwachungsinstrumente zu finden, die sich eignen gegeneinander ausgetauscht zu werden. Neben dem Austausch zweier Instrumente gegeneinander besteht auch die Möglichkeit andere Überwachungsmaßnahmen durch rechtliche, technische und organisatorische Maßnahmen so auszugestalten, dass ihre Überwachungsintensität verringert wird. Auch hier besteht jedoch die Gefahr, dass nur scheinbar eine Reduktion versucht wird, tatsächlich aber durch die Einführung intensiver Maßnahmen und die Rücknahme oder Einschränkung bestehender Instrumente, schleichend immer weiter eingreifende Instrumente eingeführt werden. Entscheidend ist eine sorgsame Prüfung und Beobachtung gerade auch der Gesetzgebungsprozesse. Dies muss zum einen erfüllt werden durch die Prüf- und Beobachtungspflichten, die dem Gesetzgeber obliegen, zum anderen kann dem auch die Öffentlichkeit nachkommen, indem sie derartige Prozesse genau beobachtet.

7.3.2.3 Justiziabilität der Überwachungs-Gesamtrechnung

Das *Bundesverfassungsgericht* wäre verpflichtet, die Verfassungswidrigkeit festzustellen, sollte gegen das Verbot umfassender gesamtgesellschaftlicher Überwachung verstoßen werden. Allerdings handelt es sich um einen durch die Verfassung nicht konkret bestimmten Begriff, der lediglich durch eine Untersuchung verschiedener Elemente näher bestimmt werden kann.[1427] Aus ihr erwächst jedoch die Pflicht des Gesetzgebers die Grenze einer umfassenden gesamtgesellschaftlichen Erfassung und Registrierung bei Gesetzgebungsmaßnahmen zu beachten. Er ist verpflichtet den Grad gesamtgesellschaftlicher Überwachung zu beobachten und verfügt wie dargelegt wurde in bestimm-

[1424] BVerfGE 125, 260 (324); vgl. dazu bereits oben S. 234 f.
[1425] *Roßnagel*, DuD 2010, 544, 547.
[1426] Vgl. dazu oben S. 236 ff.
[1427] Vgl. dazu oben S. 224f., 227ff.

ten Situationen über einen eingeschränkten Gestaltungsspielraum. Dieser wird zwar, da es sich um keinen verfassungsrechtlich klar definierten Begriff handelt vom *Bundesverfassungsgericht* nicht en Detail geprüft werden. Dennoch ist die Überwachungs-Gesamtrechnung auch ein Prüfkriterium in der Beurteilung von Sicherheitsinstrumenten durch das *Bundesverfassungsgericht.*

Zum einen kann hinsichtlich einer Verletzung der gesetzgeberischen Pflicht zur Beobachtung und Prüfung Klage erhoben werden. Das Gericht ist insofern zuständig zu prüfen, ob der Gesetzgeber Erwägungen zum Grad gesamtgesellschaftlicher Überwachung in einem Gesetzgebungsverfahren berücksichtigt hat. Das Gericht kann prüfen, ob der Gesetzgeber die doppelte Verhältnismäßigkeit geprüft und beachtet hat. Auch kann Gegenstand verfassungsgerichtlichen Beurteilung sein, ob der Gesetzgeber seiner Beobachtungspflicht nachgekommen ist.

Zum anderen kann Gegenstand eines Verfahrens vor dem *Bundesverfassungsgericht* auch die Verletzung gesetzgeberischer Erfüllungs- und Gewährleistungspflichten sein. Wie schon im Urteil zur Vorratsdatenspeicherung, in welchem die Erwägungen zum Grad der gesellschaftlichen Erfassung und Registrierung zu der Formulierung des Verbots einer umfassenden gesamtgesellschaftlichen Überwachung führten,[1428] prüft das Gericht die Vereinbarkeit eines Sicherheitsinstruments oder einer Überwachungsinfrastruktur in einer doppelten Verhältnismäßigkeitsprüfung. Es prüft sowohl die Verhältnismäßigkeit der Maßnahme an sich als auch die Verhältnismäßigkeit des mit ihr erzielten Überwachungsgrades insgesamt. Sollte das Gericht einen Verstoß feststellen, wäre die jeweilige Maßnahme verfassungswidrig. Das *Bundesverfassungsgericht* würde dann nicht nach einer *lex-posterior* Regel[1429] das Instrument auswählen welches es als verfassungswidrig beurteilt. Feststellen kann es lediglich, dass (wenn dies in einer Klage gerügt wird und das Verbot einer umfassenden gesamtgesellschaftlichen Überwachung, ob durch die Einführung eines neuen Instruments oder durch veränderte gesellschaftliche Verwirklichungsbedingungen, verletzt wird), die in der Klage vorgelegte Maßnahme aufgrund des gegenwärtigen Verstoßes, verfassungswidrig ist. Das *Bundesverfassungsgericht* würde wohl feststellen, dass die Verhältnismäßigkeit insgesamt nicht gewahrt ist. Dem Gesetzgeber wäre dann aufgegeben, dem abzuhelfen.

Dann hat der Gesetzgeber die Möglichkeit durch die Auswahl zwischen verschiedenen Instrumenten sich für diejenigen zu entscheiden, die er für die Sicherheitsgewährleistung am bedeutendsten bewertet. Er kann jene aussetzen, deren Bedeutung er als geringer beurteilt, die aber von ihrer Überwachungsintensität her ähnlich hoch sind, um so insgesamt sicherzustellen, dass die Grenze umfassender gesamtgesellschaftlicher Überwachung nicht überschritten wird.

Justiziabel ist das Verbot einer umfassenden Erfassung und Registrierung auch insofern als gegen ein beschlossenes Abstimmungsverhalten im Rat mit dem die rechtliche Grundlage einer umfassenden gesamtgesellschaftlichen Überwachungsinfrastruktur geschaffen werden soll, vor dem *Bundesverfassungsgericht* geklagt werden könnte.

[1428] Vgl. dazu oben S. 227 ff.
[1429] Ob eine solche anzuwenden wäre, fragen *Hornung/Schnabel* DVBl. 2010, 824, 827.

Einmal kann durch die Mitglieder des Bundestags ein Organstreitverfahren angestrebt werden, da sobald eine Umsetzungspflicht besteht, deren Entscheidungsfreiheit beeinträchtigt wird. Denkbar ist in einer solchen Konstellation auch eine einstweilige Anordnung gegen die Zustimmung zu einem Europäischen Rechtsakt anzustreben.[1430] Dem Bürger bleibt die Möglichkeit, sich im Wege einer Verfassungsbeschwerde gegen eine konkrete Maßnahme zu wenden und sich darauf zu berufen, dass diese die Identität der Verfassung verletze, wenn mit ihr insgesamt eine gesamtgesellschaftliche umfassende Überwachung realisiert wird.

7.3.2.4 Zurückhaltung von Polizei- und Nachrichtendiensten

Das Ergebnis der Überwachungs-Gesamtrechnung wird entscheidend geprägt durch die polizeiliche und nachrichtendienstliche Praxis. Da Polizei und Nachrichtendienste ebenfalls an die Verfassung gebunden sind, müssen auch sie sich beim Einsatz von bestimmten Instrumenten fragen, ob sie damit die Überwachungsdichte hin zu einer verfassungswidrigen umfassenden gesamtgesellschaftlichen Überwachung steigern.

Wichtig ist insofern, dass die jeweilige Behörde nicht nur zur Erfüllung der Prüfungs- und Beobachtungspflichten der gesetzgebenden Gewalt Statistiken über ihr Handeln führt, sondern diese auch in die Entscheidung über den eigenen Einsatz von bestimmten Instrumenten einfließen. Die Exekutive ist insoweit verpflichtet dafür Sorge zu tragen, dass sich keine umfassende gesamtgesellschaftliche Überwachung durch eine Ausweitung der Überwachungspraxis aufgrund vorhandener Gesetze realisiert.

Bildlich lässt sich dies anhand der Videoüberwachung verdeutlichen: hier wäre eine flächendeckende Überwachung mit dem Verbot einer umfassenden Überwachung nicht vereinbar.[1431] Wenn insofern an einem Brennpunkt Videoüberwachung eingeführt werden soll, kann dies zwar für sich genommen verhältnismäßig sein, wenn so aber das gesamte Stadtgebiet videoüberwacht würde, wäre die Überwachung unverhältnismäßig. Dies muss die Exekutive bei der Anordnung und Durchführung von Sicherheitsmaßnahmen berücksichtigen.

7.3.3 Verfassungswidrigkeit von Vorrats- und Fluggastdatenspeicherung

Nachdem in den vorangegangenen Kapiteln abstrakt das Verbot einer umfassenden gesamtgesellschaftlichen Überwachung erörtert wurde, sollen die Erkenntnisse konkret auf die Einführung der Fluggastdatenspeicherung auf Vorrat, wie sie diskutiert wird (und wie sie zum Teil auch schon für einen Transfer in die USA gespeichert werden),[1432] angewendet werden.

[1430] § 32 BVerfGG.

[1431] Dazu oben Kap. 7.2.2.

[1432] Die USA können nach dem PNR-Abkommen bereits auf Fluggastdaten zugreifen, dazu *Krempl,* heise online v. 19.4.2012, abrufbar unter: http://heise.de/-154287. Nach dem PNR-Abkommen können die US-Behörden auf die Fluggastdaten aller europäischen Fluglinien zugreifen mit dem Zweck Straftaten zu verhindern oder zu verfolgen. In den USA dürfen die Daten ohne eine Anonymisierung 15 Jahre gespeichert werden.

Die Europäische Kommission hat im Jahr 2010 einen Richtlinienentwurf für eine Speicherung von Fluggastdaten auf Vorrat vorgelegt.[1433] Ähnlich wie die Vorratsdatenspeicherung sollte auch die Fluggastdatenspeicherung ursprünglich als Rahmenbeschluss eingeführt werden.[1434] Im April 2013 stimmte der EU-Innenausschuss zunächst gegen die Richtlinie[1435]. Das Schicksal des Vorhabens ist damit jedoch noch nicht endgültig beschieden.[1436]

Der Richtlinienentwurf sieht vor, dass die Fluggesellschaften verpflichtet werden die in ihren Buchungssystemen erfassten Fluggastdaten (auch PNR-Daten)[1437] von internationalen Flügen an eine eigens dafür zuständige Zentralstelle im Ankunfts- oder Abflugmitgliedstaat innerhalb der Europäischen Union zu übermitteln.[1438]

Es handelt sich also um keine Speicherpflicht der privaten Unternehmen (wie bei der Vorratsspeicherung der Telekommunikationsverkehrsdaten), sondern um eine Übermittlungspflicht. Ein unmittelbarer staatlicher Zugriff auf die Datenbanken der Fluggesellschaften ist nicht vorgesehen. Vielmehr soll ein dezentraler Datenbankverbund, aufgeteilt auf alle Mitgliedstaaten, errichtet werden. Die jeweiligen Sammel- und Auskunftsstellen in den Mitgliedstaaten müssen nach Vorstellung der Kommission so eingerichtet werden, dass die Sicherheit der Daten bei der Verarbeitung und während der Vorhaltung gewährleistet sowie eine Kontrolle durch eine unabhängige Stelle ermöglicht wird. In den Mitgliedstaaten sollen die Daten ausschließlich zu Zwecken der Verhütung, Aufdeckung, Aufklärung und strafrechtlichen Verfolgung von schwerer Kriminalität oder terroristischen Straftaten gespeichert und ausgewertet werden und zu diesen Zwecken an die dafür zuständige Behörden übermittelt werden.[1439] Dem Richt-

[1433] Kom (2011) 32; Ristock. 6007/11; Der Juristische Dienst des Rats hat sich in zwei Gutachten mit dem RL-Entwurf befasst, Dok. 8230/11; 8850/11. Kritisch zum Fluggastdaten-Transfer in die USA generell und in Bezug auf den Richtlinienentwurf, *Boehm*/*Hornung* 2012

[1434] KOM (2007)/854 endg.; Ratsdok. 14922/07. Der Rahmenbeschluss sah eine Speicherung der Daten über 13 Jahre vor. Bei einer Neuregelung soll die Speicherung auf 5 Jahre begrenzt werden. Die Daten der Fluglinien sollen, außer wenn ein Verdacht besteht, nach 30 Tagen anonymisiert werden. Der Bundesrat kritisierte 2008, dass der Rahmenbeschluss insgesamt nicht verhältnismäßig sei, auch wenn er grundsätzlich den Ansatz unterstütze, BR Drs. 826/01/07.

[1435] https://netzpolitik.org/2013/richtlinie-uber-fluggast-daten-eu-innenausschuss-stimmt-gegen-vorratsdatenspeicherung-von-reisenden/

[1436] Ausführlich dazu: *Hornung,* ZRP 2013, 97.

[1437] PNR = Passenger-Name-Record. Sie umfassen in aller Regel 19 Datenkategorien. Dazu gehören neben Namen, E-Mail-Adresse, Telefon-, Konten- und Kreditkartennummern auch etwaige Essenswünsche. Viele Fluglinien bieten nicht nur vegetarisches Essen als Alternative an, sondern auch koscheres oder Gluten freies Essen, um religiösen oder gesundheitlichen Wünschen/ Bedürfnissen der Fluggäste zu entsprechen. Emirates bietet bspw. 22 verschiedene Menüs an, http://www.emiratesagent.at/10148987. Aus der entsprechenden Wahl eines Menüs werden Rückschlüsse auf Krankheiten oder Religionszugehörigkeiten ermöglicht.

[1438] Art. 4 Abs. 1 s. 1 des Richtlinienentwurfs, KOM (2011) 32. Die Pflicht der Mitgliedstaaten zur Einrichtung einer PNR-Zentralstelle ergibt sich aus Art. 3 Abs.1 des Richtlinienentwurfs. Das Verfahren bei dem die Fluggesellschaft die benötigten PNR-Daten in die Datenbank der zuständigen Behörde einspeisen wird auch als „Push-Methode" bezeichnet.

[1439] Art. 5 verpflichtet die Mitgliedstaaten, die zuständigen Behörden ausdrücklich zu benennen und eine Liste dieser an die Kommission innerhalb von 12 Monaten zu übermitteln. Laut Erwägungs-

linienentwurf zufolge sollen die Strafverfolgungsbehörden der Mitgliedstaaten die Daten 30 Tage nach dem jeweiligen Flug „anonymisieren". Dabei ist jedoch keine faktische Anonymisierung i. S. d. § 3 Abs. 6 BDSG vorgesehen,[1440] denn die Identität des Fluggastes soll nach Art. 9 Abs. 2 des Richtlinienentwurfs lediglich „nicht sichtbar" sein.[1441] Insgesamt dürfen die Fluggastdaten für höchstens fünf Jahre gespeichert werden. Nicht übermittelt werden sollen besonders sensitive Daten. Als solche gelten Daten, die Aufschluss geben können über rassische oder ethnische Herkunft, politische Einstellungen oder religiöse oder weltanschauliche Überzeugungen, ihre Mitgliedschaft in einer Gewerkschaft, ihren Gesundheitszustand oder ihr Sexualleben.[1442] Nach dem aktuellen Vorschlag sollen nur Daten über Flüge aus und innerhalb der Europäischen Union gespeichert werden, während die PNR-Datensätze bezüglich innereuropäischer Flüge nicht von der Speicherpflicht erfasst sind.[1443]

Der Richtlinienentwurf sieht vier Verarbeitungsvorgänge vor. Demnach sollen vor Abflug und vor Ankunft des Fluges die PNR-Daten einer eingehenden Prüfung unterzogen werden, indem die Datenbank anhand von „im Voraus festgelegten Kriterien" durchsucht wird und jeder Treffer der automatisierten Analyse nochmals genauer auf nicht-automatisierte Art überprüft werden soll. Im Nachhinein soll ein Zugriff auf die Daten bei begründeten Anfragen zuständiger Behörden möglich sein sowie eine weitergehende Verarbeitung der Daten zum Zweck der Aktualisierung oder Aufstellung neuer Kriterien erfolgen.[1444]
Sollte an einer Vorratsspeicherung der Telekommunikationsverkehrsdaten festgehalten werden und darüber hinaus eine Fluggastdatenspeicherung, wie im Richtlinienentwurf vorgesehen, eingeführt werden, stellt sich konkret die Frage, ob damit nicht das Verbot einer umfassenden gesamtgesellschaftlichen Überwachung realisiert wird.[1445]

Es handelt sich um zwei Maßnahmen, die unabhängig von einem Verdacht oder einer Gefahrensituation zu einer Speicherung personenbezogener Daten ermächtigen. Die Speicherung von Fluggastdaten, wie sie im Richtlinienentwurf vorgesehen ist, verursacht keinen gleich schweren Eingriff wie die Speicherung sämtlicher Telekommunikationsverkehrsdaten auf Vorrat. Zwar werden die Daten auch anlassunabhängig erhoben, dennoch ist die Überwachungsintensität der vorgeschlagenen Fluggastdatenspei-

---

grund 7 dienen nicht primär zur Aufklärung von Straftaten sondern im Wesentlichen als Verdachtsgewinnungsinstrument.

[1440] Hier wird die Anonymisierung legal definiert als „das Verändern personenbezogener Daten, derart, dass die Einzelangaben über persönliche oder sachliche Verhältnisse nicht mehr oder nur mit einem unverhältnismäßig großen Aufwand an Zeit, Kosten und Arbeitskraft einer bestimmten oder bestimmbaren natürlichen Person zugeordnet werden können", siehe dazu auch *Spindler/Nink* in *Spindler/Schuster*, Recht der elektronischen Medien, 2011, § 13 TMG, Rn. 11-14a.

[1441] Dass dies keine Anonymisierung ist, macht auch Juristische Dienst deutlich, Dok. 8850/11, S. 3.

[1442] Gemäß Art. 3 Abs. 3 des Richtlinienentwurfs dürfen diese PNR-Daten nicht als Prüfkriterien herangezogen werden; S.a. Art. 5 Abs.6; Art. 11 Abs. 3.

[1443] Eine solche war zwar von der Kommission angedacht aber aktuell noch für zu aufwendig und teuer erachtet worden. http://.www.heise.de/newsticker/meldung/Neuer-Vorstoss-zur-Auswertung-von-Fugpassagierdaten-auf-EU-Ebene-1182425.html.

[1444] Art. 4 Abs. 2 a-d.

[1445] Daneben ist zudem schon die Vereinbarkeit einer Fluggastdatenspeicherung mit europäischen Grundrechten umstritten, ausführlich dazu *Boehm,* KritV 2012, 82 ff.

cherung geringer als jene der Vorratsdatenspeicherung. Es werden lediglich die Daten von außereuropäischen Flügen gespeichert. Das heißt, die Erhebung erfolgt zwar anlasslos, aber nur in Bezug auf Flüge ins Ausland, sodass die tatsächlich betroffene Gruppe deutlich kleiner ist als bei der Speicherung von Telekommunikationsdaten. Auch sind die Aussagekraft der Daten und ihre Analysemöglichkeiten weitaus geringer. Sie ermöglichen nicht wie die Vorratsdatenspeicherung die Erstellung umfassender Persönlichkeits- und Bewegungsprofile.[1446]

Dennoch handelt es sich um eine umfassende, anlasslose Datensammlung, die unter anderem höchst sensitive Informationen beinhaltet. Sie ermöglicht es Kontakte und Verbindungen von Personen ins Ausland durchschaubar zu machen. Personen könnten allein deshalb in Verdacht geraten, weil sie in bestimmte Länder reisen oder bestimmte Menü-Wünsche angeben.

Eine verdachtsunabhängige Speicherung von Fluggastdaten bedeutet einen schwerwiegenden Eingriff in die durch Art. 2 Abs. 1 GG geschützte Ausreisefreiheit[1447] und das informationelle Selbstbestimmungsrecht. Betroffen sind zudem die Religionsfreiheit, die Versammlungsfreiheit sowie die Pressefreiheit. Da sich aus den gesammelten Daten jeweils Informationen über die von diesen Grundrechten geschützten Bereiche extrahieren lassen.

Letztlich lassen sich beide Instrumente als Teil einer umfassenden staatlichen Überwachungsinfrastruktur begreifen. Die Speicherung der Telekommunikationsverkehrsdaten ist eine anlasslose und infrastrukturelle Datensammlung über Bewegungen und Kontakte der Bürger innerhalb der Europäischen Union, während die Fluggastdatenspeicherung das Reiseverhalten erfasst und insofern die Verbindungen nach außen betrifft. Der Grad gesamtgesellschaftlicher Überwachung wird durch diese Ausdehnung erheblich gesteigert.

Zwar ist für die Eingriffsintensität von beiden Datensammlungen auf Vorrat der Zeitraum von Bedeutung für den die Daten vorzuhalten sind, da dies die Genauigkeit der ableitbaren Persönlichkeitsprofile beeinflusst. Allerdings ändert auch eine kurze Speicherfrist nichts daran, dass es sich um einen schwerwiegenden Eingriff handelt. Denn schon der flächendeckende Charakter der anlasslosen Datenerhebung begründet jeweils das besondere Gewicht des Eingriffs.

Die Fluggastdatenspeicherung macht einen anderen Teil personenbezogener Informationen verfügbar, der die durch die Telekommunikationsspeicherung erhobenen Datensätze ergänzt und so das Netz staatlicher Überwachungsinstrumente erweitert. Auch spricht für eine Verfassungswidrigkeit der Kumulation von Vorratsdatenspeicherung und PNR-Speicherung, dass das *Bundesverfassungsgericht* im Urteil zur Vorratsdatenspeicherung betont hat, dass der Spielraum für weitere Maßnahmen auch über den

[1446] Zu der Möglichkeit Persönlichkeitsprofile aus den auf Vorrat gespeicherten Verkehrsdaten zu erstellen, oben S. 182 f.

[1447] *Durner* in *Maunz/Dürig*, GG 2012, Art. 11, Rn. 102. Ausführlich zum Streit, ob Art. 11 GG auch die Ausreisefreiheit schütze Rn. 98 ff; *Dreier, in: Dreier,* GG 2004, Art. 2 I Rn. 35.

Umweg Europa gering sei und dies zu einem Zeitpunkt, zu welchem Vorhaben gerade die Fluggastdatenspeicherung auf europäischer Ebene diskutiert wurde.

Es handelt sich, sollten Telekommunikationsverkehrsdaten und Fluggastdaten auf Vorrat gespeichert werden, um zwei anlasslose Datenerhebungen mit denen jeweils eine Überwachungsinfrastruktur geschaffen wird und deren parallele Einführung gegen das Gebot verstoßen würde, eine Vorratsspeicherung nur als „Ausnahme" zuzulassen.[1448] Die Ausnahme würde damit zwar noch nicht zur Regel, aber ihren Ausnahmecharakter würde sie verlieren.

Die Einführung einer Telekommunikationsverkehrs- und einer Fluggastdatenspeicherung kumulativ verletzt die Identität der Verfassung, da sie zu einer umfassenden gesamtgesellschaftlichen Überwachung führt.

Sollte im Rat der Europäischen Union über den Richtlinienentwurf abgestimmt werden, müsste Deutschland – solange die Vorratsdatenspeicherungsrichtlinie in Kraft ist – gegen ein derartiges Vorhaben stimmen. Es wurde aufgezeigt, dass die Bundesregierung verpflichtet ist, sich dafür einzusetzen, dass auch über den Umweg Europa keine Instrumente eingeführt werden, die geeignet sind die Identität der Verfassung zu verletzten.

In der aktuellen politischen Diskussion ist insofern die Bundesregierung aufgerufen, abzuwiegen, welches der beiden Instrumente – Fluggastdatenspeicherung oder Vorratsdatenspeicherung – einen größeren Beitrag zur Verfolgung und Verhinderung von Terrorismus und organisierter Kriminalität leistet. Die Bundesregierung kann sich insofern nur für *ein* Instrument von beiden entscheiden. Denn es handelt sich bei beiden Instrumenten um anlasslose Datenerhebungen, die jedoch das Grundgesetz nur als Ausnahme zulässt.

Entscheiden kann sich der Gesetzgeber aber nur, insoweit er einen Gestaltungsspielraum hat. Daher ist die Bundesrepublik verpflichtet, sich dafür einzusetzen, dass nicht zwei Richtlinien in Kraft sind, zu deren Umsetzung Deutschland verpflichtet ist, die aber in Kumulation die Identität der Verfassung verletzen.

Denkbar ist insofern, dass darauf hingewirkt wird, dass die Vorratsdatenspeicherungsrichtlinie insofern geöffnet wird, als sie auch in Gestalt eines Quick-Freeze-Verfahrens umgesetzt werden kann. Dann könnte Deutschland die Vorratsdatenspeicherung nicht als vorsorglich, anlasslose Datensammlung umsetzen, sondern mittels eines Quick-Freeze-Verfahrens[1449] als anlassgebundenes Instrument. In diesem Fall wäre der Spielraum für weitere Datenerhebungen und sonstige Sicherheitsinstrumente erheblich größer.

[1448] Die Vorratsdatenspeicherung darf ja gerade „nicht als Vorbild für die Schaffung weiterer vorsorglicher anlassloser Datensammlung dienen", BVerfGE 125, 260 (324); dazu schon ausführlich oben Kap. 7.2.1.

[1449] Hier ist ein reines Schock-Frosten der Telekommunikationsverkehrsdaten gemeint. Das heißt Telekommunikationsverkehrsdaten würden nicht generell auf Vorrat gehalten werden – auch keine IP-Daten -, sondern nur im Fall eines Verdachts auf Anordnung bis zur richterlichen Entscheidung vorgehalten werden.

Wenn jedoch auf europäischer Ebene an der Verpflichtung zur Vorratsspeicherung der Telekommunikationsverkehrsdaten festgehalten wird, bleibt allein die verfassungsrechtliche Pflicht der Bundesregierung, sich der Einführung einer vorsorglich anlasslosen Fluggastdatenspeicherung zu widersetzen.

7.4 Optimierung des Interessenausgleichs bei schweren Freiheitseingriffen

Im Angesicht dessen, dass sowohl der Gesetzgeber als auch die Polizeibehörden sich im Rahmen der Terrorbekämpfung vielfach in einer Grauzone des Rechtsstaats bewegen oder die Befugnisse bis zum Äußersten ausgereizt haben,[1450] ist es nicht verwunderlich, dass sich die Befürchtungen mehren, dass sich Deutschland zu einem Überwachungsstaat wandelt. Auch wenn dargelegt wurde, dass die Verfassung an sich eine umfassende gesamtgesellschaftliche Überwachung verbietet. Die Einführung der Vorratsdatenspeicherung und das Urteil des *Bundesverfassungsgerichts* machen jedoch deutlich: die Grenzen der Sicherheitsvorsorge sind nahezu erreicht.

Wenn erneut eine Vorratsdatenspeicherung eingeführt werden sollte, ist die gesamtgesellschaftliche Überwachungsdichte, sehr hoch. Das Verhältnis von Freiheit zu Sicherheit wie es das Grundgesetz verlangt, nämlich im Sinne einer Sicherheit für Freiheit, droht verkehrt zu werden. Verfassungsrechtliche Schranken weichen im Angesicht von Versicherheitlichungen, neuen technischen Möglichkeiten und der Überlagerung durch europäisches Recht immer stärker auf. Dem Abdriften in einen Überwachungsstaat steht das Verbot einer umfassenden gesamtgesellschaftlichen Überwachung entgegen. Die Frage, ob sich die Bundesrepublik zu einem Überwachungsstaat wandelt, kann von Verfassung wegen mit einem Nein beantwortet werden.[1451] Verneint werden kann sie jedoch nur soweit die vom *Bundesverfassungsgericht* erklärte absolute Grenze nicht einem Leerlauf überlassen wird, sondern durch Konkretisierung und Operationalisierung Wirkungskraft entfaltet, nämlich indem beobachtet, geprüft und entsprechendes Handeln auch kontrolliert wird.

Vor dem Hintergrund, dass Freiheit und Sicherheit eng miteinander verquickt sind, das Spannungsverhältnis aber durch Informatisierung und die Bedrohung durch den Terror verschärft ist, gilt es „aktiv und offensiv" für die Verwirklichung der Grundrechte „in einer auf Prävention und Sicherheit ausgerichteten Gesellschaft" zu werben.[1452] Grundsätzlich ist es die Aufgabe des Gesetzgebers einen Ausgleich von Freiheits- und Sicherheitsinteressen zu erzielen. Die Verfassung gibt ihm beides auf: „die Herstellung einer Balance, die im Wechsel der politischen Lagen möglichste Freiheit in möglichster Sicherheit gewährleistet". [1453] Wie er diese Balance schafft ist an sich und soweit er sich innerhalb der verfassungsrechtlichen Schranken bewegt, der gesetzgebenden Gewalt überlassen – sie muss jedoch dafür Sorge tragen, dass sich keine umfassende gesamtgesellschaftliche Überwachung realisiert.

[1450] So für den Bereich der Telekommunikationsüberwachung *Petri*, RDV 2003, 16, 22.
[1451] Vgl. auch *Papier*, DVBl. 2010, 801, 807.
[1452] *Hassemer*, vorgänge 2002, (Nr. 159), 10, 13; Er sieht als mögliche Gegenmittel 1. Sozialpolitik 2. Beschränkung des Strafrechts auf ihre tatsächlichen Möglichkeiten und 3. andere Rechtsgebiete für Sicherheitspolitik fruchtbar zu machen.
[1453] *Horn* 2003, 449.

Gerade in Anbetracht dieser Tatsache ist für eine Rationalisierung in der Sicherheitspolitik und eine Optimierung des Interessenausgleichs im Rahmen sicherheitspolitischer Entscheidungen zu werben. Entscheidungen des Gesetzgebers sollten sich nicht nur daran orientieren, ob eine Maßnahme gerade noch verfassungskonform gestaltet werden kann, sondern ob sie auch verfassungsverträglich ist. Letztlich also ob die Maßnahme so gestaltet werden kann, dass alle betroffenen Interessen in ein ausgewogenes Gleichgewicht gesetzt werden können, das den grundsätzlichen Gewichtungen in der Verfassung entspricht.

Dies gilt im Besonderen für Datenerhebungen und -speicherungen unter dem Gesichtspunkt, dass die Digitalisierung und Informatisierung des Alltagslebens weiter schnell voran schreitet, und nicht absehbar ist, wann ein Instrument, dass sich heute an der Grenze zur Verfassungswidrigkeit bewegt, diese Grenze auf Grund veränderter gesellschaftlicher Rahmenbedingungen überschreiten. Deutlich wird dies schon mit Blick auf die Enthüllungen über das NSA-Programm PRISM: wenn tatsächlich durch die USA eine umfassende Vorratsdatenspeicherung auch der Inhalte der Telekommunikation aller Bundesbürger erfolgt und die nationalen Sicherheitsbehörden zudem die Möglichkeit haben auf diese Daten zuzugreifen, ist die Frage nach dem Grad gesamtgesellschaftlicher Überwachung in einem neuen Licht zu sehen.

Fest steht, dass verfassungsrechtlich legitim nie das Ziel absoluter Sicherheit sein kann. Insofern sind auch die Ausweitung sicherheitspolitischer Instrumente und die Schaffung neuer Eingriffsbefugnisse mit Recht kritisch zu hinterfragen. Der Gesetzgeber sollte die Interessen der von Polizeien und Innenministerien nicht priorisieren, sondern rational besonnen das Ziel verfolgen, einen optimierten Interessenausgleichs im Spannungsverhältnis von Freiheit und Sicherheit zu schaffen. Ein solches Vorgehen kann auch breite Akzeptanz für sicherheitspolitische Entscheidungen erzielen.

Teil 3: Interessenausgleich im Rahmen der Vorratsdatenspeicherung

Bei einer Vorratsspeicherung der Telekommunikationsverkehrsdaten handelt es sich um eine neue Dimension der Überwachung der Bevölkerung. Es wird eine gesamtgesellschaftliche Überwachungsinfrastruktur geschaffen, indem flächendeckend und anlasslos eine für die Informationsgesellschaft zentrale Infrastruktur auf den Ausnahmefall ausgerichtet wird. Ein solches Instrument darf nur in engen Grenzen eingeführt werden.[1454] Eine Vorratsdatenspeicherung kann mit der Verfassung in Einklang gebracht werden, ihr muss aber als flächendeckende, verdachtsunabhängiges Überwachungsinfrastruktur Ausnahmecharakter zu kommen. Die Sicherheitsgesetzgebung darf sich insgesamt nicht an diesem Vorbild ausrichten und für den Ausnahmefall vorsorgen.[1455]

Die Einführung der Vorratsdatenspeicherung ist vielfach diskutiert und hoch umstritten.[1456] Nunmehr soll der Frage nachgegangen werden, ob und wie eine Vorratsdatenspeicherung nicht nur innerhalb der Grenzen zur Verfassung, in diesem Sinne gerade noch verhältnismäßig gestaltet werden kann, sondern ob und wie verfassungsverträglich ein Ausgleich zwischen Freiheits- und Sicherheitsinteressen im Rahmen einer Vorratsdatenspeicherung erzielt werden kann. Dabei liegt im Fokus der Untersuchung nicht eine Befassung mit der Frage, ob die Richtlinie überhaupt mit den Garantien der Europäischen Grundrechtecharta vereinbar ist − der Frage, welche derzeit den Europäischen Gerichtshof beschäftigt. Denn die hier vorzunehmende Untersuchung, wie eine Speicherung sämtlicher Telekommunikationsverkehrsdaten auf Vorrat so ausgestaltet werden kann, dass die durch das Grundgesetz garantierten Werten Freiheit und Sicherheit möglichst schonend in Ausgleich gebracht werden, ist selbst dann von Relevanz, sollte die Richtlinie für unionsrechtswidrig erklärt werden. Es sei denn, der Gerichtshof käme zu der Feststellung, dass eine Speicherung von Telekommunikationsverkehrsdaten für einen bestimmten Zeitraum zur Verhinderung und Verfolgung von Straftaten, generell gegen die Europäischen Grundrechtsgarantien verstößt.

Von großem Interesse ist die Untersuchung darüber hinaus, da die Frage wie ein optimierter Ausgleich erzielt werden kann, sich nicht nur in Bezug auf eine Vorratsspeicherung der Telekommunikationsverkehrsdaten stellt, sondern auch bei Einführung anderer sicherheitspolitischer Instrumente. Sie gilt es nicht nur im Sinne einer möglichst großen Akzeptanz zu ermitteln, sondern auch weil der aktuell verbleibende

---

[1454] Vgl. ausführlich oben Kap. 6.3, S. 227 ff.

[1455] BVerfGE 125, 260 (323 f.); *Roßnagel* 2003, 17 ff.; das dem so ist wird ausführlich in Kap. 7.2.1 dargelegt und begründet.

[1456] Die Entwicklungsgeschichte und das im Urteil des *BVerfG* zur Vorratsdatenspeicherung zentrale Judikat in welchem das Gericht die Verfassungswidrigkeit einer umfassenden gesamtgesellschaftlichen Überwachung formuliert hat, wurde im vorangegangenen Abschnitt aufgezeigt, Kap. 4.

Spielraum, auf Grund der in den letzten Jahren konstant zu verzeichnenden Tendenz hin zu einem immer mehr an Sicherheit,[1457] zunehmend kleiner wird.

Anhand der Vorratsdatenspeicherung, zu deren Einführung der Gesetzgeber europarechtlich verpflichtet ist, soll der Frage nachgegangen werden, wie hier ein optimierter Interessenausgleich erzielt werden könnte. Dafür muss zunächst untersucht werden, wie methodisch ein optimierter Interessenausgleich entwickelt werden kann (Kap. 8). Der zu entwickelnde methodische Ansatz, soll dann auf die Vorratsdatenspeicherung angewendet werden, um zu untersuchen, ob und wie im Rahmen einer Vorratsdatenspeicherung ein optimierter Interessenausgleich erzielt werden kann (Kap. 9). Hier sollen dann konkrete Gestaltungsvorschläge, die in Anbetracht der aktuell gebotenen Umsetzungspflicht und der ausstehenden Überarbeitung der Richtlinie geboten sind, entwickelt werden (Kap. 10). Abschließend soll dann unter Bezugnahme auf die gewonnen Erkenntnisse dazu Stellung genommen, wie ein praktisch konkordanter Interessenausgleich im Angesicht von Informatisierung, Digitalisierung und dem gesteigerten Gefühl der Verwundbarkeit erreicht werden kann (Kap. 11).

[1457] Vgl. oben Kap. 1.4, S. 50 f.

8 Methode: Verhältnismäßigkeitsprüfung Plus

Um einen optimierten Interessenausgleich zu erzeugen, könnte die anerkannte Verhältnismäßigkeitsprüfung erweitert werden, um die Schwachstellen auszugleichen, die sie (aufgrund von Informatisierung, der schwerwiegenden Bedrohung durch terroristische Angreifer und die Überlagerung durch supranationales Recht) aufweist.[1458] Dafür ist sie nicht nur um die doppelte Verhältnismäßigkeitsprüfung zu ergänzen, die es im Rahmen der Überwachungs-Gesamtrechnung durchzuführen gilt.[1459] Sie muss darüber hinaus so ausgestaltet werden, dass sie es vermag, Freiheits- und Sicherheitsinteressen in einen optimierten Ausgleich zu bringen und zwar optimiert im Hinblick auf ihre Verfassungsverträglichkeit.[1460] Ziel ist es also, durch die Entwicklung von Gestaltungsvorschlägen einen bestmöglichen Ausgleich im Rahmen der Vorratsdatenspeicherung zu entwickeln.

Maßgeblich dafür ist das Verhältnis von Freiheit und Sicherheit, wie es im Grundgesetz angelegt ist.[1461] Priorität hat insoweit nicht das Ziel einer vermeintlich absoluten Sicherheit. Die Verfassung gibt vielmehr vor, ein möglichst hohes Maß an Sicherheit zu verfolgen, um damit ein möglichst hohes Maß an Freiheit zu gewähren. Sicherheitsmaßnahmen müssen immer freiheitssichernde Maßnahmen sein.[1462] Dieser Gedanke sollte in die Verhältnismäßigkeitsprüfung einfließen. Indem diese Perspektive die jeweiligen Prüfungspunkte der Verhältnismäßigkeitsprüfung mitbestimmt, kann sie so im Sinne einer „Verhältnismäßigkeitsprüfung Plus" dazu dienen, einen optimierten Ausgleich von Freiheits- und Sicherheitsinteressen zu ermitteln.

Dieser Ansatz ermöglicht es dem Gesetzgeber, Gestaltungsmöglichkeiten zu ermitteln und Gesetzgebungsvorhaben losgelöst von politischen und emotionalisierten Debatten dahingehend zu prüfen, wie ein Sicherheitsinstrument so gestaltet werden kann, dass dabei möglichst alle betroffenen Interessen berücksichtigt werden. Eine solche Prüfung ist auf Grund des sich im Vordringen befindenden Sicherheitsstrebens dringend geboten: Freiheit und Sicherheit setzen sich gegenseitig und keines darf zu Lasten des

[1458] Dazu ausführlich oben Kap. 6.2.3, S. 224 f.; *Hornung* möchte die Schwachstellen der Verhältnismäßigkeitsprüfung ausgleichen indem er die Argumente, die auf den ersten beiden Stufen nicht greifen, sondern diese zum Leerlauf bringen, für die Abwägung im Rahmen der Zumutbarkeit fruchtbar machen. Im Rahmen der objektiven Zumutbarkeit müsste, wenn Alternativen, wie das Quick-Freeze-Verfahren bereit stünden nicht sämtliche positive „Effekte der zu prüfenden schwerwiegenderen Maßnahme abgewogen werden, sondern nur das Mehr an Effekten, das sie im Vergleich zu der milderen Maßnahme mit sich bringt", *Hornung,* PVS 2012, 377, 394. Dieser Ansatz ist durchaus vielversprechend. Da hier jedoch nicht nur gefragt wird, wie die Schwachstellen der Verhältnismäßigkeitsprüfung ausgeglichen werden können, sondern wie insgesamt und nach Integration der Überwachungs-Gesamtrechnung ein möglichst verfassungsverträglicher Interessenausgleich entwickelt werden kann, soll hier ein anderer methodischer Ansatz verfolgt werden.

[1459] Dazu ausführlich oben Kap. 7.3.

[1460] Vgl. zum Merkmal Verfassungsverträglichkeit, *Roßnagel* 1989, 181 f.

[1461] Vgl. dazu schon ausführlich oben Kap. 3.

[1462] Vgl. oben S. 121 ff., 130 ff.

A. Moser-Knierim, *Vorratsdatenspeicherung,* DuD-Fachbeiträge,
DOI 10.1007/978-3-658-04156-4_8, © Springer Fachmedien Wiesbaden 2014

anderen gänzlich zurückgestellt werden. Ein solcher Ansatz kann auch die Akzeptanz von sicherheitspolitischen Entscheidungen verbessern.

Die Verhältnismäßigkeitsprüfung[1463] eignet sich als Anknüpfungspunkt für die Entwicklung eines methodischen Ansatzes zur Verbesserung des Interessensausgleichs, da mit ihr bereits geprüft wird, ob ein Eingriff in ein Grundrecht verfassungskonform ist. Die Verhältnismäßigkeitsprüfung muss insofern dahingehend erweitert werden, dass sie es ermöglicht, nicht nur die Verfassungskonformität zu messen sondern die Verfassungsverträglichkeit.[1464]

Verfassungsverträglich ist nicht gleich verfassungskonform. Verfassungskonform sind auch die zahlreichen Maßnahmen, die das Gleichgewicht von Freiheit und Sicherheit insgesamt zu erschüttern drohen. Verfassungskonform bedeutet lediglich, dass eine Regelung aktuell nicht gegen die Verfassung verstößt. Verfassungsverträglichkeit verlangt darüber hinaus, dass das Instrument nicht nur gerade noch mit den verfassungsrechtlichen Vorgaben übereinstimmt, sondern ein im Sinne der Verfassung bestmöglicher Interessenausgleich erzielt wird. Es geht insofern nicht darum lediglich zu prüfen, ob Unter- oder Übermaßverbot verletzt wurde, sondern darum eine Kohärenz im Sinne eines praktisch konkordanten Ausgleichs herzustellen.[1465] Es sollen auf diese Weise Lösungen gefunden werden, die einen praktisch konkordanten Interessenausgleich ermöglichen und die, gerade auch im Hinblick auf kommende Entwicklungen, dem Gesetzgeber einen Spielraum belassen.

Insofern knüpft dieser methodische Ansatz an die Erwägungen Teil 1 an und versucht eine Antwort auf die neuen Herausforderungen für die Gewährleistung von Freiheit und Sicherheit im digitalen Zeitalter zu liefern. Dabei sind die in Teil 2 gewonnenen Erkenntnisse über das Verbot einer umfassenden gesamtgesellschaftlichen Überwachung miteinzubeziehen.

Die Prüfungsmaßstäbe der klassischen Verhältnismäßigkeitsprüfung sind anzupassen: Instrumente, die der Gewährleistung von Sicherheit dienen, verfolgen stets auch einen legitimen Zweck.[1466] Ob dies tatsächlich der Fall ist und wie hoch der Beitrag zu mehr Sicherheit ist, erfolgt nicht im Rahmen der Prüfung des legitimen Zwecks, sondern kann durch eine ausgedehnte Prüfung der Geeignetheit und Erforderlichkeit beantwortet werden.

Im Rahmen der Geeignetheit sollte daher nicht nur gefragt werden, ob die Maßnahme geeignet ist, die Zweckerreichung zu fördern,[1467] sondern ob sie tatsächlichen einen Beitrag zur Zweckerreichung leistet. Es sollte also nicht nur gefragt werden, ob theore-

---

[1463] Ausführlich zur verfassungsrechtlichen Grundlage und dem Ablauf dem anerkannten Prüfungsumfang der Verhältnismäßigkeitsprüfung, schon ausführlich oben Kap. 2.1.4.2.2.

[1464] Zum Kriterium der Verfassungsverträglichkeit *Roßnagel* 1984; *Ders.* 1990.

[1465] Das dieses Ziel auch einen praktisch konkordanten Ausgleich zu ermöglichen, auch für die Auflösung von Kollisionen zwischen Freiheits- und Sicherheitsinteressen gilt, dazu oben Kap. 3.4, S. 132.

[1466] Vgl. dazu schon oben Kap. 2.2.4; Kap. 6.2.2.

[1467] Wie es das *BVerfG* prüft, BVerfGE 63, 88 (115); 67, 157 (175); 96, 10 (23); 103, 293 (307). 125, 260 (318).

tisch und abstrakt ein Kausalzusammenhang zwischen der Maßnahme und dem Zweck denkbar ist.[1468] Im Zentrum der Prüfung der Geeignetheit sollte, mit dem Ziel einen praktisch-konkordaten Ausgleich zwischen Freiheits- und Sicherheitsinteressen[1469] zu erzielen, die Frage stehen, ob die Maßnahme tatsächlich dem gesetzten Zweck dient. Geprüft werden sollte also, ob nicht auf die Maßnahme verzichtet werden kann, ohne dass die Erreichbarkeit des Ziels schwerwiegend beeinträchtigt wird. So würde nicht nur aus einer Ex-ante-Betrachtung auf eine abstrakte Eignung abgestellt werden, sondern es könnte überprüft werden, ob eine Maßnahme tatsächlich einen Beitrag zu einem mehr an Sicherheit leistet. Um diese Prüfung durchzuführen, sind Evaluationen notwendig, wie hoch der Beitrag zur Sicherheit ist. Benötigt werden empirische Untersuchungen. Statistisch muss etwa erhoben werden, wie oft eine bestimmte Überwachungsmaßnahme eingesetzt wird und welche Rolle die gewonnen Daten im Gerichtsverfahren gespielt haben. Es ist nicht nach der abstrakten Geeignetheit, sondern nach der praktischen (tatsächlichen) Verzichtbarkeit zu fragen.

Im Rahmen der Prüfung der Erforderlichkeit, sollten im Rahmen der Frage, ob es ein gleich geeignetes, weniger einschneidendes Mittel gibt, die Anforderungen an die „gleiche Eignung“ relativiert werden. Denn bei Datenerhebungen und -verarbeitungen zu Sicherheitszwecken ist es logisch bedingt so, dass umso umfassender eine Maßnahme ist, desto niedriger die Wahrscheinlichkeit ist, ein genau gleich geeignetes Äquivalent zu finden.[1470] Es sollte daher nicht gefragt werden, ob es eine genau gleich geeignete Maßnahme gibt, sondern ob es eine adäquate Maßnahme gibt, die grundrechtsschonender das gleiche Ziel verfolgt und einen annähernd hohen Beitrag zum verfolgten Zweck leistet. Insofern wird die Alternativlosigkeit untersucht.

Schließlich müsste auch die Verhältnismäßigkeitsprüfung im engeren Sinne erweitert werden. Es wurde im ersten Abschnitt aufgezeigt, dass sich Freiheit und Sicherheit gegenseitig bedingen und es das Ziel sein sollte, gerade auch bei der Kollision von Freiheits- und Sicherheitsinteressen nicht einseitige Lösungen zu präferieren, sondern einen bestmöglichen, quasi praktisch-konkordaten, Ausgleich zu finden. Dabei kann abgewogen werden, wie hoch der Beitrag einer Maßnahme zur Freiheitssicherung auf der einen Seite ist, gegen die dadurch bedingten Beeinträchtigungen der individuellen und der kollektiven Freiheit auf der anderen Seite. Eine solche Freiheits- und Sicherheitsfolgenabschätzung wird aber nur dann methodisch anerkannt, wenn damit nicht eine pauschale Wertung erfolgt, sondern dezidiert und nachvollziehbar abgewogen wird. Erforderlich ist es dafür, alle von einem sicherheitspolitischen Instrument betroffenen Freiheitsrechte zu ermitteln und sie im Hinblick darauf zu untersuchen, in welcher Form und wie stark in sie eingegriffen wird, und dies mit ihrer Bedeutung für die Erzeugung von Sicherheit abzuwiegen.

[1468] Schließlich sind kaum Datenerhebungs- und -verarbeitungsmaßnahmen denkbar, die keinen Beitrag zu mehr Sicherheit leisten könnten. Insofern verliert die Geeignetheitsprüfung in ihrer klassischen Gestalt bei datenverarbeitenden Maßnahmen ihre freiheitsschützende Funktion. Zur strukturellen Schwäche der Prüfung der Geeignetheit, vgl. oben Kap. 6.2.2.

[1469] Vgl. dazu oben Kap. 3.4.

[1470] Vgl. dazu schon ausführlich oben 6.2.2.

Die Konkretisierung von Freiheits- und Sicherheitsinteressen in verschiedenen verfassungsmäßig garantierten Rechten und die jeweilige Bewertung des Eingriffsgewichts bzw. des Beitrags zur Steigerung der Sicherheit ermöglicht es, die erforderliche Abwägung nachvollziehbar zu gestalten. Sodann können aus einer derartigen Gegenüberstellung in einer umfassenden Gesamtbetrachtung, Gestaltungsvorschläge für einen optimierten Interessenausgleich ermittelt werden.

Einen besonderen Stellenwert erhält eine solche Abwägung bei der verfassungsrechtlichen Überprüfung von Sicherheitsinstrumenten, die die Identität der Verfassung berühren können. Wenn durch Sicherheitsmaßnahmen die gesamtgesellschaftliche Überwachung zwar gesteigert wird, dabei aber eine verfassungswidrige umfassende gesamtgesellschaftliche Erfassung und Registrierung droht, muss, um dieses Ergebnis zu verhindern, gefragt werden, wie ein optimierter Interessenausgleich erzielt werden kann.

Die Auflösung von Kollisionsfällen obliegt an sich dem Gesetzgeber.[1471] Für eine verfassungskonforme Regelung genügt eine verhältnismäßige Ausgestaltung der jeweiligen sicherheitsrechtlichen Instrumente.[1472] Diese ermöglicht aber keine Bewertung und Begrenzung von sicherheitsrechtlichen Instrumenten über den Einzelfall hinaus, um die Identität der Verfassung zu schützen. Doch die Identität der Verfassung beschränkt das gesetzgeberische Ermessen. Sie verbietet eine umfassende gesamtgesellschaftliche Überwachung.[1473] Eine schrittweise Erweiterung der Sicherheitsmaßnahmen, welche Sicherheit verabsolutiert, ist nicht nur verfassungsschädlich, sondern verfassungswidrig. Die grundsätzliche verfassungsrechtliche Gewichtung „Sicherheit für Freiheit" darf nicht in ihr Gegenteil verkehrt werden. Letztlich muss damit auch das *Bundesverfassungsgericht* prüfen, soweit es um die Ausdehnung von Sicherheitsinstrumenten geht (und es in einer doppelten Verhältnismäßigkeitsprüfung den Grad gesamtgesellschaftlicher Überwachung ermittelt), ob nicht ein optimierter Interessenausgleich erzielt werden kann. Die Verhältnismäßigkeitsprüfung Plus ist also nicht allein ein Instrument, mit dem der Gesetzgeber mit dem Ziel verfassungsverträgliche, also interessengerechte und praktisch-konkordante Lösungen finden kann – und so letztlich auch die Akzeptanz neuer Sicherheitsmaßnahmen steigern kann. Sie ist auch Prüfungsmaßstab für das *Bundesverfassungsgericht,* wenn eine Verletzung der Identität der Verfassung durch eine schleichende Ausweitung von Sicherheitsinstrument hin zu einer verfassungswidrigen umfassenden gesamtgesellschaftlichen Überwachung zur Sorge steht.

Dem Gesetzgeber ermöglicht die Erweiterung der Verhältnismäßigkeitsprüfung bei Erlass eines neuen Sicherheitsgesetzes und dem *Bundesverfassungsgericht* bei der Überprüfung dieses Gesetzes, die Überprüfung im Hinblick auf die Verfassungsverträglichkeit. Dies ist besonders wichtig, da der Gesetzgeber gerade im sensitiven Bereich der Grundrechte und im Interesse einer Akzeptanz und der zukünftigen Verfassungsver-

[1471] Siehe hierzu oben Kap. 3, insbes. S. 135 f.
[1472] Zur schrittweisen Ausdehnung immer neuer Sicherheitsinstrumente in einer Art „Salami-Taktik", vgl. oben Kap. 1.4.2.
[1473] Vgl. dazu Kap. 7.1.

träglichkeit dieser, grundsätzlich nach einem optimierten Ausgleich zwischen Freiheits- und Sicherheitsinteressen suchen sollte.

Mit diesem methodischen Ansatz, soll ein Beitrag geleistet werden zu der großen Herausforderung, die sich unserer Gesellschaft zu Beginn des 21. Jahrhunderts stellt, nämlich wie praktische Konkordanz „zwischen dem Bedürfnis nach kollektiver Sicherheit und der Wahrung individueller Freiheit“ erreicht werden kann.[1474]

[1474] *Zöller* 2003, 291, 318.

9 Verfassungsrechtliche Analyse der Vorratsdatenspeicherung

Im Folgenden wird anhand der Vorratsdatenspeicherung, die paradigmatisch für das Verhältnis von Freiheit und Sicherheit steht,[1475] untersucht, wie ein optimierter Interessensausgleich erzielt werden kann.[1476] Methodisch erfolgt die Entwicklung von Gestaltungsvorschlägen für einen optimierten Interessenausgleich unter Rückgriff auf den entwickelten Ansatz einer „Verhältnismäßigkeitsprüfung Plus".

Wichtig ist es für die Entwicklung optimierter Gestaltungsvorschläge, dass sämtliche verfassungsrechtlich geschützten Rechtspositionen berücksichtigt werden. Der Konflikt zwischen Schutzpflichten des Staates und Abwehrrechten der Bürger, wie sie überwiegend die rechtswissenschaftliche Diskussion um die Vorratsdatenspeicherung geprägt haben, kann lediglich als eine erste von der Vorratsdatenspeicherung betroffene Dimension bezeichnet werden (*1. Dimension: Staat – Bürger*; Kap. 9.1). Die Vorratsdatenspeicherung greift auch in die Wirtschaft intensiv ein. Aufgrund der Liberalisierung des Telekommunikationsmarkts sind Strafverfolgungs- und Gefahrenabwehrbehörden auf die Mitwirkung der privaten Telekommunikationsdienste-anbieter bei der Durchführung von Telekommunikationsüberwachungsmaßnahmen angewiesen. Auch die Vorratsdatenspeicherung muss notwendig durch die privaten Telekommunikationsunternehmen durchgeführt werden, da ausschließlich bei diesen die Kommunikationsdaten anfallen. Dies kollidiert jedoch mit den privaten Interessen der Provider. *(2. Dimension: Staat – Wirtschaft;* Kap. 9.2). Auch zwischen Staaten (Bundesstaat – Länder; EU – Mitgliedstaat; EU-Mitgliedsstaaten – Drittstaaten) wirkt sich die Interessenkollision aus (*3. Dimension: Staat – Staat;* Kap. 9.3). Hier treffen das Interesse an einer bestmöglichen Kooperation und der Grundsatz informationeller Gewaltenteilung aufeinander – und das sowohl auf nationaler als auch auf supranationaler Ebene.

In jeder Dimension werden im Folgenden zunächst die rechtlichen Anforderungen identifiziert. Dazu werden die verfassungsrechtlichen Vorgaben beschrieben, die Chancen und Risiken einer Vorratsdatenspeicherung für diese verfassungsrechtlich geschützten Rechtspositionen erörtert und daraus die Anforderungen abgeleitet, die bei der Ausgestaltung einer Vorratsdatenspeicherung zu beachten sind. Soweit in Grundrechte eingegriffen wird, wird zum einen im Sinne der klassischen Verhältnismäßigkeitsprüfung gefragt, ob der Eingriff geeignet und erforderlich ist und sodann, ob er denn auch im Sinne einer Verhältnismäßigkeit Plus unverzichtbar und alternativlos ist. Sodann werden die Anforderungen an eine möglichst verfassungsverträgliche Ausgestaltung ermittelt.

[1475] Warum die Vorratsdatenspeicherung paradigmatisch für das Kollisionsverhältnis von Freiheit und Sicherheit im digitalen Zeitalter ist, wird in Kap. 1.5 erörtert.

[1476] Der folgende Abschnitt beruht im Wesentlichen auf den im Rahmen des Forschungsprojekts INVODAS entwickelten Erkenntnissen, welche bereits in *Roßnagel/Moser-Knierim/Schweda,* 2013, S. 89 ff. veröffentlicht wurden. Etwaige Doppelungen im Text beruhen darauf, dass die Erstellung der Dissertation im Zuge der Mitarbeit im Forschungsprojekt erfolgte. Sie reicht in Teilen über den Forschungsbericht hinaus und ergänzt diesen in anderen Punkten, in denen eine umfassendere Darstellung der Forschungsergebnisse erfolgt.

A. Moser-Knierim, *Vorratsdatenspeicherung,* DuD-Fachbeiträge,
DOI 10.1007/978-3-658-04156-4_9, © Springer Fachmedien Wiesbaden 2014

Die dimensionsorientierte Analyse der Vorratsdatenspeicherung soll die, bislang überwiegend auf das Verhältnis *Staat − Bürger* fokussierte Diskussion, um die anderen betroffenen Interessen erweitern und so die Basis schaffen, um Gestaltungsvorschläge zu entwickeln in denen sich sämtliche verfassungsrechtlich begründete Interessen widerspiegeln.

Aufbauend auf dieser Analyse werden die ermittelten Elemente dahingehend untersucht, ob und wie sie so ausgestaltet werden können, dass sie zu einem optimierten Interessenausgleich führen, weil alle betroffenen Interessen entsprechend ihres Gewichts zum Ausdruck kommen (Kap. 10).

9.1 *Staat − Bürger*

Der Widerstreit von Freiheits- und Sicherheitsinteressen als Spannungsverhältnis von staatlichen und bürgerlichen Freiheitsinteressen prägt überwiegend die Diskussion um die Vorratsdatenspeicherung und steht so auch im Zentrum der Entscheidung des *Bundesverfassungsgerichts*.[1477] Auf der einen Seite liegt die Pflicht und das Interesse des Staates seine Bürger zu schützen, auf der anderen das Interesse der Bürger, frei und unbeobachtet zu kommunizieren.

9.1.1 Pflicht zur Gewährleistung von Sicherheit

Das staatliche Sicherheitsinteresse entspricht sich weitgehend in allen drei von der Vorratsdatenspeicherung betroffenen Dimensionen. Lediglich im Hinblick auf einzelne Bewertungskriterien unterscheidet sich das in den jeweiligen Dimensionen zum Ausdruck kommende Interesse. Aus diesem Grund erfolgt hier vorab in der Dimension Staat – Bürger eine umfassende Darstellung des staatlichen Sicherheitsinteresses und die Bedeutung der Vorratsdatenspeicherung für dieses. Bei der Analyse der anderen Dimensionen wird dann darauf verwiesen und die Analyse lediglich um spezifische in der jeweiligen Dimension zu berücksichtigende Interessen ergänzt.

9.1.1.1 Sicherheit als originär staatliche Aufgabe und legitimer Eingriffszweck

Der Staat ist „Beschützer der Bürger“.[1478] Es gibt zwar kein Grundrecht auf Sicherheit,[1479] der Staat ist aber verpflichtet Sicherheit zu gewährleisten.[1480] Das Staatsziel Sicherheit ist unbestritten, allein die Begründungen unterscheiden sich.

Die staatliche Verpflichtung, Sicherheit zu gewähren, wird begründet durch Gewaltmonopol und Rechtsstaatsprinzip – denn diese verpflichten den Staat dazu, dafür Sorge zu tragen, dass der Einzelne keiner willkürlichen Gewaltanwendung ausgesetzt ist.[1481] Die Pflicht zur Gewährleistung von Sicherheit ist auch Kehrseite des Gewaltmonopols und erwächst insofern aus der Schutzpflichtendimension der Grundrech-

[1477] BVerfGE 125, 260.
[1478] Vgl. oben 2.2.7; inwiefern und aus welchen Gründen der Staat zur Gewährleistung von Sicherheit verpflichtet ist, wurde bereits umfassend in Kap. 2.2 erörtert.
[1479] Vgl. oben Kap. 2.2.3, S. 115 ff.
[1480] Vgl. oben Kap. 2.2, S. 109 ff.
[1481] Vgl. dazu ausführlich oben Kap. 2.2.1.

te.[1482] Insofern werden die Grundrechte in ihrer Funktion als Schutzpflichten begriffen und bilden zusammen die Grundlage des Staatsziels der inneren Sicherheit.[1483]

Anerkannt ist in ständiger Rechtsprechung des *Bundesverfassungsgerichts*, dass die „zu gewährleistende Sicherheit der Bevölkerung vor Gefahren für Leib, Leben und Freiheit Verfassungswerte" sind, „die mit anderen hochwertigen Gütern im gleichen Rang stehen".[1484] Das Gericht betont auch, dass die „Schutzgüter der öffentlichen Sicherheit und Ordnung hohes verfassungsrechtliches Gewicht haben. Kernaufgabe der Gewährleistung innerer Sicherheit ist die Bekämpfung von Kriminalität.[1485]

Das Bestehen der Staatsaufgabe Sicherheit wird schließlich auch durch die im Grundgesetz angelegte Sicherheitsarchitektur geprägt und bestimmt.[1486] Unstrittig ist jedenfalls, dass es sich beim Ziel, Sicherheit zu erzeugen, um ein legitimes Ziel handelt, das auch grundsätzlich geeignet ist, den damit verbundenen Eingriff in Grundrechte zu rechtfertigen.[1487] Allerdings verlangt die Verfassung nicht die Gewährleistung einer hundertprozentigen Sicherheit.[1488] Absolute Sicherheit ist nicht realisierbar.[1489]

So wie national das Grundgesetz den Staat zur Gewährleistung von Sicherheit verpflichtet, kann auch aus den Europäischen Grundrechten der Europäischen Menschenrechtskonvention und der Europäischen Grundrechtecharta eine solche hergeleitet werden. Auch hier sind Schutzpflichten anerkannt.[1490]

Die Analyse der verfassungsrechtlichen Grundlagen der unstrittig vorhandenen staatlichen Pflicht zur Gewährleistung von Sicherheit zeigt deutlich, dass zwischen dieser und den Freiheitsrechten der Bürger ein enger Kontext besteht: Sicherheit ist keine Staatsaufgabe als bloßer Selbstzweck, sondern sie zielt darauf, es dem Einzelnen zu ermöglichen, seine ihm durch die Verfassung zugesicherten Freiheiten auszuüben.[1491]

9.1.1.2 Anforderungen an eine Vorratsdatenspeicherung aus Perspektive der Sicherheitsbehörden

Im Hinblick darauf, dass die Vorratsdatenspeicherung als besonders wichtiges Instrument zur Gewährleistung von Sicherheit im digitalen Zeitalter propagiert wird,[1492] soll im Folgenden dargelegt werden, wie nach Ansicht der Ermittlungsbehörden eine Vorratsdatenspeicherung einen möglichst hohen Beitrag zu mehr Sicherheit leisten kann. Es werden die einzelnen Anforderungen dargestellt, die die Ermittlungsbehörden an Datenspeicherung und -verwendung formuliert haben. Die Darstellung basiert im We-

[1482] So auch anerkannt in stRspr des BVerfG, dazu oben Kap. 2.2, S. 113 ff.
[1483] Vgl. dazu ausführlich oben Kap. 2.2.2.
[1484] BVerfGE 120, 274 (319) mit Bezugnahme auf BVerfGE 49, 24 (56 f.); 115, 320 (346); Vgl. dazu ausführlich oben Kap. 2.2.4.
[1485] *Götz,* in: *Isensee*/*Kirchof*, HStR IV 2006, § 85 Rn. 5.
[1486] Vgl. dazu ausführlich oben Kap. 2.2.5.
[1487] Vgl. dazu schon oben Kap. 2.2.7; Kap. 3.2.
[1488] Vgl. dazu oben S. 118; sowie Fn. 727, 776.
[1489] Vgl. oben S. 116.
[1490] Vgl. dazu ausführlich oben Kap. 2.2.2.
[1491] Dies wird dargelegt, oben in S. 121 ff., 130ff.
[1492] Vgl. dazu oben Kap. 4.4.2, S. 186 ff.

sentlichen auf Interviews mit Praktikern, die im Rahmen einer Studie des Max-Planck-Instituts geführt wurden.[1493]

- Umfang der Datenspeicherung

Ermittler betonen die Bedeutung der Vorratsdatenspeicherung für den gesamten Bereich der Internetkriminalität. Es fehle ohne den Zugriff auf retrograde Daten in diesem Bereich an jeglichem Ermittlungsansatz. Auch werden Nachbesserungen gegenüber der alten Regelung gefordert. Es solle sichergestellt werden, dass auch bei IP-Sharing die Nachverfolgbarkeit gewährleistet sei. Gefordert wird dafür eine Regelung zur Speicherung der Ports. Dies müsse auch für das mobile Internet gelten. Darüber hinaus sei es erforderlich, dass die dynamische IP-Adresse in Verbindung mit der Anschlusskennung als Bestandsdatum qualifiziert wird und diese Daten ebenfalls von der Speicherungspflicht erfasst werden.[1494]

- Speicherdauer

Überwiegend wird eine Speicherdauer von sechs Monaten, wie sie auch das *Bundesverfassungsgericht* als Obergrenze einer zulässigen Speicherung erachtet hat, von den befragten Ermittlern als sachgerecht und ausreichend bewertet. Sie wird allerdings als absolute Untergrenze erachtet. Wünschenswert sei eine längere Speicherfrist vor allem im Bereich der Bekämpfung organisierter Kriminalität und im Bereich des Staatsschutzes, da hier die Daten der Aufdeckung von Täterstrukturen und Beziehungsgeflechten dienten und dafür die Möglichkeit sehr wichtig sei, auch weit zurückliegende Verbindungsstrukturen zu analysieren. Lediglich für den präventiven Aufgabenbereich werden kürzere Speicher- oder Zugriffsfristen als vertretbar bezeichnet.[1495] Auch die befragten Staatsanwälte erachteten sechs Monate als sachgerecht, drei Monate seien hingegen deutlich zu kurz.[1496] In Bezug auf den Speicherzeitraum ergibt sich zudem aus dem Bewertungsbericht der Kommission sowie den Statistiken des Bundeskriminalamts, dass die überwiegende Anzahl der Abfragen in den ersten Monaten erfolgt. Je älter die Daten sind, desto seltener wurden die Daten abgerufen.

- Zugriff auf die Daten

Laut der Studie des Max-Planck-Instituts lehnten die befragten Polizeibeamten strikt die Einführung eines abgeschlossenen Straftatenkatalogs ab.[1497] In diesem Sinne äußern sich teilweise auch die befragten Vertreter der Staatsanwaltschaft, ein abstrakter Straftatbestand indiziere nicht die Schwere im Einzelfall.[1498] Polizeivertreter begründen die Ablehnung eines Straftatenkatalogs damit, dass dies auf Grund der rasanten Entwicklung neuer Straftaten geboten sei. Sie betonten zudem die Bedeutung der Ver-

[1493] *Albrecht/Kilchling* 2011; vgl. zu den Nachweisen über die befragten Personen, oben Fn. 1170.
[1494] *Albrecht/Kilchling* 2011, 160; dieser Forderung hat nun eindeutig das *BVerfG* eine Absage erteilt, die Zuordnung einer dynamischen IP-Adresse zu einem Anschluss ist als Verkehrsdatenauskunft zu qualifizieren, *BVerfG* Beschl. v. 24.1.2012 - 1 BvR 1299/05; vgl. dazu auch schon oben S. 142.
[1495] *Albrecht/Kilchling* 2011, 162.
[1496] *Albrecht/Kilchling* 2011, 171 Nur ein Vertreter forderte eine Speicherung über zwölf Monate.
[1497] *Albrecht/Kilchling* 2011, 161 f.
[1498] *Albrecht/Kilchling* 2011, 171.

kehrsdaten für das gesamte Spektrum der Internetkriminalität.[1499] Auch die befragten Staatsanwälte forderten einen Zugriff für Internetdelikte.[1500]
Als Alternativen zu einem abgeschlossenen Straftatenkatalog wurde von Seiten der Polizei unter anderem vorgeschlagen, die Abfrage an zwei unterschiedliche Kriterien zu knüpfen: zum einen an die Qualität einer Straftat (mittels eines Straftatenkatalogs) und zum anderen an die Ermittlungsmöglichkeiten im jeweiligen Kriminalitätsbereich (also unabhängig von der Schwere der einzelnen Tat). Nach einem anderen Vorschlag solle auf die Schwere der verursachten Rechtsgutverletzung abgestellt werden. Betont wird von allen, die Bedeutung des Zugriffs für mittels Telekommunikationsmittel begangene Straftaten. Gefordert wird daher an der Formulierung des § 100g Abs. 1 Nr. 2 StPO festzuhalten, da ansonsten die Ermittlungen im gesamten Bereich der Internetkriminalität unmöglich würden. Auch wird verlangt, dass für den gesamten Bereich der Internetkommunikation der Zugriff auf Bestandsdaten auch bei allen unterschwelligen Delikten möglich sein sollte.[1501]

Im Hinblick auf die Ausgestaltung der Zugriffsregelung durch Straftatenkataloge wird von Seiten der Ermittler als Alternative auch eine Differenzierung nach bestimmten Abfragearten angeregt. So könne etwa für Zielwahlsuchen ein eigener Katalog geschaffen werden. Da hier nur ein eng begrenzter Personenkreis betroffen sei, könnten hier auch niederschwelligere Delikte in den Katalog mitaufgenommen werden (etwa Enkeltrick oder Stalking).

Für den Bereich der Gefahrenabwehr wird gefordert, den Zugriff auf die auf Vorrat gespeicherten Verkehrsdaten immer dann zu ermöglichen, wenn eine Gefahr für Leib oder Leben einer Person oder für bedeutende Sachwerte besteht.[1502]

- Abrufverfahren

Für das Abrufverfahren fordern die Polizeivertreter, dass die ständige Erreichbarkeit bei den Providern sichergestellt sein müsse. Zudem sollten einheitliche Standards für die Übermittlung von Geo-Daten eingeführt werden. Sie plädieren auch für eine Standardisierung des Abrufverfahrens und der Form der Übermittlung der Daten.[1503]
Von einem Vertreter der Staatsanwaltschaft wird als Alternative zur Speicherung bei den Privaten eine Speicherung bei einer staatlichen Agentur vorgeschlagen, da so der Arbeitsablauf erleichtert würde. Dafür spreche auch, dass die Einbindung der privaten Anbieter zu Geheimhaltungsproblemen führe, da diese so Kenntnisse über aktuelle Ermittlungsverfahren erhielten.[1504]

9.1.1.3 Bedeutung der Vorratsdatenspeicherung für die Sicherheit

Die Vorratsdatenspeicherung wird von Befürwortern der Vorratsdatenspeicherung als zentrales Instrument zur Gewährleistung von Sicherheit im digitalen Zeitalter bewer-

[1499] *Albrecht/Kilchling* 2011, 160.
[1500] *Albrecht/Kilchling* 2011, 170.
[1501] *Albrecht/Kilchling* 2011, 161 f.
[1502] *Albrecht/Kilchling* 2011, 161 f.
[1503] *Albrecht/Kilchling* 2011, 163.
[1504] *Albrecht/Kilchling* 2011, 171.

tet.[1505] Eine Vorratsspeicherung der Telekommunikationsverkehrsdaten kann in unterschiedlichsten Konstellationen für die Ermittlungsarbeit von Sicherheitsbehörden neue Erkenntnisse bringen.

Aus ermittlungstechnischer Perspektive kann festgestellt werden, je umfassender eine Vorratsspeicherung ist, desto höher ist auch ihr Beitrag zu mehr Sicherheit. Allerdings zeichnet sich auch deutlich ab, dass die Bedeutung der einzelnen Datenkategorien für die Arbeit der Ermittlungsbehörden unterschiedlich hoch ist. So wird die größte Schutzlücke ohne Vorratsdatenspeicherung in Bezug auf eine Speicherung der IP-Daten gesehen.[1506] IP-Daten werden zudem auch am häufigsten abgerufen - wohlgemerkt jedoch nicht für die Verfolgung und Verhinderung besonders schwerer Delikte.

9.1.1.4 Würdigung

Dass es sich letztlich jedoch bei der Vorratsdatenspeicherung um ein zwar in vielerlei Hinsicht taugliches, jedoch nicht unentbehrliches Instrument handelt, wurde schon in Kap. 4.4.2 ausführlich dargelegt. Dies gilt auch in Anbetracht der von den Ermittlern beschriebenen besonders hohen Bedeutung einer Vorratsdatenspeicherung für ihre Arbeit.

Insgesamt muss konstatiert werden, dass eine exakte Bewertung der einzelnen Datenkategorien im Hinblick auf ihre Bedeutung für die Gewährleistung der Sicherheit daran scheitert, dass verlässliche Zahlen darüber bis heute fehlen, welche Daten, mit welchem zeitlichen Bezug, für welche Zwecke, abgerufen wurden und wie hoch ihre Bedeutung im jeweiligen Verfahren war.[1507]

Es kann lediglich in Bezug auf die Vorratsdatenspeicherung insgesamt die Tendenz festgestellt werden, dass je älter die Daten sind, desto seltener werden sie abgerufen. Hinsichtlich einzelner Datenkategorien lässt sich feststellen, dass bezüglich IP-Adressen aktuell Anfragen vielfach ins Leere führen, da die Daten nicht mehr gespeichert sind, wobei die Daten überwiegend zur Aufklärung niederschwelliger Delikte erforderlich sind.

Daraus, dass insbesondere in Bezug auf IP-Adressen ein hohes Interesse an einer Vorratsdatenspeicherung deklariert wird, kann aber nicht unmittelbar geschlossen werden, dass die Bedeutung einer IP-Datenspeicherung auch den höchsten Beitrag zur Sicherheit insgesamt leistet. Ihnen kommt zwar zur Aufrechterhaltung von Sicherheit und Ordnung eine hohe Bedeutung zu. Allerdings werden sie überwiegend zur Verfolgung von Delikten im Bereich der Internetkriminalität und insoweit zur Aufklärung niederschwelliger Delikte abgerufen. Darüber hinaus kommt ihnen eine hohe Bedeutung bei der Verfolgung von Urheberrechtsverletzungen zu. Dies sind allerdings weniger schwere Rechtsgutsverletzungen.

[1505] Vgl. dazu oben Kap. 4.4.2.
[1506] Dazu oben S. 196.
[1507] So schon S. 168 f.

9.1.2 Freiheitsrechte der Bürger

Die Vorratsspeicherung der Telekommunikationsverkehrsdaten greift in die Freiheitsrechte der Bürger besonders stark ein, da hier flächendeckend aussagekräftige Daten über das gesamte Telekommunikationsverhalten jedes Einzelnen gespeichert werden. Eine solche Regelung kollidiert mit verschiedenen um Schutz der Freiheit des Bürgers vorgesehenen Rechten.

9.1.2.1 Telekommunikationsfreiheit

Vornehmlich greift die Speicherung der Telekommunikationsverkehrsdaten auf Vorrat in das Fernmeldegeheimnis, geschützt durch Art. 10 Abs. 1 GG, ein.[1508] Dieser schützt nicht nur den Inhalt der Kommunikation, sondern auch die Umstände. Europarechtlich wird diese durch das Recht auf Privatheit aus Art. 8 EMRK sowie durch die Art. 7 und 8 EU-GRCh. geschützt.[1509]

Art. 10 Abs. 2 S. 1 GG enthält einen unlimitierten Gesetzesvorbehalt. Eingriffe können demnach gerechtfertigt werden, wenn sie auf einem förmlichen Gesetz beruhen und materiell den verfassungsrechtlichen Anforderungen insbesondere dem Verhältnismäßigkeitsprinzip entsprechen.

Die Verpflichtung der Telekommunikationsdiensteanbieter zur Speicherung sämtlicher Verkehrsdaten ist schon an sich ein Eingriff in das Fernmeldegeheimnis. Die Speicherung stellt darüber hinaus einen weiteren eigenständigen Eingriff dar.[1510] Dieser Eingriff ist dem Staat unmittelbar zurechenbar, da die Telekommunikationsdiensteanbieter ohne die Verpflichtung zur Vorratsdatenspeicherung diese Daten nicht so lange und gesondert speichern dürften. Vielmehr werden sie durch die Speicherungsverpflichtung zur Erfüllung einer originär staatlichen Aufgabe als Hilfspersonen für die staatliche Aufgabenerfüllung herangezogen.[1511] Weitere Eingriffe liegen sodann in der Übermittlung der auf Vorrat gespeicherten Verkehrsdaten und in deren mittelbaren Nutzung durch die öffentliche Gewalt.[1512]

[1508] Ausführlich zum Schutzbereich und Umfang von Art. 10 GG, oben Kap. 2.1.3.3, S. 95 ff.

[1509] *Petri*, RDV 2003, 16, 18; dazu schon oben Kap. 2.1.3.3.5, S. 100.

[1510] BVerfGE 125, 260; *Brinkel/Lammers*, ZUM 2008, 11; ausführlich zur Kritik an der Annahme eines besonders schweren Grundrechtseingriffs durch die Senatsmehrheit in den Sondervoten der Richter *Schluckebier* und *Eichenberger,* sowie aus der Literatur, oben Kap. 4.2.4.2, S. 158 ff.

[1511] Zwar ist weitgehend ungeklärt unter welchen Voraussetzungen „der öffentlichen Gewalt ein von ihr kettenverursachtes Verhalten als Inhalt oder Grundalge einer Grundrechtsbeeinträchtigung zugerechnet werden kann (…) Allgemein anerkannt dürfte die Verantwortung des Staates für Verhalten anderer sein, dass er durch auf dieses Verhalten gerichtete Imperative veranlasst hat. Der Anspruch auf Gehorsam, den die Rechtsordnung für staatliche Imperative erhebt, schließt es aus, dass der Staat die Verantwortung für die Ausführung seiner Befehle auf die Adressaten abwälzt.“ *Stern* Staatsrecht III, Bnd. 2, 1994, § 78 III 3, S. 178; vgl. dazu auch BVerfGE 125, 260 (305); mit Verweis auf BVerfGE 107, 299 (313 f.); so auch schon *Gola/Klug/Reiff* NJW 2007, 2599; *Rusteberg* VBlBW 2007, 171, 174; In Bezug auf das Urteil zur VDS zustimmend *Klesczewski,* JZ 2010, 629. *Wolff* sieht hingegen darin einen neuen bzw. veränderten Eingriffsbegriff, da der Staat zum Zeitpunkt der Speicherung noch nicht auf die Daten zugreife, NVwZ 2010, 752.

[1512] BVerfGE 125, 260 (310) unter Bezugnahme auf BVerfGE 100, 313 (366);110, 33 (52 f.).

Das *Bundesverfassungsgericht* stellt im Urteil zur Vorratsdatenspeicherung klar, dass auch die Vertraulichkeit des E-Mail-Verkehrs dem Schutzbereich des Telekommunikationsgeheimnisses unterfällt.[1513] Da E-Mail-Kommunikation sehr leicht abgefangen werden kann, hätte dies bezweifelt werden können. Die grundsätzliche Schutzwürdigkeit einer Freiheitsausübung kann aber nicht davon abhängen, ob und wie leicht durch technische Hilfsmittel Dritte unberechtigt in einen Kommunikationsweg eingreifen können.

Auch greift die Speicherung der Daten über den Internetzugang stets in das Fernmeldegeheimnis ein, obwohl dieser zur Teilnahme an Massenkommunikation genutzt wird und so an sich der Rundfunkfreiheit aus Art. 5 Abs. 1 S.2 GG zuzuordnen wäre. Eine Unterscheidung zwischen Individual- und Massenkommunikation ist jedoch bei der Internetnutzung nicht möglich, ohne dabei an den Inhalt der Kommunikation anzuknüpfen. Den Inhalt zu ermitteln, um den Schutzbereich zu ermitteln, widerspräche der Schutzfunktion der Grundrechte allerdings diametral, so dass bereits die Speicherung der Internetzugangsdaten als ein Eingriff in Art. 10 Abs. 1 GG zu werten ist.[1514]

Mit dem Ziel Sicherheit zu erzeugen, verfolgt die Vorratsdatenspeicherung ein legitimes Ziel, das grundsätzlich geeignet ist, den Eingriff zu rechtfertigen.[1515] Fraglich ist aber, ob der Eingriff auch geeignet und erforderlich und im Sinne der Verhältnismäßigkeit Plus unverzichtbar und alternativlos ist. Schließlich ist zu untersuchen, welche Anforderungen zur Erzielung eines angemessenen Interessenausgleichs zu beachten sind.

9.1.2.1.1 Geeignet, aber verzichtbar

Die Vorratsdatenspeicherung ist jedenfalls aus einer Ex-Ante-Perspektive nicht schlechthin ungeeignet, um das Regelungsziel, Sicherheit zu erzeugen, zu befördern. In der Literatur war zum Teil vertreten worden, dass die Vorratsdatenspeicherung ungeeignet sei, da sie bei intelligenten, professionellen Kriminellen nichts nütze. Hier sei eine Vorratsdatenspeicherung eher kontraproduktiv, da sie die Entwicklung und den Einsatz von Anonymisierungstechniken und Umgehungsstrategien befördere.[1516]

Dies ändert aber nichts an der grundsätzlichen Eignung. So hat auch das *Bundesverfassungsgericht* betont: „Unerheblich ist, ob die vom Gesetzgeber geschaffenen Regelungen in der Lage sind, lückenlos alle Telekommunikationsverbindungen zu rekonstruieren. Auch wenn eine solche Datenspeicherung nicht sicherstellen kann, dass alle Telekommunikationsverbindungen verlässlich bestimmten Anschlussnehmern zugeordnet werden können, und etwa Kriminelle die Speicherung durch die Nutzung von Hotspots, Internetcafés, ausländischen Internettelefondiensten oder unter falschen Namen angemeldeten Prepaid-Handys unterlaufen können, kann dies der Geeignetheit einer solchen Regelung nicht entgegenhalten werden. Diese erfordert nicht, dass das Regelungsziel in jedem Einzelfall tatsächlich erreicht wird, sondern verlangt lediglich, dass die Zweckerreichung gefördert wird“.[1517] Selbst wenn der

[1513] BVerfGE 125, 260 (311).
[1514] BVerfGE 125, 260 (311).
[1515] Dazu oben Kap. 2.2; Kap. 3.2.
[1516] so *Breyer*, StV 2007, 214, 218 ff.
[1517] BVerfGE 125, 260 (317 f.).

Beitrag einer Vorratsdatenspeicherung faktisch zur Sicherheit nur minimal ist oder nicht nachweisbar ist, handelt es sich im Sinne der klassischen Verhältnismäßigkeitsprüfung dennoch um eine geeignete Maßnahme. [1518]

Im Sinne des Ziels, einen optimierten Interessenausgleich zu erzeugen, soll nunmehr auch untersucht werden, ob die Vorratsdatenspeicherung auch unverzichtbar im Sinne der erweiterten Verhältnismäßigkeitsprüfung ist.[1519] Zu berücksichtigen ist, dass ohne eine Verpflichtung zur Vorhaltung der Telekommunikationsverkehrsdaten viele Daten für einen vergleichbaren Zeitraum gespeichert werden. Allerdings sind große Unterschiede in der Speicherpraxis zu verzeichnen:

		Speicherzeiten (Tage) (t-Spannweite bei NB&SP)				Speicherzeiten (Tage) (t-Spannweite bei NB&SP)		
		Festnetz				Internet (DSL/Breitband)	VOIP	E-Mail
		MobFu	(analog/ISBN/VoIP)					
A1: Speicherung der Rufnummer des anrufenden Anschlusses	nicht pauschal abgerechnete Verbindungen	7-180	7-180	**A2:** zugewiesene Benutzererkennung	nicht pauschal abgerechnetet Verbindungen	7-90	7-180	1-60
	Flatrate	7-120	7-180		Flatrate	7-90	7-90	
B1: Speicherung der Rufnummer des angerufenen Anschlusses	nicht pauschal abgerechnete Verbindungen	7-180	9-210	**A2**: zugewiesene IP-Adresse	nicht pauschal abgerechnete Verbindungen	2-90	7-30	1-60
	Flatrate	7-210	7-210		Flatrate	2-10	7-30	

Abbildung 1: Speicherzeiten im Bereich Mobilfunk, Festnetz Internet, VoIP und E-Mail aus der Analyse durch das Max-Planck-Institut (Freiburg), nach *Albrecht/Kilchling* 2011, 68 f.[1520]

Die sehr kurzen Speicherfristen bei IP-Daten führen dazu, dass hier von Ermittlerseite der höchste Bedarf an einer Vorratsspeicherung formuliert wird.[1521] Allerdings ist in diesem Kontext zu berücksichtigen, dass eine Vielzahl der Abfragen von IP-Adressen nicht allein der Verfolgung schwerer Kriminalität dient, sondern überwiegend zur Verfolgung von Urheberrechtsverletzungen oder niederschwelliger Delikte (insbesondere aus dem Deliktsfeld der Informations- und Kommunikationskriminalität). Dennoch kann im Hinblick auf nicht nachweisbare Steigerung der Aufklärungsraten und der bestehenden hohen Aufklärung auch im Bereich der Internetkriminalität davon ausge-

[1518] BVerfGE 125, 260 (318); zur Schwäche der Verhältnismäßigkeitsprüfung bei Datenerhebungs- und verarbeitungsmaßnahmen, vgl. oben Kap. 6.2.2.

[1519] Zu diesem Merkmal oben, S. 238.

[1520] Als Quellle wird hier auf eine Veröffentlichung der Bundesnetzagentur verwiesen, die allerdings nicht öffentlich verfügbar ist; Aus den vom Max-Planck-Institut ermittelten Speicherzahlen, ergibt sich eine durschnittliche Speicherpraxis im Bereich des Mobilfunks von 28 Tagen (sowohl bei pauschal als auch bei nicht pauschal abgerechneten Tarifen der Rufnummer des Anrufenden). Ausgehende Anrufe werden durchschnittlich sogar 96 Tage bei Flatrate-Tarifen und 112 Tage bei nicht pauschal abgerechneten Verbindungen gespeichert. Im Festnetzbereich sind es 55 Tage bei Flatrate-Tarifen und ansonsten 132 Tage. Im Internet werden die zugewiesenen Benutzerkennungen im Durchschnitt 47 bzw. 48 Tage gespeichert. Im Bereich der Internet-Telefonie für 20 Tage und bei E-Mail für 23 Tage. Die IP-Adressen werden im Internet generell (durchschnittlich) vier Tage gespeichert, im Bereich VoIP für sieben Tage und bei E-Mail 22 Tage.

[1521] Vgl. oben S. 186 ff.

gangen werden, dass die Vorratsdatenspeicherung verzichtbar für die Gewährleistung von Sicherheit ist.[1522]

Sie ist zwar unzweifelhaft geeignet die Sicherheit zu fördern, sie ist aber nicht unverzichtbar.

9.1.2.1.2 Erforderlich, aber nicht alternativlos

Fraglich ist, ob die Vorratsdatenspeicherung erforderlich und im Sinne der Verhältnismäßigkeitsprüfung Plus alternativlos ist.[1523]

An der Erforderlichkeit fehlt es nach der klassischen Verhältnismäßigkeitsprüfung dann, wenn ein milderes, den Adressaten weniger belastendes Mittel zur Wahl steht.[1524] Verlangt wird hier vom *Bundesverfassungsgericht* eine „eindeutig gleichwertige Alternative".[1525] Das heißt, die Erfolgswahrscheinlichkeit muss sich gleichermaßen steigern. Vielfach wurde ein Quick-Freeze-Verfahren als Alternative in Diskussion um die Vorratsdatenspeicherung eingebracht.

Quick-Freezing beschreibt ein Verfahren, bei dem nicht sämtliche Kommunikationsdaten aller Bürger auf Vorrat gespeichert werden, sondern nur bei einem konkreten Anlass die Daten für einen kurzen Zeitraum vorgehalten werden und eventuell bei Vorliegen der gesetzlichen Voraussetzungen der abrufenden Behörde übermittelt werden. Der Grundrechtseingriff wiegt, soweit nicht von sämtlichen Bürgern umfassend die Telekommunikationsverkehrsdaten auf Vorrat gespeichert werden, insgesamt weniger schwer.[1526]

Quick-Freeze ist aber, so hat es das *Bundesverfassungsgericht* mit klaren Worten festgestellt, nicht gleich geeignet.[1527] Denn bei einer nur anlassbezogenen Speicherung stehen automatisch stets weniger Daten zur Verfügung als bei einer umfassende Vorratsspeicherung.[1528]

Dies ist den hohen Anforderungen, die das Gericht an die gleiche Eignung stellt, geschuldet. Im Sinne der Verhältnismäßigkeitsprüfung Plus, ist um dem Prüfungspunkt der Erforderlichkeit Wirkungskraft zu verleihen, auch zu prüfen, ob nicht zumindest auch funktional gleichwertige Maßnahmen als Alternative in Betracht kommen. Es sollte eben nicht allein auf den Umfang der Datenerhebung abgestellt werden.[1529]

[1522] Vgl. dazu oben S. 203 ff.
[1523] Zum Merkmal der Alternativlosigkeit, vgl. oben S. 259.
[1524] *Sommermann*, in *Mangoldt/ Klein/ Starck*, GG 2010, Art. 20 Abs. 3, Rn. 314; *Hofmann,* in: *Schmidt-Bleibtreu/Klein,* GG Komm 2011, Art. 20, Rn. 73.
[1525] *Sachs*, in *Sachs,* GG 2011, Art. 20 145ff, Rn. 152.
[1526] Zur Gefahr, dass sich ein Quick-Freeze als „Wolf im Schafspelz" entpuppen könnte, wenn die Ermittlungsbehörden umfassend und konstant sämtliche Verkehrsdaten auf Vorrat speichern würden (wie http://www.moenikes.de/ITC/2011/01/18/quick-freeze-ProzentE2Prozent80Prozent93-der-wolf-im-schafspelz/ meint) *Knierim* 2011a.
[1527] BVerfGE 125, 260 (318).
[1528] *Hornung/Schnabel*, DVBl. 2010, 824, 826.
[1529] *Hornung/Schnabel*, DVBl. 2010, 824, 826; Zu diesem Problem schon ausführlich oben Kap. 6.2.2.

Im Folgenden wird daher geprüft, ob die Vorratsdatenspeicherung im Sinne einer Verhältnismäßigkeitsprüfung Plus alternativlos ist. Dabei wird nicht gefragt, ob es sich um ein exakt gleich geeignetes Instrument handelt, sondern ob eine Alternative funktional entsprechend geeignet ist. Kernfrage ist also, ob eine grundrechtsschonendere, funktional entsprechende Alternative zur Vorratsdatenspeicherung denkbar ist.

Trotz der geringeren Datenmengen, die bei einem Quick-Freeze-Verfahren gespeichert werden, handelt es sich dabei um ein Verfahren, das zwar kein ebenso effektives Instrument ist, das aber auf Grund der geringeren Eingriffsintensität als grundrechtsschonendere Alternative zu diskutieren ist. Dies gilt insbesondere aufgrund der Tatsache, dass Telekommunikationsanbieter Verkehrsdaten durchaus auch zu Abrechnungszwecken für bis zu sechs Monate speichern.[1530]

Praktiker sehen jedoch über alle Berufsgruppen hinweg in einem Quick-Freeze-Verfahren kein taugliches Äquivalent zur Vorratsdatenspeicherung. Begründet wird dies damit, dass diese Methode nur ohnehin vorhandene Verkehrsdaten „selektiv vor der Löschung" bewahren kann. Die aus ermittlungstechnischer Sicht besonders wichtigen retrograden Daten können aber nicht ex post generiert werden.[1531] Polizeibeamte mahnen sodann, dass ohne Vorratsdatenspeicherung mehr Inhaltsüberwachungen durchgeführt würden.[1532]

Dennoch handelt es sich bei einem Quick-Freeze um eine funktional entsprechende Alternative, die weniger tief in die Freiheitsrechte der Bürger eingreift.[1533] Denn Quick-Freeze und Vorratsdatenspeicherung zielen beide auf die Sicherung von Telekommunikationsverkehrsdaten. Die Datenerhebung ist zwar bei einer Vorratsdatenspeicherung umfassender, jedoch genügen in einer Vielzahl der Fälle, die Verkehrsdaten, die auch durch ein Quick-Freeze gespeichert werden können. Analysen von Verkehrsdaten, die sechs Monate oder gar zwei Jahre alt sind, finden nur in einer geringen Anzahl von Fällen statt.[1534] Statistiken zeigen, dass Verkehrsdaten überwiegend in den ersten drei Monaten abgefragt werden.[1535] Es sind insofern überwiegend höchst aktuelle Daten, die für die Arbeit der Ermittlungsbehörden benötigt werden. Diese können auch mit einem Quick-Freeze-Verfahren den Ermittlungsbehörden zur Verfügung gestellt werden. Die Aussagekraft ist geringer, aber genügt in vielen Fällen für die polizeiliche Praxis. Dies gilt insbesondere, da in der Praxis Telekommunikationsanbieter trotz Flatrate-Tarifen, die Verkehrsdaten für einen gewissen Zeitraum speichern.[1536]

[1530] Vgl. Abbildung S. 271.

[1531] *Albrecht/Kilchling* 2011, 162 f., 167, 227 ff.

[1532] *Albrecht/Kilchling* 2011, 167. Vertreter der Staatsanwaltschaft betonten hingegen, dass eine Inhaltsüberwachung prinzipiell schwerer wiege, da diese auf eine Inhaltsüberwachung zielt.

[1533] Vgl. dazu auch *Arning/Moos* ZD 2012, 153 ff.

[1534] Eine Speicherung über einen längeren Zeitraum als sechs Monate wäre darüber hinaus in jedem Fall verfassungswidrig, da es die Obergrenze einer zulässigen Speicherung der Telekommunikationsverkehrsdaten auf Vorrat sprengen würde, BVerfGE 125, 260 (322).

[1535] Vgl. Nachw. in Fn. 1227.

[1536] Wobei darauf hinzuweisen ist, dass die Speicherpraxis der Unternehmen insgesamt sehr unterschiedlich ist, Vgl. dazu Abbildung, S.271; eine siebentägige Speicherung der IP-Adressen wird von Gerichten auch bei Flatrate-Verträgen als zulässig erachtet, *LG Darmstadt*, CR 2007, 574.

Lediglich im Bereich von IP-Adressen ist aktuell eine Lücke mangels Speicherung durch die Anbieter erkennbar.

Als Kompromisslösung kann daher auch eine Vorratsdatenspeicherung light oder ein „Quick-Freeze XXL" als Alternative diskutiert werden. Dabei handelt es sich um eine Kombination beider Konzepte: Die Verpflichtung zur Speicherung auf Vorrat beschränkt sich auf bestimmte Daten (und zwar auf jene, bei denen auf Grund der kurzen Speicherung durch die Anbieter und der besonderen Bedeutung für die Ermittlungsarbeit, eine Vorratsspeicherung geboten ist), während alle anderen Daten nur auf Antrag gespeichert werden. Da es sich aber auch bei einem solchen Verfahren um eine Vorratsdatenspeicherung handelt, eben nur in geringerem Umfang, soll dieser Ansatz hier nicht als Alternative diskutiert werden, da er keine wirkliche Alternative ist. Es handelt sich vielmehr um eine Gestaltungsalternative der Vorratsdatenspeicherung.

Es wurde aufgezeigt, dass die Vorratsdatenspeicherung zwar im Sinne der klassischen Verhältnismäßigkeitsprüfung erforderlich ist, im Hinblick auf eine Verhältnismäßigkeitsprüfung Plus handelt es sich aber bei Quick-Freeze um eine funktional entsprechende Alternative auch wenn hier deutlich weniger Daten erfasst werden können.

9.1.2.1.3 Angemessenheit

Für die Entwicklung eines optimierten Interessenausgleichs, der auch den Anforderungen der Verhältnismäßigkeit im engeren Sinne genügt, kommt es darauf an, wie schwer der Eingriff in das Telekommunikationsgeheimnis wiegt.

9.1.2.1.3.1 Besonders schwerer Grundrechtseingriff

Der Erste Senat wertet den Eingriff durch die Vorratsdatenspeicherung überzeugend als besonders schwerwiegend.[1537] Das Gericht begründet dies mit der Streubreite der Maßnahme, ihrer Anlasslosigkeit, der Möglichkeit aus den Daten umfassende Bewegungs- und Persönlichkeitsprofile zu erstellen und Rückschlüsse auf den Inhalt der Kommunikation zu ziehen.[1538] Darüber hinaus steige mit einer Vorratsdatenspeicherung das Risiko weiterer Eingriffe, „ohne selbst Anlass dazu gegeben zu haben. Es reicht etwa aus, zu einem ungünstigen Zeitpunkt in einer bestimmten Funkzelle gewesen oder von einer bestimmten Person kontaktiert worden zu sein, um in weitem Umfang Ermittlungen ausgesetzt zu werden und unter Erklärungsdruck zu geraten. Auch die Missbrauchsmöglichkeiten, die mit einer solchen Datensammlung verbunden sind, verschärfen deren belastende Wirkung. Das gilt insbesondere wegen der Vielzahl verschiedener privater Anbieter, bei denen die Telekommunikationsdaten gespeichert werden. Schon angesichts der Anzahl der Speicherungsverpflichteten ist die Zahl derjenigen groß, die Zugriff auf solche Daten haben und haben müssen. Da die Speicherungspflicht kleinere Dienstanbieter mitbetrifft, stößt die Sicherung vor Missbrauch ungeachtet aller möglichen und erforderlichen Anstrengungen des Gesetzgebers auch mit Blick auf deren Leistungsfähigkeit auf strukturelle Grenzen. Verstärkt

[1537] BVerfGE 125, 260 (318); oben in Kap. 4.2.4.2 ausführlich zur Kritik in den Sondervoten und aus der Literatur, dass es sich um keinen besonders schwerwiegenden Grundrechtseingriff handle (S. 158 ff.)

[1538] BVerfGE 125, 260 (319). Daher könne auch „nicht ohne Weiteres davon ausgegangen werden, dass der Rückgriff auf diese Daten grundsätzlich geringer wiegt als eine inhaltsbezogene Telekommunikationsüberwachung", BVerfGE 125, 260 (328).

wird dies dadurch, dass die Anforderungen an die Datenverwaltung und die Übermittlung der Daten an die Behörden ein hohes Maß an Technikbeherrschung sowie anspruchsvolle Software voraussetzen, womit sich zwangsläufig die Gefahr von Schwachstellen und das Risiko von Manipulationen durch interessierte Dritte verbinden. Besonderes Gewicht bekommt die Speicherung der Telekommunikationsdaten weiterhin dadurch, dass sie selbst und die vorgesehene Verwendung der gespeicherten Daten von den Betroffenen unmittelbar nicht bemerkt werden, zugleich aber Verbindungen erfassen, die unter Vertraulichkeitserwartungen aufgenommen werden. Hierdurch ist die anlasslose Speicherung von Telekommunikationsverkehrsdaten geeignet, ein diffus bedrohliches Gefühl des Beobachtetseins hervorzurufen, das eine unbefangene Wahrnehmung der Grundrechte in vielen Bereichen beeinträchtigen kann".[1539]

Insbesondere aufgrund der Analysemöglichkeiten, der Anlasslosigkeit der Erhebung und den damit einhergehenden Risiken ist der Eingriff durch die Verpflichtung zur Speicherung der Telekommunikationsverkehrsdaten auf Vorrat einvernehmlich mit dem *Bundesverfassungsgericht* und entgegen aller vorgebrachter Kritik im Ergebnis als besonders schwer zu qualifizieren.

Den Wesensgehalt sieht das *Bundesverfassungsgericht* bei einer sechsmonatigen Speicherung der Umstände der Telekommunikation als noch nicht verletzt an. Sie bleibe „trotz ihrer außerordentlichen Weite noch wirksam begrenzt".[1540] Anders in der Literatur, hier wurde zum Teil auch angenommen, dass schon die anlassunabhängige, generelle Speicherung aller Telekommunikationsverkehrsdaten den Wesensgehalt von Art. 10 GG verletzte.[1541] Fest steht jedenfalls, dass wenn eine Vorratsspeicherung flächendeckend die Inhalte der Kommunikation erfassen sollte, der Wesensgehalt verletzt würde.[1542] Wesentlich für die Verfassungsmäßigkeit einer Vorratsdatenspeicherung ist, dass sie in ihrem Umfang „wirksam begrenzt" ist.[1543] Im Hinblick auf den Speicherzeitraum liegt nach Ansicht des *Bundesverfassungsgerichts* eine sechsmonatige Speicherung an der „Obergrenze" des verfassungsrechtlich Zulässigen.[1544]

9.1.2.1.3.2 Anforderungen an eine verhältnismäßige Ausgestaltung

„Maßgeblich für die Rechtfertigungsfähigkeit" einer Verpflichtung zur Vorratsdatenspeicherung ist, so das *Bundesverfassungsgericht*, „dass sie nicht direkt durch staatliche Stellen erfolgt, dass sie nicht auch die Kommunikationsinhalte erfasst und dass auch die Speicherung der von ihren Kunden aufgerufenen Internetseiten durch kommerzielle Dienstanbieter grundsätzlich untersagt ist."[1545] Im Anschluss an die Erwägungen zur Eingriffsintensität betont das Gericht, dass es für die verfassungsrechtliche Unbedenklichkeit der Vorratsdatenspeicherung Voraussetzung sei, „dass die Ausgestaltung der Speicherung und der

[1539] BVerfGE 125, 260 (320).
[1540] Auch der Menschenwürdekern sei nicht verletzt, BVerfGE 125, 260 (322).
[1541] Durch die anlassunabhängige, generelle Speicherung aller Verkehrsdaten würde die Geheimnisqualität prinzipiell beeinträchtigt werden, *Dix/Petri*, DUD 2009, 531, 532 f.; *Gercke* in *Roggan* 2006, 177.
[1542] So auch *Hofmann*, in *Schmidt-Bleibtreu/Klein*, GG 2011, Art. 10, Rn. 4a.
[1543] BVerfGE 125, 260 (322).
[1544] BVerfGE 125, 260 (322).
[1545] BVerfGE 125, 260 (324).

Verwendung der Daten dem besonderen Gewicht einer solchen Speicherung angemessen Rechnung trägt".[1546]

Als „maßgeblich" dafür wertet das Gericht zunächst, „dass die vorgesehene Speicherung der Telekommunikationsverkehrsdaten nicht direkt durch den Staat, sondern durch eine Verpflichtung der privaten Dienstanbieter verwirklicht wird".[1547] Eine unmittelbare Speicherung beim Staat oder auch bereits die staatliche Möglichkeit unvermittelt auf die Daten zuzugreifen, wäre mit der datenschutzrechtlichen Dimension des Telekommunikationsgeheimnisses nicht zu vereinbaren. Das *Bundesverfassungsgericht* argumentiert, dass die Daten so auf viele Einzelunternehmen verteilt würden und damit dem Staat nicht unmittelbar zur Verfügung stünden. Dies könne dazu beitragen, dass die tatsächliche Verwendung auf den unbedingt erforderlichen Teil beschränkt wird. Zudem würden Transparenz und Kontrolle befördert.[1548]

Letztlich stärkt das *Bundesverfassungsgericht* mit dem Verbot, die Daten unmittelbar beim Staat zu speichern, den Datenschutz zu Lasten der Datensicherheit. So liegt es nahe, dass bei einer Verteilung auf die vielen, zum Teil sehr kleinen Telekommunikationsanbieter, kein so hoher technischer Sicherheitsstandard realisiert werden kann, wie er bei einer zentralen Speicherung umgesetzt werden könnte.[1549] Es kann insofern festgestellt werden, dass das Gericht mit der Anforderung, die Daten bei den Anbietern zu speichern, darauf zielt, den Datenschutz durch eine dezentrale Organisation der Speicherung zu stärken. Insofern darf die Übertragung der Speicherungsverpflichtung auf die Privaten nicht dazu führen, dass diese vielfach die Speicherungsverpflichtung auf ein drittes Unternehmen auslagern und so letztlich doch eine zentrale Datenbank entsteht.

Fraglich ist insofern, ob nicht sogar zu fordern wäre, dass auch große Telekommunikationsanbieter nicht zentral, sondern dezentral die Telekommunikationsverkehrsdaten auf Vorrat speichern. Es handelt sich dabei um eine Forderung, die aus datenschutzrechtlicher Sicht zu begrüßen wäre, deren Verhältnismäßigkeit jedoch abhängig ist von den zusätzlichen Kosten, die eine solch dezentrale Speicherung bei den großen Anbietern verursachen würde.

Das Gericht fordert aber nicht nur aus datenschutzrechtlichen Gründen eine dezentrale Speicherung, sondern verlangt vor allem auch, dass die Daten nicht staatsunmittelbar gespeichert werden. Damit soll schon strukturell die Trennung zwischen Erhebung und Verwendung der Daten betont und so das Gefühl des Überwachtwerdens reduziert werden.

Neben der Forderung die Daten nicht unmittelbar beim Staat zu speichern, verlangt das Gericht, dass sie „besonderen verfassungsrechtlichen Anforderungen insbesondere hin-

[1546] BVerfGE 125, 260 (324)
[1547] BVerfGE 125, 260 (321).
[1548] BVerfGE 125, 260 (322).
[1549] *Forgò/Krügel* K&R 2010, 217, 219 verweisen darauf dass in Anbetracht der Datenskandale bei Privaten jedenfalls eine umfassende staatliche Kontrolle geboten wäre; dass bei einer zentralen staatlichen Datenspeicherung ein höherer Sicherheitsstandard gewährleistet werden könnte, führt *Ziebarth*, DuD 2009, 25, 29 aus.

sichtlich der Datensicherheit, des Umfangs der Datenverwendung, der Transparenz und des Rechtsschutzes“ unterliegen. „Nur wenn diesbezüglich hinreichend anspruchsvolle und normenklare Regelungen getroffen sind, ist der in einer solchen Speicherung liegende Eingriff verhältnismäßig im engeren Sinne.“[1550]

Das Gericht hat sehr konkrete Anforderungen an die verhältnismäßige Ausgestaltung einer Vorratsdatenspeicherung formuliert, da auf Grund des besonders hohen Eingriffsgewichts, dem Gesetzgeber für die Ausgestaltung der Maßnahme nur ein geringer Gestaltungsspielraum verbleibt. Das besonders hohe Eingriffsgewicht macht besonders hohe Schutzmaßnahmen des Gesetzgebers erforderlich.[1551]

Insofern ist von zentraler Bedeutung, dass nur Verkehrsdaten gespeichert werden und keine Inhaltsdaten. Darüber hinaus ist erforderlich, um die grundsätzliche Vertraulichkeit der Telekommunikation zu wahren, dass die Datenerhebung nicht total ist. Das heißt, es müssen noch unüberwachte Kommunikationswege verbleiben. Die Speicherung darf nicht auf unbestimmte Zeit erfolgen. Dies folgt aus der datenschutzrechtlichen Dimension des Telekommunikationsgeheimnisses.[1552]

Der datenschutzrechtliche Kern des Telekommunikationsgeheimnisses verlangt, dass der Einzelne grundsätzlich wissen muss, wer was wann über ihn weiß. Da die Vorratsdatenspeicherung an sich eine Maßnahme ist, die alle Bürger betrifft, jedoch bei der Speicherung noch keine (bewusste/menschliche) Kenntnisnahme erfolgt, muss dann, wenn auf personenbezogene Daten zugegriffen wird, der Einzelne darüber unterrichtet werden. Es müssen daher Informationspflichten eingeführt werden darüber, wann wer zu welchem Zweck auf die Daten zugegriffen hat.

Bei der Verpflichtung zur Speicherung muss die Verwendung der Daten bestimmt sein.[1553] Notwendig ist, gerade auch, um Rechtssicherheit zu gewährleisten, dass eine präzise und abschließende Regelung darüber getroffen wird, wann und für welche Zwecke auf die Daten zugegriffen werden darf. Um eine Zweckentfremdung der Daten zu vermeiden, ist eine Kennzeichnung der Daten erforderlich.[1554] Damit der Zweckbindungsgrundsatz darüber hinaus – durch die erfolgte veränderte Auslegung des Verbots einer Datenspeicherung auf Vorrat[1555] – nicht insgesamt ausgehöhlt wird, ist sicherzustellen, dass eine anlasslose Sammlung personenbezogener Daten auf Vorrat zu einem bestimmten Zweck nur als Ausnahme erfolgt.

[1550] BVerfGE 125, 260 (325).
[1551] *Britz*, JA 2011, 81, 82; zur Kritik, das Gericht habe seine Kompetenzen überschritten und die Gesetzgebungsprärogative unzulässig beschnitten, oben S. 129 ff.
[1552] Zum Verhältnis des Rechts auf informationelle Selbstbestimmung und des Telekommunikationsgeheimnisses, vgl. oben S. 100 ff.
[1553] BVerfGE 125, 260 (317).
[1554] So auch BVerfGE 125, 260 (333).
[1555] Dazu oben S. 139 f.

Darüber hinaus verlangt der Zweckbindungsgrundsatz, dass eine informationelle Gewaltenteilung sichergestellt wird, die Daten gegenüber Unberechtigten gesichert werden und ein Zugriffsschutz garantiert wird.[1556]

Um dem datenschutzrechtlichen Erforderlichkeitsgrundsatz zu genügen, sind die Daten sobald sie nicht mehr erforderlich sind, zu löschen.[1557] Darüber hinaus muss gerade bei der Ausgestaltung der Vorratsdatenspeicherung die Erforderlichkeit der jeweiligen Datenerhebung gewahrt werden. Aus dem Grundsatz der Datensparsamkeit und Datenvermeidung ergibt sich, dass die Vorratsdatenspeicherung so auszugestalten ist, dass dabei möglichst wenig Daten erzeugt und gespeichert werden.

9.1.2.1.3.3 Richtervorbehalt

Das *Bundesverfassungsgericht* geht in gefestigter Rechtsprechung davon aus, dass der Verhältnismäßigkeitsgrundsatz verlangt bei besonders schwerwiegenden Eingriffen in die Telekommunikationsfreiheit eine präventive richterliche Prüfung vorzusehen.[1558] Auch im Urteil zur Vorratsdatenspeicherung stellt das *Bundesverfassungsgericht* fest, dass eine verhältnismäßige Ausgestaltung voraussetzt, dass die Verwendung der Daten durch einen Richtervorbehalt verfahrensrechtlich begrenzt wird.[1559] Sinn und Zweck des Richtervorbehalts besteht darin vorbeugend eine tief in die Freiheitsrechte der Bürger eingreifende Maßnahme durch eine unabhängige Instanz zu kontrollieren.

Ob der Richtervorbehalt jedoch tatsächlich eine effektive Schutzwirkung zu Gunsten der Freiheitsrechte der Bürger entfaltet, kann im Hinblick auf die Praxis bezweifelt werden.

So wurde im Jahr 2011 bekannt, dass Ermittlungsbehörden bei Anti-Nazi-Demonstrationen in Dresden über bis zu zwei Tagen sämtliche Verkehrs- und Bestandsdaten mehrerer Funkzellen erhoben haben (insgesamt über 1 Mio. Verbindungsdaten).[1560] Zunächst war die Erhebung mit Ermittlungen wegen Landfriedensbruch begründet worden.[1561] Dabei wurden auch die Handy-Daten von Journalisten, Bundestagsabgeordneten wie jene der ansässigen Bürger inklusive Ärzte und Seelsorger erfasst. Rechtsgrundlage der nicht-individualisierte Funkzellenabfragen war § 100g Abs. 1 i.V.m. Abs. 2 S. 2 StPO, so dass es einem richterlichen Beschluss bedurfte, der auch erteilt wurde.

Die Abfragen wurden dennoch im Nachhinein überwiegend als unverhältnismäßig kritisiert.[1562] Zutreffend ist dies insbesondere im Hinblick auf die Tatsache, dass hier eine

---

[1556] Vgl. Nachw. oben in Fn. 508.
[1557] *Roßnagel* 2007, 117.
[1558] Etwa: BVerfGE 120, 274 (331); ausführlich dazu bereits oben, S. 99 f.
[1559] BVerfGE 125, 260 (336 f).
[1560] *Gieselmann,* heise online v. 26.6.2011, abrufbar unter: http://www.heise.de/-1268104.html.
[1561] Zweck waren „Strukturermittlungen" gegen eine kriminelle Vereinigung, *Wilkens,* heise online v. 12.9.2011, abrufbar unter: http://www.heise.de/-1341233.html; vgl. Nachw. in Fn. 1560.
[1562] http://www.saechsdsb.de/images/stories/sdb_inhalt/behoerde/oea/bericht-funkzellenabfragen.pdf; http://www.internet-law.de/2011/06/funkzellenuberwachung-bei-demonstration.html; https://www.bfdi.bund.de/bfdi_forum/archive/index.php/t-2437.html, In der Folge wurde unter an-

Demonstration, die durch die Versammlungsfreiheit einen besonderen verfassungsrechtlichen Schutz genießt, umfassend überwacht wurde.[1563]

Einen weiteren Skandal provozierte das Bekanntwerden des Einsatzes eines Trojaners zur Durchführung von Online-Durchsuchungen, dessen technische Fähigkeiten weit über das rechtlich erlaubte hinausgingen.[1564] Der *Chaos Computer Clu*b analysierte den Binärcode des Trojaners (der auch Bundes-, Bayern- oder Staats-Trojaner genannt wird) und zeigte auf, dass das Instrument eine deutlich umfassendere Online-Durchsuchung ermöglicht als offiziell bekannt war und verfassungsrechtlich zulässig ist.[1565] Zudem ist umstritten, ob es überhaupt eine Rechtsgrundlage für den Einsatz eines Trojaners im Rahmen strafrechtlicher Ermittlungen gibt. Zum Teil wird zwar angenommen, dass eine „Quellen-TKÜ", also eine Überwachung der IP-Telefonie, von § 100a StPO erfasst sei.[1566] Dagegen spricht aber, dass mit der „Infiltration" des Systems, selbst dann wenn sie allein zu Zwecken der IP-Telefonie-Überwachung erfolgt, eine Gefährdung des IT-Grundrechts einhergeht.[1567] Der Einsatz des Trojaners wurde richterlich genehmigt. Vor allem im Fall des Trojaner-Einsatzes wurde das Instrument über die richterliche Genehmigung hinaus (hier nämlich nur für die Überwachung der IP-Telefonie) genutzt.

Die Gründe mögen vielfältig sein, die Fälle zeigen jedoch, dass das zum Schutz der Bürgerrechte normierte Instrument des präventiven Richtervorbehalts in der Praxis vielfach versagt.[1568]

---

derem wurde ein Gesetzentwurf zur Eingrenzung von Funkzellenabfragen eingebracht; BT-Drs. 17/7033 v. 21.9.2011.

[1563] Auch im Zuge der Ermittlungen gegen massenweise Autobrandstiftungen in Berlin wurden mehrere Millionen Verkehrsdaten abgefragt. Diese Abfragen waren ebenfalls richterlich genehmigt (führten aber zu keinem Erfolg). Auch hier wurde das nicht zielgerichtete Vorgehen, Handeln der Polizei vielfach kritisiert, vgl. http://taz.de/Autobrandstiftung-in-Berlin/!86239/.

[1564] Dazu schon oben, S. 66.

[1565] http://ccc.de/de/updates/2011/staatstrojaner; So ermöglicht die Software neben der Überwachung von Skype-Telefonie und der Aufzeichnung und Übermittlung von Browser-Screenshots in regelmäßigen Zeitabständen es auch weitere Programme nachzuladen und diese ferngesteuert auszuführen. Grundsätzlich möglich ist auch das Manipulieren von Dateien oder aber der Zugriff auf Mikrophon und Kamera. Erhobene Daten werden zunächst an einen Server in den USA übermittelt. Dies ist aber in Anbetracht der fehlenden Rechtsgrundlage rechtlich betrachtet das kleinste Übel, denn für eine Onlinedurchsuchung fehlt es jenseits von § 20k BKAG, der allein das *–BKA* zur Durchführung von Online-Durchsuchungen ermächtigt, vielfach an einer Rechtsgrundlage, nur zum Teil findet sich eine Regelung in den Landespolizeigesetzen. Für strafverfolgungsrechtliche Ermittlungen fehlt es in der StPO gänzlich an einer Rechtsgrundlage, dazu ausführlich *Braun*, K&R 2011, 681, 682 f.

[1566] vgl. *LG Landshut*, 20.1.2011 – 4 Qs 346/10; *Braun* jurisPR-IR 3/2011 Anm. 3; *AG* Bayreuth, 17.9.2009 – Gs 911/09 – MMR 2010, 266, mit Anm. *Bär*, 267; LG Hamburg, 31.8.2010 – 608 Qs 17/10.

[1567] BVerfGE 120, 274.

[1568] In diesem Sinne auch *Biermann,* „Staatstrojaner: Rettet den Richtervorbehalt", Die Zeit v. 12.10.2011, abrufbar unter http://www.zeit.de/politik/deutschland/2011-10/trojaner-richtervorbehalt-2.

Auch in der rechtswissenschaftlichen Diskussion wird die Effektivität des Richtervorbehalts vielfach bezweifelt.[1569] Diagnostiziert werden „auffällige Diskrepanzen zwischen rechtsstaatlichem Anspruch und alltäglicher Justizwirklichkeit".[1570] So zeigte sich auch in einer empirischen Untersuchungen, dass wohl faktisch mehr kooperiert als kontrolliert wird.[1571]

In Bezug auf die Wirkungsmacht des Richtervorbehalts bei der präventiven Rasterfahndung wird kritisiert, dass die Richter zwar in richterlicher Unabhängigkeit handelten, sie könnten aber nicht ihrer typischen Funktion als Instanzen der unbeteiligten Streitentscheidung nachkommen, da sie entscheidend am Verfahren beteiligt sind. Daher könne der präventive Richtervorbehalt nicht die nachträgliche richterliche Kontrolle ersetzen.[1572]

Vorgeschlagen wird in der rechtswissenschaftlichen Diskussion, um die Wirkungskraft des Richtervorbehalts zu verbessern, dass höhere Begründungspflichten an einen stattgebenden richterlichen Beschluss zu einem Antrag der Staatsanwaltschaft zu stellen seien als an einen ablehnenden. „Begründungsbedürftig ist der Eingriff in die Rechte der Bürger, nicht derjenige in die Rechte der Staatsanwaltschaft. Daher stehen stattgebende Entscheidungen unter einem höheren Rechtfertigungsdruck als ablehnende Beschlüsse."[1573] Erforderlich sei es jedenfalls, dass diejenigen Gründe, aus welchen der Richter dem staatsanwaltschaftlichen Antrag stattgegeben hat, ausdrücklich genannt werden. Es müsste im richterlichen Beschluss dokumentiert werden, dass und wie der Richter den Antrag zum Gegenstand einer eigenständigen rechtlichen Prüfung gemacht hat.[1574]

Als wichtig wird sodann erachtet, dass die Erreichbarkeit der Richter verbessert wird und durch eine gezielte Fortbildung der Richter das zur Prüfung erforderliche technische Knowhow ausgebaut wird.[1575]

Denkbar ist auch entsprechend der Qualifizierung wie sie für die Anordnung einer akustischen Wohnraumüberwachung in Art. 13 Abs. 3 S. 3 GG vorgesehen ist, einen Mindeststandard für die Besetzung des Gerichts zu verlangen.[1576] Dies erscheint aber wenig geeignet den Rechtsschutz durch den Richtervorbehalt zu stärken – jedenfalls solange diese Anforderung nicht durch konkrete verfahrensrechtliche Vorschriften flankiert wird.[1577] Denn nur weil mehr Richter eine Anordnung unterschreiben müssen,

---

[1569] *Petri,* in: *Lisken/Denninger* 2012, G, Rn. 539; kritisch zur richterlichen Prüfung bei der präventiven Rasterfahndung *Lisken* NVwZ 2002, 513, 518; *Gusy,* ZRP 2003, 275.
[1570] *Gusy,* ZRP 2003, 275.
[1571] *Gusy,* ZRP 2003, 275; Die Ergebnisse zu einer empirischen Untersuchung zur Effektivität des Richtervorbehalts in der Praxis der Jahre 1996-1998, *Backes/Gusy* 2003, S. 44 ff., 77 ff., 91, 111, 123 f.
[1572] *Petri,* in: *Lisken/Denninger* 2012, G, Rn. 539; *Lisken,* NVwZ 2002, 523, 528; dazu auch *Welsing* 2009, 246.
[1573] *Gusy,* ZRP 2003, 275, 277
[1574] *Gusy,* ZRP 2003, 275, 277.
[1575] *Gusy,* ZRP 2003, 277.
[1576] *Kloepfer,* Verfassungsrecht II, 2010, § 51 Rn. 57.
[1577] *Gusy,* ZRP 2003, 275, 276 f.

wird dadurch die Kontrolle nicht zwangsläufig besser. Dies gilt insbesondere in Anbetracht der Überbelastung der Gerichte.

Auch das *Bundesverfassungsgericht* formuliert respektive der im Verfahren vorgebrachten Kritik an der Effektivität des Richtervorbehalts im Urteil zur Vorratsdatenspeicherung qualifizierte Anforderungen an dessen Ausgestaltung: „Der Gesetzgeber hat das Gebot vorbeugender richterlicher Kontrolle in spezifischer und normenklarer Form mit strengen Anforderungen an den Inhalt und die Begründung der gerichtlichen Anordnung zu verbinden. Hieraus folgt zugleich das Erfordernis einer hinreichend substantiierten Begründung und Begrenzung der Abfrage der begehrten Daten, die es dem Gericht erst erlaubt, eine effektive Kontrolle auszuüben. Erst auf dieser Grundlage kann und muss das anordnende Gericht sich eigenverantwortlich ein Urteil darüber bilden, ob die beantragte Verwendung der Daten den gesetzlichen Voraussetzungen entspricht. Dazu gehört eine sorgfältige Prüfung der Eingriffsvoraussetzungen einschließlich insbesondere der gesetzlich vorgeschriebenen Eingriffsschwelle. Der Anordnungsbeschluss des Gerichts muss gehaltvoll begründet werden. Überdies sind die zu übermittelnden Daten nach Maßgabe des Verhältnismäßigkeitsgrundsatzes hinreichend selektiv und in klarer Weise zu bezeichnen.“[1578]

Einvernehmlich mit den Anforderungen, die das Bundesverfassungsgericht formuliert hat und unter Berücksichtigung der in der rechtswissenschaftlichen Literatur entwickelten Optimierungsvorschläge, ist im Hinblick auf die vielfach fehlende Effektivität der ermittlungsrichterlichen Prüfung, der Richtervorbehalt beim Zugriff auf die Vorratsdaten zu qualifizieren. Erforderlich dafür ist eine Verbesserung der gerichtlichen Organisation, indem etwa jeweils spezifisch geschulte Ermittlungsrichter für die Abfrage von Telekommunikationsverkehrsdaten zuständig sind und deren Erreichbarkeit auch zu Nachtzeiten und an den Wochenenden sichergestellt ist. Sodann sind die Begründungs- und Dokumentationspflichten der Richter auszuweiten und zu konkretisieren.[1579] Wichtig ist, dass auch der Umfang des Datenabrufs richterlich voll überprüft wird.[1580] Zudem bedarf es, um sicherzustellen, dass tatsächlich gehaltvoll geprüft und begründet wird, spezifischer, normenklarer Bestimmungen zu den formalen Anforderungen.

Schließlich ist zu erwägen, ob nicht durch statistische Erhebungen über die Abfragepraxis und die Bedeutung der Abfragen für das weitere Verfahren, es ermöglicht wird die richterliche Praxis auch für die Öffentlichkeit transparent zu gestalten ohne die richterliche Unabhängigkeit zu gefährden.

9.1.2.1.4 Mittelbare Nutzung zur Bestandsdatenauskunft

Ein Eingriff in die Telekommunikationsfreiheit liegt auch dann vor, wenn lediglich mittelbar Verkehrsdaten zur Beauskunftung von Bestandsdatenabfragen genutzt werden. Eine solche mittelbare Nutzung ist vor allem im Bereich der Zuordnung dynamischer IP-Adressen zum Anschlussinhaber relevant. Dabei werden die auf Vorrat ge-

[1578] BVerfGE 125, 260 (338).
[1579] Ähnliche Vorschläge finden sich auch bei: *Gusy,* ZRP 2003, 275, 278.
[1580] Vgl. dazu oben S. 364 f.

speicherten Verkehrsdaten nicht an Ermittlungsbehörden herausgegeben, sondern es werden allein Bestandsdaten übermittelt nachdem die Telekommunikationsdiensteanbieter unter Rückgriff auf die Verkehrsdaten einen Anschlussinhaber identifiziert haben. Das *Bundesverfassungsgericht* hat eine „mittelbare Verwendung" der Vorratsdaten für Bestandsdatenauskünfte unter geringeren Voraussetzungen als zulässig erachtet.[1581] Der Vorratsdatenspeicherungsrichtlinie selbst lässt sich keine ausdrückliche Aussage dazu entnehmen, ob eine mittelbare Verwendung von auf Vorrat gespeicherten Daten auch zur Verfolgung niederschwelliger Delikte zulässig sein soll.

Das *Bundesverfassungsgericht* argumentiert, dass eine behördliche Auskunft zu einem Inhaber einer bestimmten IP-Adresse an weniger hohe Anforderungen geknüpft werden könne, da die Behörden hier selbst gar keine Kenntnisse der vorsorglich gespeicherten Daten erhalten würden.[1582] Ihnen würde in dieser Konstellation lediglich ein Bestandsdatum übermittelt, das unter Verwendung der auf Vorrat gespeicherten Verkehrsdaten ermittelt wurde. Zudem sei die Aussagekraft der Daten „eng begrenzt", da sie nur die Auskunft beinhalte, welcher Anschlussinhaber im Internet angemeldet war. Eine solche Auskunft habe eine gewisse Ähnlichkeit mit der Abfrage des Inhabers einer Telefonnummer. Ihr Erkenntniswert bleibe „punktuell". Da an diesen Informationen über die Kommunikationsteilnehmer im Internet aber ein gesteigertes Interesse zum Rechtsgüterschutz und zur Wahrung der Rechtsordnung bestünde, sei es der Gestaltungsfreiheit des Gesetzgebers überlassen, ob eine mittelbare Nutzung der auf Vorrat gespeicherten Verkehrsdaten zu weitergehenden Zwecken zugelassen wird. Dementsprechend könne der Gesetzgeber solche Auskünfte „auch unabhängig von begrenzenden Rechtsgüter- oder Straftatenkatalogen" für die Verfolgung von Straftaten, für die Gefahrenabwehr und die Aufgabenwahrnehmung der Nachrichtendienste auf der Grundlage der allgemeinen fachrechtlichen Eingriffsermächtigungen zulassen.[1583] Auch sei hier eine richterliche Prüfung entbehrlich.[1584]

Gegen diese Argumentation wird vorgebracht, dass sie zu Wertungswidersprüchen führe, wenn die Identifizierung anhand einer (dynamischen) IP-Adresse unter geringeren Anforderungen erfolgen könnte, als wenn auf andere auf Vorrat gespeicherte Verkehrsdaten zurückgegriffen werde: So dürfe bei einem Anruf „mit unterdrückter Rufnummer zu einer bekannten Uhrzeit" der Anschluss der unterdrückten Nummer nur mit richterlicher Anordnung und bei Vorliegen der Voraussetzungen des § 100g StPO identifiziert werden („Zielwahlsuche").[1585] Entsprechend könne, wenn ein anonymer Anruf über Internet-Telefonie (z.B. Skype) erfolgt, der Anrufer mittels bekannter Verbindungsdaten (IP-Adresse, Zeit) und ohne eine richterliche Anordnung identifiziert werden. Zulässig sei dies bereits zur Aufklärung des Verdachts einer „erheblichen"

[1581] BVerfGE 125, 260 (340).
[1582] BVerfGE 125, 260 (340).
[1583] BVerfGE 125, 260 (341).
[1584] BVerfGE 125, 260 (344).
[1585] http://www.daten-speicherung.de/index.php/scharfe-kritik-an-urteil-des-bundesverfassungsgerichts-zur-vorratsdatenspeicherung/

Ordnungswidrigkeit oder Bagatellstraftat zulässig sein.[1586] Eine Gleichbehandlung sei nur möglich, wenn sie stets als Eingriff in das Telekommunikationsgeheimnis gewertet würden und diese Einordnung eben nicht von der Art des genutzten Telekommunikationsmittels abhängig gemacht würde.[1587]

Diese Argumentation überzeugt besonders, wenn man bedenkt, dass ebenfalls nach Rechtsprechung des *Bundesverfassungsgerichts* die Zuordnung einer Telekommunikationsnummer zu ihrem Anschlussinhaber „nur" ein Eingriff in die informationelle Selbstbestimmung ist, während die Zuordnung einer IP-Adresse zum Anschlussinhaber einen Eingriff in das Telekommunikationsgeheimnis bedeutet.[1588]

Dennoch lässt sich fragen, ob der Gesetzgeber nicht auch die Differenzierung nach Art des genutzten Telekommunikationsmittels vornehmen kann: Weder kann ein Abruf eines Bestandsdatums zu einer IP-Adresse mit einer Telefonnummernabfrage gleichgesetzt werden, noch kann insgesamt klassische Telekommunikation mit der Kommunikation über das Internet gleich gesetzt werden. Das Interesse, IP-Adressen zuzuordnen, ist aus sicherheitspolitischer Perspektive zudem deutlich höher.

Dies ändert aber nichts daran, dass es sich faktisch um einen Eingriff in das Telekommunikationsgeheimnis handelt. Zudem ermöglicht die Abfrage des Anschlussinhabers zu einer IP-Adresse vielfach sogar Rückschlüsse auf die inhaltliche Kommunikation. Es handelt sich insofern auch wenn es sich nur um eine punktuelle Auskunft handelt um einen schwerwiegenden Eingriff.[1589] Dieser schwerwiegende Eingriff in das Telekommunikationsgeheimnis verlangt eine entsprechende Rechtfertigung.[1590]

Zudem gilt es zu berücksichtigen, dass die Auskunft nur ermöglicht wird durch die anlasslose flächendeckende Speicherung sämtlicher Verkehrsdaten. Diese Speicherungsverpflichtung wiegt schon von sich aus besonders schwer und darf nur zu entsprechend hochrangigen Zwecken erfolgen. Eine besonders strenge Achtung des Zweckbindungsgrundsatzes ist aber gerade bei der Vorratsdatenspeicherung geboten, da diese Konstruktion ansonsten den Zweckbindungsgrundsatz gänzlich aufzuweichen

---

[1586] Ähnliches gilt bei dem Vergleich von Fax und E-Mail-Versand: „Sendet jemand ohne Rufnummernübermittlung ein Telefax, so darf seine Anonymität im Wege einer Zielwahlsuche nur mit richterlicher Anordnung nach Maßgabe des § 100g StPO aufgehoben werden. Wird dasselbe Dokument dagegen über ein anonymes E-Mail-Postfach versandt, so soll die Identifizierung des Anschlussinhabers anhand der verwendeten IP-Adresse ohne richterliche Anordnung und bereits zur Aufklärung des Verdachts einer „erheblichen" Ordnungswidrigkeit oder Bagatellstraftat zulässig sein. Die Privilegierung einer Internet-Zielwahlsuche gegenüber einer Telefon-Zielwahlsuche ist sachlich nicht zu rechtfertigen. Auch ist nicht plausibel zu machen, weshalb unbedeutende Verkehrsdaten zu schon bekannten Verbindungen (z.B. Datenvolumen, genaue Anrufdauer) einen besseren Schutz genießen sollen als die äußerst grundrechtsbedeutsame Identität eines noch unbekannten Kommunikationsteilnehmers", so *Breyer*, NJW aktuell 2010, 12.

[1587] http://www.daten-speicherung.de/index.php/scharfe-kritik-an-urteil-des-bundesverfassungsgerichts-zur-vorratsdatenspeicherung/

[1588] Beschl. v. 24.1.2012 - 1 BvR 1299/05; LS 1.

[1589] *Breyer*, NJW aktuell 2010, 12

[1590] Vgl. oben S. 272 ff.

droht.[1591] Bei einer mittelbaren Verwendung der Verkehrsdaten zur Auskunft eines Bestandsdatums werden zwar keine Vorratsdaten übermittelt, sie werden aber verwendet. Auch hier ist der Zweckbindungsgrundsatz zu beachten. Dieser würde konterkariert, wenn die Daten zu anderen Zwecken verwendet werden als jene für die sie gespeichert wurden.

Hinzukommt, dass − sollte eine derartige Ausnahme zugelassen werden − sich in der Praxis wohl die Mehrheit der Anfragen auf die Auskunft über Anschlussinhaber einer dynamischen IP-Adresse beziehen würde und somit auf die Verfolgung niederschwelliger Delikte und der Verfolgung zivilrechtlicher Ansprüche, wodurch die Akzeptanz eine Vorratsdatenspeicherung voraussichtlich stark beeinträchtigt würde. Eine mittelbare Verwendung von Vorratsdaten für zivilrechtliche Ansprüche und für niederschwellige Delikte ist daher zu untersagen.[1592]

9.1.2.1.5 Vereinbarkeit mit europäischen Grundrechten?

Die Verpflichtung zur Speicherung der Umstände jedweder Telekommunikationsverbindung auf Vorrat greift in den Schutz der Kommunikationsfreiheit ein, der europarechtlich durch Art. 8 EMRK und Art. 7 EU-GRCh. gewährleistet wird.[1593] Der Eingriff kann gerechtfertigt werden, soweit er „gesetzlich vorgesehen und in einer demokratischen Gesellschaft notwendig ist für die nationale oder öffentliche Sicherheit, für das wirtschaftliche Wohl des Landes, zur Aufrechterhaltung der Ordnung, zur Verhütung von Straftaten, zum Schutz der Gesundheit oder der Moral oder zum Schutz der Rechte und Freiheiten anderer".[1594]

Als Unionsrechtsakt handelt es sich bei der Vorratsdatenspeicherungsrichtlinie um eine taugliche Grundrechtsschranke,[1595] das gleiche gilt für einen nationalen Rechtsakt, der zu einer Vorratsdatenspeicherung verpflichtet. Es bestehen jedoch Bedenken,[1596] ob eine Vorratsdatenspeicherung auch verhältnismäßig ist. Im Rahmen der Verhältnismäßigkeit prüft der *Europäischen Gerichtshofs für Menschenrechte* (ganz ähnlich der deutschen Verhältnismäßigkeitsprüfung) die „Notwendigkeit" des Eingriffs. Die

[1591] Die vom *Bundesverfassungsgericht* zugelassene Ausnahme stellt insoweit eine unsystematische Aufweichung des Zweckbindungsgrundsatzes dar, vgl. oben S. 139 ff.

[1592] A.a. BVerfGE 125, 260 (340 ff.); jedenfalls wäre auch wenn man der Argumentation des Verfassungsgerichts folgen sollte und eine mittelbare Verwendung unter geringeren Voraussetzungen als zulässig erachten sollte, aus Gründen eines optimierten Interessenausgleichs dies zu unterbinden, vgl. oben S. 281 f.

[1593] Vgl. dazu schon oben S. 100 f.

[1594] Art. 8 Abs. 2 EMRK.

[1595] *Derksen* 2011, 13.

[1596] Es wird in Bezug auf die VDS-RL auch kritisiert, dass die Richtlinie zu unbestimmt sei, da sie nicht definiere welche Behörden Zugriff auf die Daten haben sollen. *Westphal* zielt mit dieser Kritik aber vor allem darauf, dass so eine Harmonisierung nicht erreicht werden könne. *Westphal,* EuR 2006, 706, § 716. Da diese Kritik aber nicht für die Bestimmung der grundrechtlichen Anforderungen an die Vorratsdatenspeicherung relevant ist, soll sie hier auch nicht näher erörtert werden.

Prüfung der Geeignetheit steht an ihrer Spitze. In ihrem Zentrum steht die Prüfung der Angemessenheit.[1597]

Eine Vorratsdatenspeicherung verfolgt auch im Sinne der europäischen Grundrechtsjurisdiktion mit dem Ziel Sicherheit zu erzeugen und Straftaten zu bekämpfen, ein legitimes Ziel.[1598] Auch ist sie dafür geeignet.[1599] In Bezug auf die Beurteilung der Notwendigkeit billigt der *Europäische Gerichtshof für Menschenrechte* den Vertragsstaaten einen großen Beurteilungsspielraum zu.[1600] In der Entscheidung *Klass* betont das Gericht, dass dies nicht bedeutet „dass (…) die Vertragsstaaten hätten ein unbegrenztes Ermessen (latitude illimitée / unlimited discretion), Personen innerhalb ihres Hoheitsbereichs geheimer Überwachung zu unterwerfen. Im Bewusstsein der Gefahr, die ein solches Gesetz in sich birgt, nämlich die Demokratie mit der Begründung, sie zu verteidigen, zu untergraben oder sogar zu zerstören, bekräftigt der Gerichtshof, dass die Vertragsstaaten nicht im Namen des Kampfes gegen Spionage und Terrorismus zu jedweder Maßnahme greifen dürfen, die ihnen geeignet erscheint."[1601]

In Bezug darauf fragt *Dix,* ob nicht gerade in Anbetracht dessen, die Vorratsdatenspeicherung mit den europäischen Grundrechtsgewährleistungen unvereinbar sei.[1602] Zwar liege dem Fall *Klaas,* anders als im Fall einer Vorratsdatenspeicherung, eine inhaltliche und heimliche Überwachung der Telekommunikation zu Grunde. Aber schließlich habe auch das *Bundesverfassungsgericht* anerkannt, dass der Eingriff durch eine Verpflichtung zur Vorratsspeicherung der Telekommunikationsverkehrsdaten nicht grundsätzlich geringer wiege.[1603] Auf Grund dessen fragt er, ob die Vorratsdatenspeicherung „zwingend notwendig in einer demokratischen Gesellschaft" sei. Ihre Nützlichkeit sei nicht zu bestreiten. Unter Hinweis auf die Studie des Max-Planck-Instituts[1604] betont er aber, dass es an Nachweisen dafür fehle, dass die Strafverfolgung und Gefahrenabwehr ohne Vorratsdatenspeicherung erheblich erschwert werde. Zudem berge die Vorratsdatenspeicherung neue Sicherheitsrisiken.[1605] Die anlassunabhängige Speicherung der Verkehrsdaten sei jedenfalls nicht zwingend erforderlich in einer demokratischen Gesellschaft.[1606]

Allerdings bleibt zu berücksichtigen, dass der *Europäische Gerichtshof für Menschenrechte* an sich nicht derart detailliert prüft, sondern den Mitgliedstaaten einen weiten

---

[1597] *Grabenwarter/Pabel* 2011, §§ 18 Rn. 14 ff.
[1598] Art. 8 Abs. 2 EMRK nennt als legitime Ziele die nationale oder öffentliche Sicherheit, das wirtschaftliche Wohl des Landes, die Aufrechterhaltung der Ordnung, die Verhütung von Straftaten, den Schutz der Gesundheit oder der Moral oder zum Schutz der Rechte und Freiheiten anderer.
[1599] Auch in der europäischen Grundrechtsdogmatik genügt eine abstrakte Eignung. Zum gleichen Ergebnis kommt auch *Derksen* 2011, 15.
[1600] *Grabenwarter/Pabel* 2011, §§ 18 Rn. 20.
[1601] *EGMR*, Urt. v. 6.9.1978, *Klaas ./. Deutschland* EGMR-E I, 320, 334 Rn. 48.
[1602] *Dix* 2012.
[1603] BVerfGE 125, 260 (283); so *Dix* 2012, 4.
[1604] Vgl. zu dieser oben S. 192 ff.
[1605] *Dix* 2012, 7 f.; vgl. auch zu den Missbrauchsrisiken, oben S. 184 f.; vgl. auch BVerfGE 125, 260 (320).
[1606] *Dix* 2012, 5; Vgl. oben S. 203 ff.

Gestaltungsspielraum belässt. Dennoch kann mit *Dix* die Vereinbarkeit der Vorratsdatenspeicherung mit der Europäischen Menschenrechtskonvention bezweifelt werden.

9.1.2.1.6 Zwischenergebnis

Da es sich jedenfalls um einen besonders schweren Eingriff handelt, muss dies entsprechend in der Normierung der Vorschriften, die zur Datenspeicherung verpflichten sowie jenen über die Datenverwendung adäquat zum Ausdruck kommen. Das heißt, dass die Vorratsdatenspeicherung so ausgestaltet sein muss, dass sie zum einen geeignet ist, das Regelungsziel zu fördern und zum anderen so, dass die Schwere des Eingriffs mit rechtlichen, technischen und organisatorischen Instrumenten begrenzt wird.

9.1.2.2 Recht auf informationelle Selbstbestimmung

Im Rahmen der Speicherung sämtlicher Telekommunikationsverkehrsdaten auf Vorrat steht im Zentrum nicht unmittelbar die Telekommunikation, sondern die Verarbeitung von Daten, die sich auf die Umstände von Telekommunikationsverbindungen beziehen. Diese Verkehrsdaten sind personenbezogene Daten, so dass das Recht auf informationelle Selbstbestimmung grundsätzlich einschlägig ist. Allerdings enthält Art. 10 GG bezüglich Telekommunikationsverkehrsdaten die speziellere Garantie als das durch Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG garantierte Recht auf informationelle Selbstbestimmung, so dass dies nicht zur Anwendung kommt.[1607] Allerdings sind aufgrund des datenschutzrechtlichen Gehalts des Telekommunikationsgeheimnisses, die Erwägungen zum informationellen Selbstbestimmungsrecht mit einzubeziehen.[1608] Daran würde sich auch durch die Verabschiedung einer Datenschutz-Grundverordnung, wie sie im Januar 2012 vorgestellt wurde, nichts ändern.[1609]

Für eine verhältnismäßige Ausgestaltung einer Vorratsdatenspeicherung heißt das, dass die datenschutzrechtlichen Grundprinzipien (Zweckbindungsgrundsatz, Grundsatz der Erforderlichkeit, der Grundsatz der Datensparsamkeit und Datenvermeidung, Transparenz) zu beachten sind.

9.1.2.3 Unschuldsvermutung

Da von einer Verpflichtung zur Speicherung sämtlicher Telekommunikationsverkehrsdaten auf Vorrat unterschiedslos jeder Bürger betroffen ist, wird argumentiert, dass sie die Unschuldsvermutung verletze.[1610]

Im Grundgesetz ist die Unschuldsvermutung nicht ausdrücklich normiert. Sie ist jedoch im Rechtsstaatsprinzip verankert[1611] und als solches auch mit Verfassungsrang

---

[1607] BVerfGE 125, 260 (310).

[1608] BVerfGE 125, 260 (310); zum Gewährleistungsgehalt des Rechts auf informationelle Selbstbestimmung, ausführlich schon oben Kap. 2.1.3.1.

[1609] Vgl. dazu oben Kap. 2.1.3.1.4.2, S. 91 f.

[1610] So etwa *Puschke/Singelnstein*, NJW 2008, 113, 118; Auch wurde in der Vergangenheit vertreten, dass ein grundsätzliches Misstrauen gegen den Bürger und seine Rechtstreue ohne konkrete, einzelfallbezogene Anhaltspunkte mit der Menschenwürde als oberstem Wert unserer Verfassung nicht vereinbar sei, so *Hund*, NJW 1992, 2118, 2119 immer wieder auch der AK-Vorrat, dazu etwa http://www.vorratsdatenspeicherung.de/content/view/22/49/lang,de/; ebenso aus der politischen Diskussion etwa http://sozis-gegen-vds.de/argumente.

versehen. Zum Teil wird die Unschuldsvermutung aus der Menschenwürdegarantie hergeleitet.[1612] Das *Bundesverfassungsgericht* hat sie als im Rechtsstaatsprinzip verwurzelt anerkannt.[1613] Positiv im Rang eines einfachen Gesetzes ist sie ins deutsche Recht durch Art. 6 Abs. 2 EMRK i. V. m. Art. 59 Abs. 2 GG eingeführt.[1614]

Die Unschuldsvermutung enthält das subjektive Recht, dass bis zur Schuldspruchreife keine strafprozessualen Entscheidungen getroffen werden dürfen, die mit Feststellungen zur Schuld begründet werden.[1615] Der Einzelne gilt (im Strafverfahren) als unschuldig bis seine Schuld bewiesen ist. Das heißt, der Bürger darf bis er als schuldig verurteilt wurde, weder so bezeichnet noch so behandelt werden.[1616]

Die Wirkung der Unschuldsvermutung ist allerdings nicht nur darauf beschränkt. Sie ist auch grundlegend für den Aufbau von Ermittlungs- und Strafverfahren. Ein Ermittlungsverfahren darf grundsätzlich erst bei einem Anfangsverdacht gegen eine bestimmte Person eingeleitet werden.[1617]

Zwar werden mittlerweile auch sogenannte Vorfeldermittlungen durchgeführt.[1618] In diesem Stadium sucht die Polizei einen Anfangsverdacht**,** um erst dann nach der Strafprozessordnung weiter zu verfahren.[1619] Diese Aktivitäten werden von Polizeibehörden vor allem in den Sektoren Betäubungsmittelkriminalität und Organisierte Kri-

---

[1611] *Hofmann* in *Schmidt-Bleibtreu/Klein*, GG 2011, Art. 20 Rn. 63.

[1612] So u.a. *Degener*, 1985, 213 f. (der sie als strafprozessuale Ausprägung von Art. 1 Abs. 1 GG begreift); *Meyer* in: FS Tröndle 1989, 61, 62; *Vogler* 1985, 436; *Sommermann* sieht sie schwerpunktmäßig in Art. 1 GG verortet (materielle Rechtsstaatlichkeit), in *Mangoldt/Klein/Starck* 2010, Art. 20, Rn. 324; zur materiellen Rechtsstaatlichkeit Rn. 238; Sie weist jedenfalls einen sehr engen Bezug zur Menschenwürdegarantie auf und wird so auch durch Art. 1 Abs. 1 GG gewährleistet.

[1613] Siehe vor allem schon BVerfGE 19, 342 (347); spricht von Unschuldsvermutung und wirksamer Strafverfolgung als zwei gleich wichtigen Prinzipien des Rechtsstaats; vgl. dazu auch BVerfGE 35, 185 (190); 53, 152 (158); 115, 166 (192): „Die Sicherung des Rechtsfriedens durch Strafrecht ist seit jeher eine wichtige Aufgabe staatlicher Gewalt. Die Aufklärung von Straftaten, die Ermittlung des Täters, die Feststellung seiner Schuld und seine Bestrafung wie auch der Freispruch des Unschuldigen sind die wesentlichen Aufgaben der Strafrechtspflege, die zum Schutz der Bürger den staatlichen Strafanspruch in einem justizförmigen und auf die Ermittlung der Wahrheit ausgerichteten Verfahren in gleichförmiger Weise durchsetzen soll." Siehe auch BVerfGE 61, 28 (32) für den Auslieferungshaftbefehl; vgl. dazu auch *Grabitz*, in: *Isensee*/*Kirchof*, HStR VI, § 130, Rn. 40; *Sommermann* in *Mangoldt/Klein/Starck,* GG 2010, Art. 20, Rn. 324

[1614] *Grawert* in HGR III, 2009, § 81, Rn. 61; so auch *VG Lüneburg* v. 21. 2. 2006, 3 A 141/04, abgedr. in NVwZ-RR 2006, 542, 543; auch ist sie in mehreren Landesverfassungen verankert, z.B. in Art. 20 Abs. 2 HV.

[1615] *Di Fabio,* in: *Maunz/Dürig*, GG 2011, Art. 2, Rn. 69.

[1616] *Eser* in *Meyer*, EU-GRCh. 2003, Art. 48, Rn. 5; BVerfGE 19, 342 (347); 74, 358 (370); Sie verbietet es, gegen den Beschuldigten im Vorgriff auf die Strafe Maßregeln zu verhängen, die in ihrer Wirkung der Freiheitsstrafe gleichkommen, so BVerfGE 35, 311 (320) dazu auch *Graf,* StPO 2011, Vorbem. Rn. 8.

[1617] Pflicht zur Erforschung der Wahrheit setzt erst mit dem Vorliegen von „zureichenden tatsächlichen Anhaltspunkten", § 152 Abs. 2StPO ein.

[1618] Vorfeldermittlungen setzen dort an, wo weder eine konkrete Straftat noch eine konkrete Gefahr gegeben sind; dazu ausführlich *Lange* 1999, 23 ff.

[1619] *Hellebrand* 1999, Rn. 21; Führt aus, dass diese Ermittlungen im BtM-Bereich und zur Bekämpfung der organisierten Kriminalität besonders wichtig seien.

minalität als besonders wichtig erachtet, da es hier nur wenige Anzeigen und kaum Zufallserkenntnisse gibt.[1620] Allerdings ist ihre rechtliche Problematik insbesondere im Hinblick auf eine Verletzung der Unschuldsvermutung bislang noch weitgehend ungeklärt.[1621] Die Frage der Vereinbarkeit von Vorfeldermittlungen mit der Unschuldsvermutung kann hier aber offen bleiben. Denn die Vorratsdatenspeicherung unterscheidet sich von diesen, da es sich bei ihr um eine Maßnahme der so genannten Strafverfolgungsvorsorge handelt und nicht um Vorfeldermittlungen. Ziel der Vorratsdatenspeicherung ist die Beweisbeschaffung für ein eventuell in der Zukunft einzuleitendes Ermittlungsverfahren und nicht, Ermittlungen zu führen, um einen Verdacht zu begründen.

Nichtsdestotrotz kann ein gewisses Spannungsverhältnis zwischen einer Verpflichtung zur Vorratsdatenspeicherung und der Unschuldsvermutung nicht von der Hand gewiesen werden. Denn die Vorratsspeicherung der Telekommunionsverkehrsdaten widerspricht insoweit der Unschuldsvermutung, als hier vollkommen unabhängig von einem Anlass in das Telekommunikationsgeheimnis eingegriffen wird.[1622] Damit wird aber nicht generell die Unschuldsvermutung untergraben.

Soweit gewährleistet wird, dass ein Zugriff der Strafverfolgungsbehörde auf die Daten erst möglich ist, wenn ein Anfangsverdacht besteht, wird das Grundprinzip, dass in die Freiheitsrechte der Bürger nur dann eingegriffen werden darf, wenn es einen Anlass dazu gibt, jedoch nicht (vollkommen) ausgehöhlt. Denn der in der Speicherung liegende Eingriff bleibt punktuell und ist nicht an Ermittlungsmaßnahmen geknüpft. Die Verwertung der Daten erfolgt damit erst, wenn ein Verdacht vorliegt. Wesentlich im Hinblick auf die Unschuldsvermutung ist damit, dass die Speicherung nicht durch den Staat erfolgt und dieser auch keinen direkten Zugriff auf die Daten erhält, sowie die Vorratsspeicherung von Telekommunikationsverkehrsdaten nur als eine Ausnahme von den sonstigen an einen Verdacht geknüpften Ermittlungsmaßnahmen der StPO möglich ist.

Ein Verstoß gegen die Unschuldsvermutung, scheidet zudem aus, da in der Speicherung keine Aussage über die Schuld oder Strafbarkeit einer Person zu erkennen ist. Zwar können auch gesetzliche Bestimmungen unter bestimmten Voraussetzungen die Unschuldsvermutung verletzen.[1623] Eine Vorschrift, die lediglich die Speicherung von Daten für eine spätere Verwendung zu Beweiszwecken anordnet, enthält jedoch noch

---

[1620] *Pfeiffer* in KarlsruherKomm StPO, 2008, Einleitung, Rn. 34.

[1621] *Pfeiffer* in KarlsruherKomm StPO, 2008, Einleitung, Rn. 34; dazu auch *Hellebrand* 1999, Rn. 204; Das *BVerfG* hat Vorfeldermittlungen im Bereich des Staatsschutzes zur Abwehr verfassungsfeindlicher Bestrebungen als verfassungskonform anerkannt, BVerfGE 30, 1 (29); generell zu Vorfeldermittlungen allg. *Lange* 1999; *Weßlau* 1989.

[1622] So führt etwa *Orantek* aus, dass bei der Vorratsdatenspeicherung alle Bürger unter „Generalverdacht" gestellt würden, *Orantek*, NJ 2010, 193, 195; zum Merkmal der Anlasslosigkeit in Abgrenzung zu verdachtsunabhängigen Maßnahmen wie Rasterfahndung oder Kfz-Kennzeichenscanning, vgl. oben S. 233.

[1623] *Frowein/Peukert*, EMRK 2009, Art. 6 Rn. Rn. 264, so der *EGMR* Bezüglich einer Regelung, die Erben für Steuerhinterziehungen des Erblassers strafrechtlich zur Verantwortung zog (*E.P., M.P. und T.P. ./. Schweiz,* Rs. 19958/1997-V, Rn. 45).

keine (abschließende) strafrechtliche Einordnung von Handlungen der Personen, deren Daten gespeichert werden. Auch der Abruf stellt noch keine Verletzungshandlung dar, denn die Abrufanordnung selbst beinhaltet als bloße Ermittlungsmaßnahme noch nicht die Äußerung, dass eine bestimmte Person eine konkrete Straftat begangen habe.[1624] Eine Verpflichtung zur Vorratsspeicherung der Telekommunikationsverkehrsdaten verletzt somit nicht die Unschuldsvermutung.

9.1.2.4 Schutz von Vertrauensbeziehungen

Die Vorratsdatenspeicherung erfasst grundsätzlich auch die unter Vertraulichkeitserwägungen aufgenommenen Telekommunikationsverbindungen. Vertrauensbeziehungen genießen jedoch – auch via Telekommunikation – verfassungsrechtlich einen besonderen Schutz.

9.1.2.4.1 Schutzbereich der Berufsfreiheit

Art. 12 GG schützt die Berufsfreiheit. Diese wird in die Freiheit der Berufswahl und in die Freiheit der Berufsausübung unterteilt. Die Berufsfreiheit umfasst auch den Schutz der Berufsausübungsfreiheit von Berufsgeheimnisträgern.[1625]

Beruf im Sinne des Art. 12 Abs. 1 GG ist jede auf Dauer angelegte Tätigkeit zur Schaffung und Erhaltung einer Lebensgrundlage. Eingriffe sind als imperative oder faktische Beeinträchtigungen denkbar.[1626] Die Berufsfreiheit schützt allerdings „nur vor solchen Beeinträchtigungen, die gerade auf die berufliche Betätigung bezogen sind. Es genügt also nicht, dass eine Rechtsnorm oder ihre Anwendung unter bestimmten Umständen Rückwirkungen auf die Berufstätigkeit zulässt. Art. 12 Abs. 1 GG entfaltet seine Schutzwirkung nur gegenüber solchen Normen oder Akten, die sich entweder unmittelbar auf die Berufstätigkeit beziehen oder die zumindest eine objektiv berufsregelnde Tendenz haben“.[1627]

Allerdings kann, so das *Bundesverfassungsgericht,* „der besondere Freiheitsraum, den das Grundrecht der Berufsfreiheit sichern will, (…) auch durch Vorschriften ohne primär berufsregelnde Zielrichtung (…) berührt sein, wenn ihre tatsächlichen Auswirkungen zu einer Beeinträchtigung der freien Berufsausübung führen“.[1628] Dafür muss die grundrechtlich geschützte Tätigkeit nicht ganz oder teilweise unterbunden werden, vielmehr genügt es, „dass sie auf Grund der staatlichen Maßnahmen nicht mehr in der gewünschten Weise ausgeübt werden kann“.[1629]

Die Berufsfreiheit von Ärzten, Priestern, Psychologen, Therapeuten und Anwälten (alle in § 203 Abs. 1 StGB erwähnten Berufe) verlangt die Achtung der Vertraulichkeit

[1624] Auch die öffentliche Erhebung eines Tatverdachts kann nicht generell als Verletzung der Unschuldsvermutung angesehen werden kann, *Eser* in *Meyer*, EU-GRCh. 2003, Art. 48, Rn. 7.

[1625] Das *BVerfG* hat den normativen Schutz solcher Vertrauensverhältnisse in doppelter Hinsicht verfassungsrechtlich fundiert, zum einen im Persönlichkeitsrecht des Bürgers, seinem Anspruch auf Achtung seines privaten Bereichs zum anderen im Grundrecht des jeweiligen Berufsträgers auf freie Berufsausübung; *Ignor*, NJW 2007, 3403, 3404.

[1626] *Ruffert,* in: BeckOK, 2010, Art. 12 GG, Rn. 1.

[1627] *BVerfG* NJW 2007, 2749 unter Verweis auf vgl. BVerfGE 95, 267 (302); 97, 228 (253 f.).

[1628] BVerfGE 13, 181 (185 f.); 36, 47 (58); 61, 291 (308 f.); 110, 226 (254).

[1629] BVerfGE 82, 209 (223); siehe auch BVerfGE 86, 28 (37); dazu *Scholz,* in: *Maunz/Dürig,* GG 2011, Art. 23 Rn. 301.

des Verhältnisses zu ihren Patienten, Klienten und Mandanten. Auch aus deren Perspektive besteht ein Anspruch auf Schutz des Vertrauensverhältnisses durch einzelne Freiheitsrechte wie der Religionsfreiheit (Art. 4 Abs. 1 GG), die allgemeine Handlungsfreiheit (Art. 2 Abs. 1 GG) oder der Kernbereich privater Lebensgestaltung (Art. 1 Abs. 1 GG).

Ins Gewicht fällt bei der Kommunikation mit Geheimnisträgern, dass sich hier schon unmittelbar aus den Umständen der Kommunikation Rückschlüsse auf den Inhalt ziehen lassen.[1630] Die Speicherung von Inhaltsdaten ist jedoch verfassungswidrig und wird zudem von Art. 1 Abs. 2 Satz 2 VDS-RL untersagt. Letztlich können auch Daten als Inhaltsdaten verstanden werden, die lediglich Aufschluss über den Inhalt eines Kommunikationsvorgangs ermöglichen. Insofern wird ein Verbot der Speicherung der Verkehrsdaten von besonderen Vertrauensbeziehungen schon durch das Verbot der Speicherung von Inhalten erfasst.

Regelungen über die Speicherung von Telekommunikationsverkehrsdaten zielen nicht primär darauf, die Berufsfreiheit von Berufsgeheimnisträgern zu beeinträchtigen. Ziel der Speicherungsverpflichtung ist es, die Daten über den Telekommunikationsverkehr zu Zwecken der Strafverfolgung und Gefahrenabwehr zu speichern. Sie hat somit zwar keinen unmittelbaren Bezug zur Berufstätigkeit der Berufsgeheimnisträger, jedoch kann eine Vorratsdatenspeicherung die Berufsausübungsfreiheit von Berufsgeheimnisträgern beeinträchtigen. Schließlich werden hier vertrauliche Daten gespeichert werden, die dem Geheimnis- und Mandantenschutz unterliegen. Zudem ist ein Bezug zur Berufstätigkeit gegeben, wenn die Vorratsdatenspeicherung tatsächlich dazu führen sollte, dass die Kommunikationspartner von Berufsgeheimnisträgern auf die Kommunikation via Telefon oder E-Mail verzichten. Dann wäre es etwa Telefonberatungsstellen, Psychologen, Anlaufstellen für Krisensituationen, (spezialisierten) Medizinern und anderen nicht mehr möglich, ihren Beruf in der gewünschten Weise auszuführen.

Für die Anbieter und Mitarbeiter anonymer Telefonseelsorge, Suchtberatungsstellen oder anderer Beratungseinrichtungen ist das Risiko einer Verletzung der Berufsfreiheit besonders wahrscheinlich, da ihr Angebot auf dem Grundsatz der Anonymität aufbaut.

Beispielsweise wird eine anonyme Telefonseelsorge von den katholischen und evangelischen Kirchen angeboten.[1631] Die Mitarbeiter der Telefonseelsorge sind in der Mehrheit ehrenamtlich tätig. Die ehrenamtliche Betätigung wird zwar nicht durch Art. 12 Abs. 1 GG geschützt.[1632] Es gibt jedoch auch hauptberufliche Mitarbeiter und es erscheint möglich, dass durch eine Vorratsspeicherung der Telekommunikationsverkehrsdaten, die auch die Verbindungen zur Telefonseelsorge erfassen, das Vertrauen in die Anonymität der Telefonseelsorge so stark beeinträchtigt wird, dass im Ergebnis deutlich weniger Menschen auf das seelsorgerische Angebot zurückgreifen. Das könnte dazu führen, dass weniger Mitarbeiter benötigt werden. Dann würde die Berufsfreiheit sogar ganz unterbunden. Dies ist für einen Eingriff in Art. 12 Abs. 1 GG nicht

[1630] So auch BVerfGE 125, 260 (319); Darüber hinaus stellt es fest, dass sich aus der Analyse der Umstände sogar bis in Intimsphäre reichende Schlüsse ziehen lassen.
[1631] http://www.telefonseelsorge.de/.
[1632] Da diese nicht auf die Erhaltung der Lebensgrundlage angelegt ist.

einmal erforderlich. Es genügt, wenn die Tätigkeit nicht mehr in gewünschter Weise ausgeführt werden kann. Dies ist schon der Fall, wenn bei dem Angebot „anonymer Telefonseelsorge" das Interesse der Anbieter, nämlich die Möglichkeit einer wirklich anonymen Seelsorgeleistung, beeinträchtigt wird, weil die vollständige Anonymität durch eine gesetzliche Vorratsdatenspeicherung nicht gewährleistet ist.

Die Gefahr einer Beeinträchtigung der Berufsausübungsfreiheit besteht auch für andere medizinische, psychologische und therapeutische Anlaufstellen. Sie ist darüber hinaus denkbar für Angebote von Telefonsex. Denn in all diesen Bereichen lässt sich allein aus den Angaben über die Umstände der Telekommunikation ein Schluss auf die Inhalte des Gesprächs ziehen und so liegt es nahe, dass bei Kontaktaufnahmen, die dem höchstpersönlichen oder zumindest sehr persönlichen Bereich des Einzelnen zuzuordnen sind, die Vorratsdatenspeicherung dazu führen kann, das von entsprechenden Angeboten und Kommunikationswegen kein Gebrauch mehr gemacht werden wird.

So hat das *Bundesverfassungsgericht* festgestellt, es gehe „von einem ungenügenden rechtlichen Schutz des Vertrauensverhältnisses (…) ein „chilling effect" aus, der als Nebeneffekt den Bürger faktisch von einer verfassungsrechtlich geschützten Kommunikation abhält."[1633] Auch wenn sich das *Bundesverfassungsgericht* bei dieser Aussage auf die Gefahr eines staatlichen Zugriffs auf die Inhalte einer Telekommunikation bezieht, muss dies auch für die generelle Erfassung der Telekommunikationsumstände gelten.[1634] Hier droht zwar kein unmittelbarer Zugriff auf die Inhalte, aber es droht ein staatlicher Zugriff auf die Umstände, aus denen sich Schlüsse auf die Inhalte ableiten lassen, die insofern quasi Inhaltsdaten sind.

Ob es in der Praxis zu einer solchen Beeinträchtigung kommt ist bislang nicht nachgewiesen. Die Ergebnisse einer *forsa-Studie*[1635] im Auftrag des *AK Vorratsdatenspeicherung* legen dies zumindest nahe.[1636]

Auch europarechtlich ist ein Schutz der Vertrauensbeziehungen im Rahmen der Vorratsdatenspeicherung geboten. Ein Schutz des Berufsgeheimnisses ist zwar in der Europäischen Menschrechtskonvention nicht ausdrücklich normiert – der *Europäische Gerichtshof* hat einen solchen aber aus Art. 8 EMRK, dem Recht auf ein faires Verfahren, und aus dem Recht auf Verteidigung aus Art. 6 Abs. 3 lit. c EMRK hergeleitet. Das Gericht hat so einen Grundsatz der Vertraulichkeit des Schriftverkehrs zwischen Anwalt und Mandant entwickelt.[1637] Der *Europäische Gerichtshof für Menschenrechte* und der *Europäische Gerichtshof* erkennen darüber hinaus einen ähnli-

[1633] *Ignor*, NJW 2007, 3403, 3405.

[1634] So im Ergebnis auch BVerfGE 125, 260 (319); „Da eine Auswertung dieser Daten tief in das Privatleben eindringende Rückschlüsse und unter Umständen detaillierte Persönlichkeits- und Bewegungsprofile ermöglicht, kann insoweit nicht ohne Weiteres davon ausgegangen werden, dass der Rückgriff auf diese Daten grundsätzlich geringer wiegt als eine inhaltsbezogene Telekommunikationsüberwachung"

[1635] http://www.daten-speicherung.de/data/forsa_2008-06-03.pdf.

[1636] http://www.heise.de/newsticker/meldung/Forsa-Umfrage-Vorratsdatenspeicherung-beeinflusst-Telefonierverhalten-211882.html.

[1637] *EuGH*, Urt. v. 18.5.1982, Rs. 155/79, Slg. 1982, 1575 ff. (*AM & S Europe Limited* ./. Kommission *der Europäischen Gemeinschaften*); vgl. dazu *Schorkopf* in *Ehlers/Becker* § 16.1, Rn. 26.

chen Schutz auch bei anderen (Dienstleistungs-) Berufen durch das Berufsgeheimnis an, jedenfalls soweit diese ein besonderes Vertrauensverhältnis voraussetzen.[1638]

9.1.2.4.2 Pressefreiheit

Die Vorratsdatenspeicherung könnte schließlich die Pressefreiheit verletzen. Da Voraussetzung für das Funktionieren des demokratischen Staates eine möglichst an Tatsachenkenntnissen orientierte Wahlentscheidung des Bürgers ist und diese in aller Regel nur über Presse und sonstige Massenkommunikationsmittel erreicht werden kann, kommt der Pressefreiheit eine staatstragende und grundlegende Bedeutung zu.[1639] Die Pressefreiheit ist aber nicht nur zentrales Wesensmerkmal der Demokratie, sondern wird auch durch das Grundrecht des Art. 5 Abs. 1 S. 2 GG gewährleistet.[1640] Dieser schützt die Arbeit und Arbeitsfähigkeit der Presse.[1641] Davon erfasst sind nicht nur der Druck und die Veröffentlichung, sondern ebenso alle vorbereitenden Tätigkeiten, wie etwa das Aufspüren von Nachrichten, das Befragen von Personen, das Recherchieren von Tatsachenmaterial, von Sachen und Personen, jedes zu einem dieser Zwecke geführte Telefongespräch oder jeder Schriftwechsel.[1642] Auch das Verhältnis zwischen Presseorgan und seinen Informanten ist im Interesse der Funktionsfähigkeit des Rundfunks geschützt, wobei Beschränkungen nicht grundsätzlich ausgeschlossen sind.

Ein Eingriff in die Pressefreiheit liegt dann vor, wenn die Presse in ihrer Ausübung durch staatliche Maßnahmen beeinträchtigt wird.[1643] Dies ist bei der Erhebung von Daten über den Telekommunikationsverkehr von Presse- und Rundfunkveranstaltern der Fall.[1644]

Das *Bundesverfassungsgericht* führte dazu in einer Entscheidung aus dem Jahr 2003 aus, dass soweit auf Verkehrsdaten von Pressevertretern zugegriffen werde, dies ge-

---

[1638] Vgl. z. B. für das Arztgeheimnis *EGMR*, Urt. v. 12.2.2007, *L. L./. Frankreich,* Az. 7508/02; *EuGH*, Urt. v. 8.4.1992, Rs. C-62/90. Im Bereich des Informantenschutzes sind Eingriffe in Telekommunikationsverbindungen von Journalisten zusätzlich zu Art. 8 Abs. 1 EMRK auch durch Art. 10 EMRK geschützt, ohne dass damit allerdings ein höheres Schutzniveau verbunden wäre; vgl. *Hochreiter* 2002, 51; *EGMR*, Urt. v. 10.12.2007, Stoll./. Schweiz, Az. 69698/01.

[1639] *Herzog* in *Maunz/Dürig*, GG 2011, Art. 5, Rn. 118; *Schulze-Fielitz* in *Dreier,* GG 2004, Art. 5 Rn. 209.

[1640] Wie genau der Schutzbereich definiert werden kann, ist umstritten, so *Herzog* in *Maunz/Dürig*, GG 2011, Art. 5, Rn. 125; allerdings handelt es sich dabei im Wesentlichen um Abgrenzungsprobleme zwischen den einzelnen durch Art. Geschützten Freiheitsgrundrechten, die praktisch keine Auswirkung haben auf Grund der identischen Maßstäbe für die Grundrechtsbeschränkung, so *Schulze-Fielitz,* in *Dreier,* GG 2004, Art. 5 Rn. 88.

[1641] *Herzog* in *Maunz/Dürig*, GG 2011, Art. 5, Rn. 135; *Schulze-Fielitz* in *Dreier,* GG 2004, Art. 5 Rn. 95.

[1642] *Herzog* in *Maunz/Dürig*, GG 2011, Art. 5, Rn. 137.

[1643] *Schemmer* in BeckOK, Art. 5 GG, Rn. 53; Ein Eingriff in die Grundrechte aus Art. 5 Abs. 1 GG ist jede staatliche Maßnahme, die final in den Schutzbereich eines der jeweiligen Grundrechte regelnd eingreift, *Schulze-Fielitz* in *Dreier,* GG 2004, Art. 5 Rn. 124; Faktische Beeinträchtigungen, können aber von solchem Gewicht sein, dass sie rechtlich regelnden Eingriffen gleichgestellt werden, bspw. das heimliche Abhören von Gesprächen (*Schulze-Fielitz,* Rn. 128). Das *BVerfG* hat Eingriffe festgestellt bei dem Verbot der Berufsausübung als Redakteur, BVerfGE 10, 118 (121); sowie der Beschlagnahme von Presseprodukten, BVerfGE 56, 247 (248 f.).

[1644] BVerfGE 107, 299 (330 f.).

rechtfertigt werden könne, „wenn sie zur Verfolgung einer Straftat von erheblicher Bedeutung erforderlich sind, hinsichtlich der ein konkreter Tatverdacht besteht und wenn eine hinreichend sichere Tatsachenbasis für die Annahme vorliegt, dass der durch die Anordnung Betroffene mit dem Beschuldigten über Telekommunikationsanlagen in Verbindung steht."[1645] Art. 5 Abs. 1 S. 2 GG gebietet es nicht, Journalisten „generell" von strafprozessualen Maßnahmen auszunehmen.[1646]

Fraglich ist, ob etwas anderes für die verdachtsunabhängige Verpflichtung zur Speicherung der Verkehrsdaten auf Vorrat gelten muss. Es wurde argumentiert, dass die Pressefreiheit von einer Vorratsdatenspeicherung mit unverhältnismäßiger Intensität getroffen würde, da Journalisten in besonderem Maße auf eine besondere Vertraulichkeit der Kommunikation angewiesen seien.[1647] Die Bereitschaft von Informanten könnte mit der Möglichkeit ihrer Enttarnung sinken.

Eine solche Sichtweise wird belegt durch einen Skandal in Polen: Hier wurden von zehn Journalisten, die durch investigative Artikel aufgefallen waren, umfassende Kommunikations- und Bewegungsprofile angelegt. Mit Hilfe der „Vorratsdaten" wurde das Leben der Journalisten bis in die Vergangenheit durchleuchtet, wohl um diese einzuschüchtern.[1648]

Nach der Rechtsprechung des *Bundesverfassungsgerichts* ist es zwar nicht zwingend geboten, Journalisten generell von strafprozessualen Maßnahmen auszunehmen. Dennoch gilt besonders für Journalisten, dass die Vorratsdatenspeicherung in einem hohen Maße einschüchternd wirkt. Der besonderen Bedeutung der Pressefreiheit – und der Bedeutung einer freien Kommunikation für die Presse – sollte bei der Ausgestaltung einer Vorratsdatenspeicherung Rechnung getragen werden. Es ist insofern zu empfehlen, auch die Verbindungsdaten von den Grundrechtsträgern des Art. 5 Abs. 1 S. 2 GG wie von anderen Berufsgeheimnisträgern vollständig von einer Vorratsdatenspeicherung auszunehmen.

Dies ist jedoch nicht zwingend verfassungsrechtlich gefordert. Gefordert ist jedenfalls eine verfahrensrechtliche Flankierung derselben durch spezielle Sicherungen zugunsten der Presse.[1649] Im Hinblick auf einen optimierten Interessenausgleich ist eine solche Ausgestaltung aber geboten. Denn der Eingriff in die Pressefreiheit ist nicht alternativlos und auch nicht unverzichtbar.

9.1.2.4.3 Erforderlichkeit eines besonderen Schutzes

Soweit Verkehrsdaten über die Kommunikation mit Berufsgeheimnisträgern gespeichert werden, handelt es sich um einen Eingriff in die Berufsfreiheit von Geheimnisträgern. Dieser Eingriff kann mit dem Ziel, Sicherheit zu erzeugen, grundsätzlich gerechtfertigt werden. Er ist auch geeignet und erforderlich im Sinne der klassischen Verhältnismäßigkeitsprüfung. Allerdings ist er weder unverzichtbar noch alternativlos.

[1645] BVerfGE 107, 299 (LS 3).
[1646] BVerfGE 107, 299 (331).
[1647] *Gola/Klug/Reif,* NJW 2007, 2599, 2601.
[1648] http://fm4.orf.at/stories/1669759/.
[1649] So auch: *Gola/Klug/Reif,* NJW 2007, 2599, 2601.

Als Alternative bietet sich neben einem Quick-Freeze-Verfahren auch eine Vorratsspeicherung ohne die Daten von Berufsgeheimnisträgern an.

Auch das *Bundesverfassungsgericht* hat im Urteil zur Vorratsdatenspeicherung ausgeführt, dass für die Verkehrsdaten, die Vertrauensbeziehungen betreffen, ein „grundsätzliches Übermittlungsverbot" bestünde. Das Gericht nennt als Beispiele „Verbindungen zu Anschlüssen von Personen, Behörden und Organisationen in sozialen oder kirchlichen Bereichen, die grundsätzlich anonym bleibenden Anrufern ganz oder überwiegend telefonische Beratung in seelischen oder sozialen Notlagen anbieten und die selbst oder deren Mitarbeiter insoweit anderen Verschwiegenheitsverpflichtungen unterliegen".[1650]

9.1.2.5 Rechtssicherheit

Die Verpflichtung zur Speicherung der Verkehrsdaten erfolgt bei der Vorratsdatenspeicherung zwar durch ein öffentlich verkündetes Gesetz, dennoch droht die Vorratsdatenspeicherung Rechtsunsicherheit zu erzeugen, wenn der Einzelne nicht weiß, ob oder wann, auf welche seiner Daten zugegriffen und wie sie verwendet wurden.

Das Rechtsstaatsprinzip beinhaltet mit der Rechtssicherheit die Forderung, dass staatliche Hoheitsakte so klar und bestimmt und zugleich so beständig sein sollen, dass sich der Bürger auf sie hinreichend verlassen kann (Verlässlichkeit der Rechtsordnung).[1651] Dadurch soll die Vorhersehbarkeit staatlichen Handelns sichergestellt werden, um zu verhindern, dass sich der Einzelne als Objekt willkürlicher Staatsgewalt empfindet.[1652] Erforderlich ist dafür unter anderem eine inhaltlich hinreichend klare Fassung von Normen, damit sich der Betroffene ein eigenes Bild von der Rechtslage machen kann.

Daneben gilt das Gebot der Bestimmtheit von Normen, das nicht eindeutig vom Gebot der inhaltlichen Klarheit zu unterscheiden ist. Die Folgen der Regelung müssen so vorhersehbar und berechenbar sein, dass zum einen der Einzelne sein Verhalten daran ausrichten kann, und zum anderen, dass die Verwaltung klare Handlungsmaßstäbe hat und eine hinreichende gerichtliche Kontrolle möglich ist.[1653]

Das *Bundesverfassungsgericht* hat in der Rechtsprechung betont, dass für die Anforderungen an Klarheit und Bestimmtheit wesentlich die Bedeutung und die Eingriffsintensität der Norm und die Eigenheiten des sachlichen Regelungsgegenstands seien.[1654] Generell steht das Bestimmtheitsgebot in enger Beziehung zum Parlamentsvorbehalt,

---

[1650] BVerfGE 125, 260 (334) unter Verweis auf § 99 Abs. 2 TKG.

[1651] Vgl. dazu oben S. 105.

[1652] *Grzeszick* in *Maunz/Dürig,* GG 2011, Art. 20, Rn. 59.

[1653] *Grzeszick* in *Maunz/Dürig,* GG 2011, Art. 20, Rn. 58.

[1654] Treffend formuliert *Grzeszick* „Je bedeutsamer die Norm ist, insbesondere je intensiver die damit verbundene Freiheitseinschränkung des Bürgers ausfällt, und je eindeutiger, abgrenzbarer und vorhersehbarer der Regelungsgegenstand ist, desto höher ist das Maß der gebotenen inhaltlichen Bestimmtheit der Norm. Ist dagegen die Norm von geringer Bedeutung, vor allem weil sie nicht oder nur in geringem Maße in die Freiheit der Bürger eingreift, und ist der Regelungsgegenstand vielgestaltig, unübersichtlich und raschen Änderungen unterworfen, fällt das Maß der gebotenen Bestimmtheit geringer aus." *Grzeszick* in *Maunz/Dürig,* GG 2011, Art. 20, Rn. 60; zur Rspr des *BVerfG* zu den Anforderungen an die Bestimmtheit im Verhältnis zum Eingriffsgewicht, vgl. bereits oben S. 105; aus der Rspr. vgl. BVerfGE 110, 33 (55); 120, 378 (408).

der sicherstellen soll, dass wesentliche Entscheidungen auch inhaltlich durch das Parlament entschieden werden müssen.[1655]

Für eine Verpflichtung zur Vorratsdatenspeicherung bedeutet dies, da es sich bei ihr um einen besonders schwerwiegenden Eingriff in die Freiheitsrechte der Bürger handelt,[1656] dass hohe Anforderung an die Bestimmtheit der zur Speicherung und vor allem auch zur Verwendung der Daten ermächtigenden Normen zu stellen sind. Die Regelungen in den §§ 113a, 113b a.F. TKG würden dem genügen, so das *Bundesverfassungsgericht*.[1657] Das Gericht hat jedoch betont, dass die Daten „von vornherein nur zu bestimmten, bereichsspezifischen, präzise und normenklar festgelegten Zwecken gespeichert werden" dürfen, „so dass bereits bei der Speicherung hinreichend gewährleistet ist, dass die Daten nur für solche Zwecke verwendet werden, die das Gewicht der Datenspeicherung rechtfertigen. Eine Speicherung kann nicht als solche abstrakt gerechtfertigt werden, sondern nur insoweit, als sie hinreichend gewichtigen, konkret benannten Zwecken dient".[1658] Wenn eine Vorratsdatenspeicherung eingeführt wird, müssen die Zwecke zu denen auf die Daten zugegriffen werden darf, konkret und abschließend bestimmt werden.

9.1.2.6 Verbot der Profilbildung

Die Auswertung der auf Vorrat gespeicherten Verkehrsdaten ermöglicht es, umfassende Persönlichkeits- und Bewegungsprofile zu erstellen.[1659] Sie droht daher mit dem Verbot der Bildung von Persönlichkeitsprofilen zu kollidieren.[1660]

Letztlich ist in Anbetracht der umfassenden Analysemöglichkeiten von Vorratsdaten sicher-zustellen, dass keine selbstständigen Abbilder der Bürger geschaffen werden. Das Verbot der Bildung von Persönlichkeitsprofilen reicht zwar nicht soweit, als dass es die Verknüpfung von Vorratsdaten mit anderen Daten generell verbietet. Sie ist allerdings nur in Ausnahmefällen zulässig und auch nur, soweit dies für die Verfolgung eines bestimmten Zwecks erforderlich ist. Es muss insofern sichergestellt sein, dass die Daten nicht ohne gewichtigen und den Eingriff überwiegenden Grund zu einem Profil zusammengestellt werden. Soweit ein Profil erstellt wird, muss die strikte Zweckbindung beachtet werden.

9.1.2.7 Anforderungen an eine Vorratsdatenspeicherung aus Perspektive bürgerlicher Freiheitsrechte

Zur Sicherung der Freiheitsrechte der Bürger muss der Wesensgehalt des Telekommunikationsgeheimnisses muss gewahrt werden, erforderlich ist daher eine Begrenzung des Umfangs der Vorratsspeicherung – Inhaltsdaten dürfen keinesfalls mit gespeichert werden. Für die Ausgestaltung der Speicherung selbst sind sodann die datenschutzrechtlichen Grundprinzipien zu beachten. Gefordert ist ein umfassender Schutz von

---

[1655] BVerfGE 120, 378 (408)
[1656] Vgl. dazu oben Kap. 9.1.2.1.3.1.
[1657] BVerfGE 125, 260 (315).
[1658] BVerfGE 125, 260 (345).
[1659] Dazu ausführlich mit zahlreichen Nachweisen oben S. 183 f.
[1660] Zu diesem, vgl. oben Kap. 5.1.2.

Vertrauensbeziehungen und zwar sowohl von Ärzten, Abgeordneten, Rechtsanwälten, Seelsorgern als auch von Journalisten. Auf Grund des hohen Eingriffsgewichts sind die Anforderungen an die Bestimmtheit der Regelung sehr hoch. Schließlich muss bezüglich der Verwendung der Daten sichergestellt werden, dass nicht gegen das Verbot der Bildung von Persönlichkeitsprofilen verstoßen wird. Von zentraler Bedeutung ist zudem, dass sichergestellt wird, dass die Vorratsdatenspeicherung weder für sich genommen noch im Zusammenspiel mit anderen Maßnahmen zu einer umfassenden gesamtgesellschaftlichen Überwachung führt.

9.1.3 Elemente eines Interessenausgleichs

Es zeichnet sich ab, dass die Elemente die einen Interessenausgleich in dieser ersten Dimension befördern können, primär jene sind, die den Umfang der Maßnahme bestimmen: Speicherungsverpflichtung und Zugriffs- und Verwendungsregelungen. Diese prägen aus Perspektive des Bürgers das Eingriffsgewicht und bestimmen für Sicherheitsbehörden den Nutzen der Vorratsdatenspeicherung. Von Bedeutung sind dafür technische und organisatorische Maßnahmen, die im Hinblick auf Speicherort, Datensicherheit, Abrufverfahren und die Vorkehrungen zur Wahrung des Verbots umfassender gesamtgesellschaftlicher Überwachung Anknüpfungspunkte bieten, um einen Ausgleich der Interessen zu befördern.

Neben der rechtlichen Ausgestaltung der Speicherungsregelung und Verwendungsregelung bieten Regelungen zu Rechtsschutz und Transparenz die Möglichkeit das Spannungsverhältnis optimiert aufzulösen.

9.2 *Staat − Wirtschaft*

Die Einführung einer Vorratsdatenspeicherung verursacht eine mehrdimensionale Grundrechtskollision.[1661] Neben dem Eingriff in die Grundrechte der Telekommunikations-nutzer erfolgen auch Eingriffe in die Grundrechte der Telekommunikationsanbieter. Denn notwendigerweise müssen die Telekommunikationsdiensteanbieter verpflichtet werden, die Daten zu erheben.

Im Urteil des *Bundesverfassungsgerichts* kommt zudem zum Ausdruck, dass die Speicherung durch die Telekommunikationsanbieter quasi der „Schlüssel zur Zulässigkeit" der Vorratsdatenspeicherung ist.[1662] Denn Voraussetzung für eine verhältnismäßige Ausgestaltung ist, dass sie „nicht direkt durch den Staat" erfolgt, „sondern durch eine Verpflichtung der privaten Dienstanbieter verwirklicht wird".[1663]

Die betroffenen Grundrechte der Telekommunikationsunternehmen kollidieren insoweit in der Dimension *Staat - Wirtschaft* zum einen mit dem Interesse des Staates, Sicherheit zu erzeugen, und zum anderen mit der staatlichen Schutzpflicht zu Gunsten der Freiheitsrechte der Bürger. Denn der Staat muss sicherstellen, dass auch bei einer Speicherung durch die Privaten, das Telekommunikationsgeheimnis und die informa-

[1661] Art. 10 GG umfasst auch den Auftrag an den Staat, gegen den missbräuchlichen Zugriff privater auf Inhalt und Umstände der Telekommunikationsbeziehungen Schutz zu gewähren, so *Hoffmann-Riem*, JZ 2008, 1009, 1014. Dies gilt auch, wenn der Staat Private zur Speicherung verpflichtet.

[1662] *Eckhardt/Schütze* CR 2010, 225 (227).

[1663] BVerfGE 125, 260 (321); dazu auch schon oben S. 276.

tionelle Selbstbestimmung gewahrt werden. Darüber hinaus sind in der zweiten Dimension noch weitere staatliche Interessen relevant, die er bei der Ausgestaltung der Sicherheitsmaßnahme berücksichtigen muss.

Die mit der Vorratsdatenspeicherung verbundenen Auswirkungen auf die Telekommunikationsindustrie, werden in der Diskussion um die Vorratsdatenspeicherung vielfach vernachlässigt.[1664] Dies kann durchaus verwundern, da die Richtlinie ursprünglich als Instrument zur Harmonisierung des Binnenmarktes erlassen wurde.[1665]

Für einen Interessenausgleich ist es wesentlich zu klären, ob und in welchem Umfang die Verpflichtung zur Speicherung und Verarbeitung der Daten auf die privaten Anbieter übertragen werden kann. Wo liegen die Grenzen der Übertragung von staatlichen Aufgaben auf Private? Was ist dabei zu beachten? Können auch die Kosten übertragen werden und wenn ja, bis zu welcher Grenze?

9.2.1 Staatliche (Sicherheits-)Interessen

Wichtig ist aus Perspektive staatlicher Sicherheitsinteressen[1666], dass möglichst umfassend alle Anbieter und Unternehmen verpflichtet werden um möglichst lückenlos Verkehrsdaten zu jedweder Telekommunikationsverbindung verfügbar zu halten.

Darüber hinaus ist im Kollisionsverhältnis mit der Wirtschaft neben dem allgemeinen staatlichen Sicherheitsinteresse vor allem die Wahrung des staatlichen Gewaltmonopols zu beachten, das für die Gewährleistung von Sicherheit von zentraler Bedeutung ist. Von Belang ist auch der Grundsatz der Steuerstaatlichkeit. Auch dieses Interesse ist im Hinblick auf die Gewährleistung von Sicherheit zu berücksichtigen, da gespeicherte Verkehrsdaten nur dann einen ermittlungstechnischen Vorteil bringen, wenn ihre Integrität gewahrt wird. Verfälschte Daten würden die Ermittlungsarbeit behindern und nicht befördern.

9.2.1.1 Staatliches Gewaltmonopol

Da im Rahmen der Vorratsdatenspeicherung private Unternehmen verpflichtet werden an der Gewährleistung der Sicherheit mitzuwirken, könnte dies mit dem staatlichen Gewaltmonopol kollidieren. Denn zum einen werden auf diesem Weg die Telekommunikationsanbieter zu Hilfspersonen des Staates[1667] und zum anderen entsteht so ein

---

[1664] So etwa im Jahr 2007 der Branchenverband bitkom: „Pläne zur Vorratsdatenspeicherung ignorieren weiter die Auswirkungen für die TK-Wirtschaft“, http://www.bitkom.org/de/themen/54882_46205.aspx; Der folgende Abschnitt basiert auf einem bereits veröffentlichten Text der Autorin *Knierim* 2011b.

[1665] Rechtsgrundlage der RL ist ex-Art. 95 EGV. Der *EuGH* hat die Wahl der Rechtsgrundlage bestätigt, da sie „in überwiegendem Maße“ dem Funktionieren des Binnenmarktes diene, so *EuGH*, Urt.v. 10.2.2009 - Rs. C-301/06; s. zu diesem Argument auch *Roßnagel,* DuD 2010, 544; ausführlich zur Entstehung der Richtlinie, oben Kap. 4.2.1.

[1666] Vgl. generell zum Staat als „Beschützer der Bürger“, oben Kap. 2.2; spezifisch in Bezug auf die Vorratsdatenspeicherung, vgl. Kap. 9.1.1.

[1667] „Denn diese werden allein als Hilfspersonen für die Aufgabenerfüllung durch staatliche Behörden in Anspruch genommen“, BVerfGE 125, 260 (366), dazu auch oben S. 269.

Geheimhaltungsproblem, da die Telekommunikationsanbieter Kenntnisse über laufende Verfahren erhalten.[1668]

Das Gewaltmonopol des Staates ist essentiell für die völkerrechtliche Bestimmung des Staates.[1669] Auch das Rechtsstaatsprinzip dessen Aufgabe und Ziel es ist, Rechtsfrieden und Rechtssicherheit zu gewährleisten, setzt das staatliche Gewaltmonopol voraus.[1670] Dieses wird verstanden als Möglichkeit der physischen Gewaltanwendung des Staates und ist unverzichtbarer Bestandteil staatlicher Daseinssicherung und Zukunftsvorsorge.[1671]

Sicherheit und Ordnung sind Staatsaufgaben, die grundlegend für die Wahrung des staatlichen Gewaltmonopols sind. Wenn der Staat dem nicht nachkommt, verliert er seine Legitimation. Der Staat ist „Beschützer der Bürger"[1672] und muss seine ureigene Aufgabe Sicherheit zu gewährleisten erfüllen.[1673] Insofern ist auch der Staatszweck Sicherheit in seiner Kernsubstanz unantastbar.[1674] Es handelt sich mithin um eine „notwendige Staatsaufgabe". Eine solche ist grundsätzlich nicht privatisierungsfähig.[1675] Eine Privatisierung ist hier lediglich im Rahmen der Unterstützung bei der operativen Durchführung möglich, wenn die Verantwortung für die Erfüllung der Staatsaufgabe bei diesem verbleibt. Der Verfassung ist kein striktes Verbot der kooperativen Erfüllung staatlicher Gewaltaufgaben zu entnehmen.[1676] Es gilt insofern auch im Bereich der Gefahrenabwehr und Strafverfolgung kein absolutes Privatisierungsverbot.[1677]

Zum Teil wird vertreten, dass es sich bei der Vorratsdatenspeicherung um ein „Outsourcing" handle, „bei dem die Grenze zwischen öffentlichem und nicht-öffentlichem Bereich überschritten wird", da sie nicht klar zu beantwortende Fragen nach der datenschutzrechtlichen Verantwortung aufwerfe.[1678] Zwar würden nicht unmittelbar Straf-

---

[1668] Vgl. *Albrecht/Kilchling* 2011, 171.

[1669] *Isensee,* in: *Isensee/Kirchof* HStR II, § 15 Rn. 53; im Völkerrecht werden Staaten anhand der Drei-Elemente-Lehre *Jellinek*s definiert. Ein Staat ist demnach dann gegeben, wenn ein Staatsgebiet, ein Staatsvolk und Staatsmacht gegeben ist. Dazu ausführlich schon oben S. 111.

[1670] *Stober*, NJW 1997, 889, 893; Zum ideengeschichtlichen Hintergrund, oben Kap. 1.1; zur verfassungsrechtlichen Verortung und dem Umfang des Gewaltmonopols, vgl. oben Kap. 2.2.1.

[1671] *Stober*, NJW 1997, 889, 890.

[1672] *Roßnagel*, Informatik-Spektrum 2002, 33, 34; vgl. dazu Kap. 2.2.7.

[1673] Wobei er nicht verpflichtet ist hundertprozentige/ absolute Sicherheit zu gewährleisten, da eine solche nicht realisierbar ist (vgl. S. 116). Dazu generell ausführlich Kap. 2.2, insbesondere S. 118, 122.

[1674] *Stober*, NJW 1997, 889, 890.

[1675] *Jachmann* in *Mangoldt/Klein,* GG 2010, Art. 33, Rn. 38 Notwendige Staatsaufgaben sind jene die unerlässlich für die Funktionsfähigkeit des Staates sind. Zu nennen sind insoweit insbesondere Selbstorganisation, Selbstschutz und Außenvertretung des Staates sowie die Aufrechterhaltung der inneren Sicherheit und Ordnung, die Steuererhebung, die Justiz und das Währungswesen (Rn. 34).

[1676] *Stober*, NJW 1997, 889, 893.

[1677] Das *BVerwG* hat dazu etwa im sog. Flugsicherheitsgebührenfall ausgeführt, dass der Staat nicht, „jede von ihm als erforderlich angesehene Maßnahme durch eigene Dienstkräfte" erledigen muss, sondern sich auch privater Personen bedienen könne, weil nicht festgelegt sei, in welcher Weise der Staat seinen Pflichten genüge, BVerwGE95, 188 (197).

[1678] *Weichert* 2011b, 3 führt aus dass die Verantwortlichkeit und die Kosten auf die Privaten abgeschoben werden solle.

verfolgung und Gefahrenabwehr privatisiert, aber der Staat würde immer stärker von der Kooperationsbereitschaft Privater abhängig.[1679]

Fraglich ist wo verfassungsrechtlich die Grenze der Privatisierungsfähigkeit staatlicher Aufgaben verläuft: Zum Teil wird eine Missachtung des Gewaltmonopols erst angenommen, wenn die Privatisierung mit der Ausübung physischen Zwangs verbunden sei. Allein vorbereitenden Tätigkeiten oder Privatisierungen, die sich nur auf die Erbringung einzelner Leistungen bezögen, verstießen nicht gegen ein dem Gewaltmonopol immanenten Privatisierungsverbot.

Überzeugender ist es jedoch nicht an der Ausübung von Gewalt anzuknüpfen, da auch wenn der Staat Hilfstätigkeiten überträgt, er verpflichtet ist sicherzustellen, dass die rechtsstaatlichen Standards eingehalten werden.[1680] Denn durch die Privatisierung einer Aufgabe dürfen die rechtsstaatlichen Standards nicht geschmälert werden. Das Gewaltmonopol dient ja gerade dazu sicherzustellen, dass der Einzelne keiner willkürlichen Gewaltausübung ausgesetzt wird. Daher muss die Verantwortung für die Erfüllung der Staatsaufgaben auch bei der Übertragung von Hilfsaufgaben auf Private beim Staat bleiben.[1681]

Im Ergebnis kann die Übertragung der Vorratsspeicherung auf die privaten Anbieter aber so gestaltet werden, dass sie nicht mit dem Interesse des Staats das Gewaltmonopol zu wahren, kollidiert. Erforderlich ist dafür, dass die Organisationshoheit in staatlicher Hand verbleibt. Insofern muss auch, soweit die Speicherungsverpflichtung ausgelagert wird, sichergestellt sein, dass sämtliche rechtsstaatlichen Standards gewahrt werden. Insbesondere muss auch durch rechtliche und organisatorische Maßnahmen gewährleistet werden, dass auch die Verarbeitung der Vorratsdaten bei den Anbietern strengen Geheimhaltungsvorschriften unterliegt.

9.2.1.2 Grundsatz der Steuerstaatlichkeit

Bezüglich der Frage, ob die im Rahmen einer Vorratsdatenspeicherung entstehenden Kosten auf die Telekommunikationsanbieter übertragen werden können, ist neben dem haushaltsrechtlichen Interesse die Kosten möglichst gering zu halten auch der Grundsatz der Steuerstaatlichkeit als staatliches Interesse zu berücksichtigen.

Der Grundsatz der Steuerstaatlichkeit wurzelt in der Finanzverfassung[1682] und gebietet grundsätzlich die im Rahmen der Wahrnehmung hoheitlicher Aufgaben entstehenden Kosten im Haushalt abzubilden. Entsprechend ist für die im Rahmen der Wahrneh-

---

[1679] Dies zeige sich schon bei der klassischen Auftragsdatenverarbeitung, wenn sich öffentliche Stellen derart stark auf die Hilfe des privaten Auftragnehmers verlassen, dass sie dem „faktisch hilflos ausgeliefert" sind, so *Weichert* 2011b, 4.

[1680] *Stober*, NJW 2008, 2301, 2305.

[1681] *Stober*, NJW 2008, 2301, 2305.

[1682] *Wagner*, PharmR 2003, 409, 414 Die Finanzverfassung des GG gehe davon aus, dass die Gemeinlasten aus Steuern finanziert werden. Nichtsteuerliche Abgaben seien zwar nicht ausgeschlossen, dürften aber die Finanzverfassung nicht aushöhlen; zum Grundsatz der Steuerstaatlichkeit als verfassungsrechtlich anerkanntes Prinzip, *Kube*/*Palm*/*Seiler*, NJW 2003, 927, 928; dazu auch *Sacksofsky/Wieland* 2000; *Sacksofsky* 2000.

mung hoheitlicher Aufgaben entstehenden Kosten aus Gründen der staatsbürgerlichen Lastengleichheit eine finanzielle Kompensation vorzusehen.[1683]

Zum Teil wird das Bestehen eines Grundsatzes der Steuerstaatlichkeit bestritten.[1684] Aus der Finanzverfassung lasse sich kein Primat der Steuer ableiten. Dem Gesetzgeber sei nicht die Wahl zwischen verschiedenen Abgabenformen verwehrt, sondern der Finanzverfassung sei lediglich ein Gebot der Abgabenklarheit zu entnehmen. Verfassungswidrig sei allein eine abgabenrechtliche Willkür.[1685]

Letztlich ist der Kritik am Prinzip der Steuerstaatlichkeit zwar insoweit zuzustimmen als sich dieses nicht unmittelbar aus dem Wortlaut der Verfassung ergibt.[1686] Der Grundsatz der Steuerstaatlichkeit ist aber aus der Zusammenschau der Eigentumsgarantie und der Finanzverfassung ableitbar.[1687] Zudem besteht ein enger Zusammenhang zwischen dem Prinzip der Steuerstaatlichkeit und dem Verfassungsgrundsatz der Vollständigkeit des Haushaltsplans.[1688] Der Spielraum zur Erhebung nicht-steuerlicher Abgaben ist jedenfalls insoweit eingeschränkt, als die prinzipielle Steuerstaatlichkeit nicht tangiert werden darf.[1689] Grundsätzlich gebührt der Erhebung von Steuern als Lenkungsinstrument der Vorrang. Denn soweit beliebig weitere Abgaben erhoben würden, kann dies unter anderem die Eigentumsfreiheit, die Berufsfreiheit und noch weitere Freiheitsrechte des Bürgers gefährden.[1690]

Der individualschützende Aspekt hat seine Wurzel im Leistungsfähigkeitsprinzip. Der Bürger soll für hoheitliche Aufgaben, dies gebietet das Sozialstaatsprinzip, nur ent-

---

[1683] *Schirra* 2002, 138 f.

[1684] *Sacksofsky*, 2000, 162.

[1685] *Schirra* 2002, 160.

[1686] Darauf weist hin *Schirra* 2002, 56, der sich im Folgenden ausführlich mit dem Meinungsstand zum Steuerstaatsprinzip auseinandersetzt. Heute ist das Steuerstaatsprinzip weitgehend anerkannt.

[1687] So *Schirra* 2002, 60 auf den S. 57 ff. legt er ausführlich dar, inwiefern das Steuerstaatsprinzip zentral das System abgabenrechtlicher Balance in Bund und Ländern abschließt. Auf den S. 68 ff. setzt er sich so dann mit der Frage auseinander inwiefern das Steuerstaatsprinzip auch individualschützende Wirkung entfaltet. Als Leitlinien des grundgesetzlichen Finanzsystems, die durch die Kompetenzverteilung und durch die Freiheitsrechte bestimmt sind betont *Kube*, dass zwischen Steuern und anderen Abgaben unterschieden werden müsse. *Kube*, *Palm, Seiler*, NJW 2003, 927, 928.

[1688] So würde das Budgetrecht des Parlaments beeinträchtigt, weil die Kostenübertragung den vorgesehenen Planungs-, Kontroll- und Rechenschaftsverfahren entzogen ist, *Wagner*, PharmR 2003, 409, 414 f. Sie führt dies als dritten Grund an, der gegen die Übertragung von Kosten durch sonstige Modelle in den Markt spricht. Bei jeder anderen als einer steuerlichen Übertragung von Kosten auf die Staatsbürger, argumentiert *Wagner*, handele es sich um Sonderabgaben, die nur unteren strengen Voraussetzungen zulässig wären. Nach ihrer Ansicht sind Sonderabgaben mit Finanzierungsfunktion nur dann zulässig, wenn ein Zweck verfolgt wird, der über die bloße Mittelbeschaffung hinausgehet, eine homogene Gruppe belastet wird, die in einer spezifischen Beziehung zu dem mit der Abgabenerhebung verfolgten Zweck steht, ihr Aufkommen gruppennützig verwendet wird. Der Gesetzgeber sei darüber hinaus verpflichtet die Erhebung der Sonderabgabe zu prüfen und ggf. diese aufzuheben bzw. anzupassen, die zudem durch haushaltsrechtliche Informationspflichten ergänzt wären, um nämlich die Wahrnehmung der Planungs- und Kontrollaufgab en es Parlaments – wie der Öffentlichkeit – zu gewährleisten.

[1689] *Weber-Grellet*, NJW, 3657, 3662.

[1690] *Weber-Grellet*, NJW, 3657, 3661.

sprechend seiner Leistungsfähigkeit in Anspruch genommen werden.[1691] Entsprechend ist es verboten den Bürger über seine allgemeinen Steuerpflichten hinaus in beliebigem Umfang zu sonstigen, nicht an seiner Leistungsfähigkeit anknüpfenden Abgaben zu verpflichten.[1692]

Auch bei der Übertragung der Aufgaben im Rahmen der Vorratsdatenspeicherung handelt es sich um originär hoheitliche Aufgaben, die im alleinigen staatlichen Interesse stehen. Es kann daher argumentiert werden, dass aus Gründen der Steuerstaatlichkeit für die Kosten, die im Rahmen der Vorratsdatenspeicherung entstehen, eine finanzielle Kompensation vorgesehen werden muss.

Eine Ausnahme vom Prinzip der Steuerstaatlichkeit ist ausnahmsweise zulässig, wenn ein Privater die Kosten zurechenbar verursacht. In diesem Sinne argumentiert auch das *Bundesverfassungsgericht* im Urteil zur Vorratsdatenspeicherung.[1693] Im Hinblick darauf, dass die Regelungsbedürftigkeit erst aufgrund der marktwirtschaftlichen Betätigung der Telekommunikationsunternehmen entstanden und sie die Kosten wieder in den Markt integrieren könnten, könne die Kostenübertragung gerechtfertigt werden.[1694]

Diese Betrachtung kann aber kritisch hinterfragt werden, denn grundsätzlich gebietet es der Grundsatz der Steuerstaatlichkeit, dass die Erfüllung originär hoheitlicher Aufgaben durch den Staat erfolgt. Es ist zwar richtig, dass das Bedürfnis nach einer Regelung zur Vorrats-speicherung erst auf Grund der Ausweitung des Telekommunikationssektors entstanden ist. Jedoch führt die Abwälzung der Kosten auf die Telekommunikationsanbieter dazu, dass im Ergebnis der Kunde die Kosten für die Vorratsdatenspeicherung trägt. Damit ist es nicht der Staatsbürger der entsprechend seiner Leistungsfähigkeit durch die Steuerlast für die Kosten dieser Sicherheitsmaßnahme aufkommt, sondern es ist der Kunde der einzelnen Telekommunikationsanbieter, der entsprechend seines Telekommunikationsbedarfs für die Kosten der Vorratsdatenspeicherung zahlt. Hierfür ist kein zwingender argumentativer Zusammenhang erkennbar. Insofern widerspricht eine Übertragung der Kosten auf die Anbieter dem Grundsatz der Steuerstaatlichkeit.

9.2.1.3 Schutzpflichten zu Gunsten der Freiheit der Bürger

Staatliches Interesse ist in der Dimension Staat – Wirtschaft auch der Schutz der Telekommunikationsfreiheit der Bürger. Dies gilt vor allem im Hinblick auf das hohe Missbrauchsrisiko,[1695] das auf Grund der Speicherung bei den Telekommunikationsdiensteanbietern gesteigert wird. Das Missbrauchsrisiko wird gesteigert, da der Schutz vor Missbrauch nicht unmittelbar in staatlicher Hand liegt, sondern in den Händen Privater, die selbst ein Interesse an der Verwertung dieser Daten haben.

[1691] Insofern schützt die Finanzverfassung den Bürger vor Zugriff auf seine keineswegs unerschöpflichen Ressourcen, so *Wagner*, PharmR 2003, 409, 414.

[1692] *Schirra* 2002, 68; Dagegen spricht aber, dass ein Schutz vor willkürlichen Belastungen bereits durch Art. 3 Abs. 1 GG gewährleistet sei, so etwa *Arndt* NVwZ 1988, 787, 791.

[1693] BVerfGE 125, 260 (360 f.).

[1694] BVerfGE 125, 260 (361).

[1695] Vgl. dazu oben S. 184 f.

Der Staat muss, wenn er die Telekommunikationsdiensteanbieter zu Mindestspeicherfristen verpflichtet, seinem Schutzauftrag zu Gunsten der Grundrechte[1696] nachkommen indem er sicherstellt, dass die Freiheitsrechte der Bürger bei der Speicherung geachtet werden und insofern die Daten vor missbräuchlicher Nutzung geschützt sind. Er muss dafür sorgen, dass die innerhalb der ersten Dimension (Staat – Bürger) ermittelten verfassungsrechtlichen Anforderungen an die Datensicherheit, geachtet werden.[1697] Die in der ersten Dimension ermittelten Abwehrrechte des Bürgers gegenüber dem Staat, werden in der zweiten Dimension zu Schutzpflichten des Staates.[1698]

Dabei ist unter anderem „maßgeblich" „dass auch die Speicherung der von ihren Kunden aufgerufenen Internetseiten durch kommerzielle Dienstanbieter grundsätzlich untersagt ist".[1699] Der Staat muss also sicherstellen, dass private Anbieter nicht grundsätzlich die von ihren Kunden aufgerufenen Seiten speichern. Hier zeigt sich das Verbot einer umfassenden gesamtgesellschaftlichen Überwachung in seiner Schutzpflichtendimension.

9.2.1.4 Anforderungen der Wirtschaft an die Ausgestaltung

Im Verhältnis Staat – Wirtschaft kulminieren verschiedenste staatliche Interessen, die zum Teil auch eine gegenläufige Stoßrichtung haben. So ist staatliches Interesse sowohl die Kosten möglichst gering zu halten, als auch die Steuerhoheit zu wahren. Der Staat ist darauf angewiesen die Aufgabe zu übertragen, muss aber zugleich die Organisationshoheit behalten. Nahezu widersprüchlich zum Interesse, Sicherheit zu gewährleisten ist sodann, die einschlägige Schutzpflichtendimension der in der ersten Dimension berührten Freiheitsgrundrechte.

9.2.2 Wirtschaftliche Freiheit

Für die Anbieter von Telekommunikationsdienstleistungen[1700] bedeutet die Einführung der Verkehrsdatenspeicherung, dass zunächst erhebliche organisatorische und finanzielle Aufwendungen für die Einrichtung und Programmierung aufgebracht werden müssen (Investitionskosten). Es entstehen aber auch fortlaufend Kosten, um den Betrieb aufrecht zu erhalten (Betriebskosten). Dazu gehören auch die durch jeden Datenabruf verursachten Übermittlungskosten. Die Regelung kollidiert so mit verschiedenen verfassungsrechtlich geschützten Rechtspositionen, die die wirtschaftliche Freiheit schützen.

Die Einführung der Vorratsdatenspeicherung im Jahr 2008 verursachte bei den Telekommunikationsanbietern Kosten in mehrstelliger Millionenhöhe. Wobei die Angaben über die entstandenen Kosten stark variieren.[1701]

[1696] Insbesondere dem Telekommunikationsgeheimnis, Art. 10, dem Recht auf informationelle Selbstbestimmung aus Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1, der Berufsausübungsfreiheit aus Art. 12 Abs. 1, der Pressefreiheit aus Art. 5 sowie dem durch Art. 1 Abs. 1 GG absolut geschützten Kernbereich privater Lebensgestaltung.

[1697] Dazu oben Fn. 1549.

[1698] Dazu bereits oben S. 242 ff.

[1699] BVerfGE 125, 260 (324).

[1700] Eine Definition des Begriffs TK-Anbieter findet sich oben S. 140.

[1701] *Eco* gab 2007 in einer Stellungnahme zu dem kurz darauf verabschiedeten Gesetzesentwurf zur Vorratsdatenspeicherung an, dass insgesamt Kosten in Höhe von 241 Mio. € entstünden.

Unabhängig von konkreten Zahlen steht jedoch fest, dass die tatsächlich entstehenden Kosten von der konkreten Ausgestaltung der Vorratsdatenspeicherung abhängen und insoweit nur schwerlich abstrakt veranschlagt werden können. Die Höhe der Investitionskosten hängt unter anderem davon ab, wie viele Daten wie lange gespeichert werden, ob diese automatisch generiert werden und vor allem auch welche Sicherheitsvorkehrungen bei der Speicherung vorgesehen sind.[1702] Die Höhe der Betriebs-kosten wird durch die Organisation des Abrufverfahrens stark beeinflusst – etwa ob diese manuell durchgeführt werden oder ob automatisierte Verfahren eingesetzt werden. Einfluss hat auch die Anzahl der zu erwartenden Abfragen. Denn desto häufiger die Daten abgerufen werden, desto höher sind die Abrufkosten.

Die entstehenden Kosten korrelieren nicht mit der Größe des Unternehmens. Die Modifikation der laufenden Geschäftsprozesse sowie die Einrichtung der Datenspeicher erfordern umfassende und jeweils teure Arbeiten an der Informationstechnik. Diese sind nicht umso aufwendiger, je mehr Datensätze zu speichern sind, sondern verursachen auch bei wenigen Daten bereits sehr hohe Investitionskosten. Sie steigen also gerade nicht proportional zur Größe der Betreiber.[1703]

9.2.2.1 Berufsfreiheit

Die Verpflichtung zur Vorratsdatenspeicherung kollidiert mit den Interessen der Telekommunikationsanbieter frei ihrer Tätigkeit nachzugehen. Dieses Interesse wird durch die Berufsfreiheit geschützt,[1704] die auf juristische Personen ihrem Wesen nach anwendbar ist.[1705] Zur Beurteilung der Verhältnismäßigkeit von Eingriffen in Art. 12 Abs. 1 GG wird die Drei-Stufen-Theorie herangezogen,[1706] wonach Eingriffe in die Berufswahl stärker rechtfertigungsbedürftig sind als bloße Regelungen der Berufsausübung.[1707]

---

http://www.eco.de/verband/202_2418.htm; In einem *FDP*-Papier von 2010 beruft sich diese auf Angaben von eco und führt aus, dass die Vorratsdatenspeicherung Kosten in Höhe von sogar 336 Mio. Euro verursachen würde, so http://www.marco-buschmann.de/files/26-949/10_12_13_Argumentationshilfe_VDS.pdf; Laut Angaben des Brachenverbands *bitkom* beliefen sich die Kosten hingegen lediglich auf 50 - 75 Mio. € (zitiert nach *Gausling* 2010, 150); Im Evaluationsbericht der Kommission wird davon ausgegangen, dass sich die Kosten bei einem Internetprovider mit 500.000 Kunden auf 375.240 € im ersten Jahr belaufen, Kom (2011) 225, 31.

[1702] Der Generalsekretär der österreichischen Vertretung der ISPs (ISPA) Wildberger führt dazu in einem Interview aus, dass die Kosten für „die Implementierung (…) bei etwa 15 bis 20 Millionen Euro (liegen), wobei es dabei natürlich auf die wahrscheinlich per Verordnung festgelegten Parameter der technischen Umsetzung ankommt,“ www.computerwelt.at/detailArticle.asp?a=133018&n=5&n2=0.

[1703] A. A. KOM (2011) 225, 31 mit Verweis auf: http://www.etsi.org/website/technologies/lawfulinterception.aspx. Allerdings ist nicht ersichtlich wie die angegebene Fundstelle belegen soll, dass die Kosten proportional zur Größe des Unternehmens entstehen.

[1704] Zum Schutzbereich der Berufsfreiheit, vgl. schon oben Kap. 9.1.2.4.1.

[1705] Art. 19 Abs. 2 GG.

[1706] Mit dieser versuchte das *BVerfG* in der frühen Apothekenentscheidung (BVerfGE 7, 377 (408)) die Verhältnismäßigkeitsprüfung im Rahmen der Berufsfreiheit zu typisieren, dazu *Manssen,* in: *Mangoldt/Klein/Starck,* GG 2010, Art. 12 Rn. 140. Es wird dabei unterschieden zwischen Berufsausübungsregelungen, subjektiven und objektiven Berufswahlregelungen.

[1707] *Schirra* 2002, 90.

Das *Bundesverfassungsgericht* befasste sich im Urteil zur Vorratsdatenspeicherung auch mit der Klage einer Anonymisierungsdienstleisterin. [1708] Das Gericht stellte hier fest, dass es sich bei der Verpflichtung einer Anbieterin von Anonymisierungsdiensten um eine Berufsausübungsregelung handle und nicht etwa um eine Berufswahlregel, wie die Beschwerdeführerin vorgebracht hatte. Denn das Angebot von Anonymisierungsdiensten werde durch die Verpflichtung zur Vorratsdatenspeicherung nicht unmöglich gemacht.[1709] Der Eingriff verfolge einen legitimen Zweck, sei geeignet und erforderlich. Weder die Übertragung der Speicherungsverpflichtung noch die finanziellen Lasten seien unverhältnismäßig.[1710] Eine erdrosselnde Wirkung sei nicht substantiiert vorgetragen worden.

Das Gericht handelt die Frage der Verhältnismäßigkeit des Eingriffs in die Berufsfreiheit relativ kurz ab. Dennoch könnte gerade der Eingriff in die Berufsfreiheit der Telekommunikationsanbieter im Fall einer Neuregelung den Anknüpfungspunkt für deren Verfassungswidrigkeit bilden.

9.2.2.1.1 Eingriff in die Berufsfreiheit

Wie das *Bundesverfassungsgericht* festgestellt hat, handelt es sich bei der Verpflichtung zur Speicherung von Verkehrsdaten auf Vorrat und zur Übermittlung der Verkehrsdaten unter bestimmten Voraussetzungen, um Berufsausübungsregelungen,[1711] die auf der ersten Stufe angesiedelt sind und die grundsätzlich mit jeder vernünftigen Erwägung des Allgemeinwohls legitimiert werden können.[1712] Allerdings entbindet diese grundlegende Einordnung auf der ersten, der drei Stufen, nicht von einer konkreten Verhältnismäßigkeitsprüfung.[1713] Die Maßnahme ist hinsichtlich ihrer Geeignet-

[1708] Verfahren 1 BvR 256/08.

[1709] „Sie ermöglichen damit Nutzern, die eine statische (und folglich offene) IP-Adresse haben, ihre Identität zu verbergen und schützen andere Nutzer vor Hackern oder sonstigem illegalen Zugriff", BVerfGE 125, 260 (359).

[1710] BVerfGE 125, 260 (359 f.).

[1711] Die Verpflichtung zur Speicherung wie zur Übermittlung stellen sich als technische Maßgaben dar. Auch in Bezug auf Anonymisierungsdienstleister soll es sich, nach Ansicht des *BVerfG*, dabei nicht um Berufswahlregelungen handeln, da die Berufswahl durch die Speicherungsverpflichtung nicht objektiv unmöglich gemacht wird. Schließlich können Anonymisierungsdienste ihren Nutzern weiterhin anbieten, ohne Identifizierungsmöglichkeit der IP-Adresse durch Private im Internet zu surfen, was für Kunden mit statischer IP-Adresse von Bedeutung ist. Da die Anonymisierung nur gegenüber staatlichen Zugriffen aufgehoben wird, wären lediglich diejenigen Kunden, deren Anonymisierungsinteresse darin liegt nicht von staatlichen Behörden bei der Begehung schwerer Delikte entdeckt zu werden. BVerfGE 125, 260 (359).

[1712] *Wieland*, in *Dreier*, GG 2004, Art. 12, Rn. 117; Die Einordnung auf der ersten Stufe dient aber nur als Indiz für die Beurteilung der Rechtfertigungsfähigkeit des Eingriffs. Denn insgesamt erweist sich die Kategorisierung in drei Stufen als zu unspezifisch. So kommt etwa Berufsausübungsregelungen nicht immer nur eine geringes Eingriffsgewicht zu, da sie auch so schwer wiegen können, dass sie Berufsangehörige zur Berufsaufgabe zwingen *Ipsen*, JuS 1990, 634, 635; *Schwabe*, DÖV 1969, 734, 737; vgl. dazu auch BVerfGE 121, 317 (380) – für solche Differenzierungen ist die Drei-Stufen-Theorie jedoch offen. Kritisch zur Drei-Stufen-Theorie *Manssen* in *Mangoldt/Klein/Starck,* GG 2010, Art. 12 Rn. 141 ff.

[1713] Auch die Drei-Stufen-Theorie sollte eine Abkehr von der Verhältnismäßigkeitsprüfung einläuten, sondern diese lediglich strukturieren; BVerfGE 7, 377 (408); vgl. *Manssen,* in: *Mangoldt/Klein/*

heit, Erforderlichkeit und ihre Verhältnismäßigkeit im engeren Sinne (Zumutbarkeit) zu prüfen.

Das *Bundesverfassungsgericht* prüft Geeignetheit und Erforderlichkeit von Speicherungsverpflichtung und Kostenübertragung nicht getrennt. Dafür spricht, dass eine gesonderte Prüfung im Ergebnis dazu führen würde, dass jede kostenträchtige Indienstnahme ausscheiden würde, da immer mit einer Kostenentschädigung eine mildere Alternative denkbar ist.[1714] Ein solches Ergebnis widerspricht aber Art. 14 Abs. 3 GG, der Entschädigungen nur bei Enteignungen vorsieht.[1715] Der Annahme, dass eine Kostenerstattung stets das mildere Mittel und insofern bei jeder Übertragung einer staatlichen Aufgabe auf Private vorzusehen wäre, steht zudem entgegen, dass die Freiheitsbeschränkung der Inpflichtnahme an sich durch eine Kostenerstattung nicht abgemildert wird. Dies entspricht dem höchstrichterlich anerkannten Grundsatz, dass eine rechtswidrige Grundrechtsbeschränkung nicht durch eine finanzielle Erstattung auf Sekundärebene ausgeglichen werden kann.[1716] Insofern ist in Übereinstimmung mit dem *Bundesverfassungsgericht* die Erforderlichkeit der Kostenübertragung nicht gesondert zu prüfen.[1717]

Die Zumutbarkeit ist sodann für die Speicherungs- und Übermittlungsverpflichtung sowie die Kostenübertragungsregelung einzeln zu prüfen.

Es wird schließlich im Sinne der erweiterten Verhältnismäßigkeitsprüfung erörtert, ob die Übertragung auch unverzichtbar und alternativlos ist und wie ein bestmöglicher Interessenausgleich erzielt werden kann.

9.2.2.1.2 Geeignet und erforderlich, aber alternativ lösbar

Die Verpflichtung der Telekommunikationsunternehmen zur Speicherung der Verkehrsdaten legitimiert sich aus der Zielsetzung einer Effektivierung der Strafverfolgung, der Gefahrenabwehr und der Aufgaben der Geheimdienste.[1718] Sie ist zu diesem Zweck auch geeignet und erforderlich.[1719]

Im Sinne einer Verhältnismäßigkeitsprüfung Plus ist der Eingriff in die Berufsfreiheit jedoch verzichtbar. Würde auf die Speicherungsverpflichtung verzichtet, wären allein die zu Vertragszwecken gespeicherten Verkehrsdaten vorhanden. Da es in diesem Fall

---

Starck, GG 2010, Art. 12 Rn. 140, der davon spricht, dass die Apothekenentscheidung eine „Typisierung" der Verhältnismäßigkeitsprüfung versuchte.

[1714] *Schirra* 2002, 109.

[1715] *Schirra* 2002, 109.

[1716] BVerfGE 58, 300; In dieser Entscheidung hat das *BVerfG* mit dem Grundsatz des „Dulde und liquidiere" gebrochen, vgl. ausführlich dazu *Schirra* 2002, 109.

[1717] *Schirra* 2002, 110.

[1718] BVerfGE 125, 260 (316, 360).

[1719] Denn sie ist zur Förderung dieses Ziels geeignet. Auch ist sie erforderlich, da die tatsächliche Sach- und Funktionsherrschaft über die Telekommunikationsanlagen bei den Betreibern liegt, muss die Speicherung durch die TK-Anbieter erfolgen. Eine unmittelbare Übermittlung sämtlicher Verkehrsdaten an den Staat kommt auf Grund der „damit verbundenen Risiken sowohl für den Schutz des Telekommunikationsgeheimnisses als auch für die Sicherheit und Vollständigkeit der Daten" nicht als milderes Mittel in Betracht, BVerfGE 125, 260 (360).

nicht zu erheblichen Schutzlücken kommt,[1720] ist ein Verzicht auf die Vorratsdatenspeicherung möglich.[1721] Insbesondere kann die Erforderlichkeit der Verpflichtung zur Vorratsdatenspeicherung von Anonymisierungsanbietern und von reinen Geschäftskundenanbietern bezweifelt werden. Denn die von diesen zu speichernden Daten sind überwiegend für die Arbeit der Ermittlungsbehörden ohne Belang sind.[1722] Eine Vorratsdatenspeicherung ohne derartige Anbieter zu verpflichten, stellt sich zumindest aus deren Perspektive als mildere Alternative dar, die einen annähernd hohen Beitrag zur Sicherheit leistet.

Als Alternative stellt sich auch in der Dimension Staat – Wirtschaft die Frage, ob es sich bei einem Quick-Freeze-Verfahren um eine grundrechtsschonendere Alternative handelt. Dies kann (aus Sicht der Telekommunikationsunternehmen) bezweifelt werden, da hier die Anbieter nicht einmalig eine Infrastruktur errichten müssen, die gewährleistet, dass sämtliche Daten gespeichert werden, sondern konstant und unmittelbar die Speicherungsanordnungen umsetzen müssen. Erforderlich ist insofern ein höherer personeller Einsatz. Die Betriebskosten würden daher bei einem Quick-Freeze-Verfahren deutlich höher ausfallen als bei einer Vorratsspeicherung. Allerdings sind die Investitionskosten voraussichtlich geringer, da eben keine Datenbanken mit einem besonders hohen Sicherheitsstandard geschaffen werden müssen.[1723] Dies zeigt, dass es sich aus Perspektive der Telekommunikationsanbieter um zwei ungleiche Alternativen handelt. Welche davon grundrechtsschonender ist, kann abstrakt nicht bewertet werden. Deutlich wird jedoch, dass eine Kombination beider Ansätze für die Unternehmen in jedem Fall belastender wäre. Hier müssten die Anbieter beide Konzepte umsetzen, was voraussichtlich den größten Aufwand und die höchsten Kosten verursachen würde.

9.2.2.1.3 Zumutbarkeit der Indienstnahme

Für die Beurteilung der Angemessenheit der Übertragung der Speicherungsverpflichtung auf die Telekommunikationsanbieter kommt es darauf an, ob diese Übertragung einer staatlichen Aufgabe auf die privaten Anbieter zumutbar ist.

Bei der Übertragung staatlicher Aufgaben auf Private wird unterschieden zwischen Indienstnahmen und Eigensicherungspflichten.[1724] Während bei Eigensicherungspflichten ein sowohl eigenes als auch staatliches Interesse besteht,[1725] knüpft eine Indienst-

[1720] Vgl. oben Kap. 4.4.2.
[1721] Vgl. oben S. 203.
[1722] *Knierim* 2011b, 441 f.
[1723] Ausführlich zu den unterschiedlichen Anforderungen an die Technikgestaltung bei Vorratsdatenspeicherung und Quick-Freeze, *Knierim* 2011a.
[1724] Eine solche Differenzierung erfolgt im Rahmen von Art. 14 GG. Wenn man der Annahme folgt, dass es sich bei der Indienstnahme um eine umgekehrte Gebührenkonstellation handelt, kann die Argumentation mit der Sozialpflichtigkeit des Eigentums auf Art. 12 GG übertragen werden, jedenfalls insoweit untersucht wird, wie die i.R.d. beruflichen Tätigkeit zu erfüllende Aufgabe zu beurteilen ist.
[1725] Es handelt sich insofern um Eigensicherungspflichten, wenn die auferlegte Maßnahmen zur öffentlichen Sicherheitsgewährleistung erforderlich ist und sich eine Eigenverantwortung des Privaten aus der Sozialpflichtigkeit des Eigentums ableiten lässt, dazu *Braun*, K&R 2009, 386, Rn. 386; Zu Eigensicherungspflichten im Luftverkehrsrecht und der hier zeitweise umstrittenen Abgrenzung

nahme[1726] allein an hoheitlichen Interessen an.[1727] Die Verpflichtung zur Vorratsdatenspeicherung begünstigt mit der Zielsetzung Strafverfolgung und Gefahrenabwehr ausschließlich den Staat (und die Gesamtheit aller Staatsbürger). Es handelt sich somit um die Wahrnehmung einer originär hoheitlichen Aufgabe, also um eine Indienstnahme.[1728]

Der Eingriff dient dem Schutz hoher Gemeinschaftsgüter. Da die tatsächliche Sach- und Funktionsherrschaft über die Telekommunikationsanlagen bei den Betreibern entsprechender Telekommunikationseinrichtungen liegt, muss, um überhaupt die Speicherung realisieren zu können, in die Berufsfreiheit der Telekommunikationsdiensteanbieter eingegriffen werden. Schon aufgrund dieser Realisierungsbedingungen jeglicher Telefonüberwachung seit der Liberalisierung des Telekommunikationsmarktes kann der Eingriff in Gestalt einer Berufsausübungsregelung mit der Verfolgung von Gemeinwohlzwecken gerechtfertigt werden. Es sind insofern zunächst die rein faktischen Verwirklichungsbedingungen, die den Eingriff durch Speicherungs- und Übermittlungsverpflichtung rechtfertigen.

Wesentlich für die Rechtfertigungsfähigkeit einer Indienstnahme ist grundsätzlich, dass es sich um keine unternehmensfremde Tätigkeit handelt. Dies ist bei der Vorratsdatenspeicherung kritisch zu hinterfragen. Es wird argumentiert, dass die Verpflichtung zur Vorratsdatenspeicherung unternehmensfremd sei, da eine Datenerhebung für Vertrags- und Abrechnungszwecke, die nicht erforderlich ist, ordnungswidrig ist.[1729]

Eine solche Betrachtung überzeugt im Ergebnis nicht. Schließlich handelt es sich bei der konkreten Aufgabe, nämlich der Verpflichtung zur Speicherung von Telekommunikationsverkehrsdaten, um eine Handlung, die zwar zu anderen Zwecken im Unternehmen erfolgt, aber als Maßnahme an sich zum üblichen Handeln gehört. Das gleiche gilt auch für die Datenübermittlung an die zuständigen behördlichen Stellen für Strafverfolgungs- und Gefahrenabwehrzwecke. Als technischer Vorgang ist dieser nicht un-

---

zwischen hoheitlicher Gefahrenabwehr und Eigensicherungspflichten, *Schneider*, NVwZ 1988, 605.

[1726] Indienstnahme ist die Bezeichnung für einseitige staatliche Maßnahmen, aufgrund derer im öffentlichen Interesse liegende Handlungspflichten einem Privaten auferlegt werden, und sich diese nicht allein in der Zahlung eines Geldbetrags erschöpfen, *Schirra* 2002, 14.

[1727] Indienstnahme und Eigensicherungspflichten werden zum Teil auch als einheitliche Rechtsinstitute betrachtet, dazu *Braun*, K&R 2009, 386.

[1728] Die Frage, ob es sich um Eigensicherungspflicht oder um eine Indienstnahme dient auch als Indiz für die Frage der Rechtfertigungsfähigkeit der Kostenübertragung. Jedoch kann auch wenn sich eine Aufgabenübertragung als Indienstnahme darstellt, die Übertragung der Kostenlast gerechtfertigt werden, dafür sind allerdings zusätzliche Rechtfertigungsmomente erforderlich.

[1729] *Berger*, CR 2008, 557, 559 bezieht sich hier auf die Auslandskopfüberwachung. Die Argumentation ist jedoch übertragbar; In eine ähnliche Richtung zielt die Argumentation, dass es sich dabei um das genaue Gegenteil der von den Netzbetreibern angebotenen Dienstleistung handle: „Obwohl sie ihren Kunden gegenüber eine verfassungsrechtliche, gesetzliche und vertragliche Pflicht haben, die ungestörte und anonymisierte Übermittlung von Sprache und Daten zu gewährleisten, sollen sie die Möglichkeiten vorhalten, diese Anonymität zu durchbrechen und bei der Überwachung des Kommunikationsverkehrs ihrer Kunden mitzuwirken“, so *V. Hammer*stein, MMR 2004, 222, 225.

ternehmensfremd.[1730] Dies zeigt sich auch daran, dass nicht bezweifelt werden kann, dass in einem Telekommunikationsunternehmen das technische Knowhow zur Speicherung und Verarbeitung von Verkehrsdaten zwingend vorhanden ist. Insofern handelt es sich bei der Verpflichtung zur Vorratsdatenspeicherung letztlich nur um eine quantitative Steigerung von Belastungen.[1731]

Zu fragen ist neben der grundsätzlichen Rechtfertigungsfähigkeit der Indienstnahme, ob nicht mit einer Verpflichtung zur Vorratsdatenspeicherung private Unternehmen unzulässig mit Staatsaufgaben betraut werden. Das *Bundesverfassungsgericht* führt dazu aus, dass sich „eine kategorische Trennung von „Staatsaufgaben" und „privaten Aufgaben" mit der Folge der grundsätzlichen Unzulässigkeit einer Indienstnahme für Gemeinwohlzwecke von Privaten" der Verfassung nicht entnehmen lasse.[1732] Allerdings ist auch bei der Übertragung der Speicherungsverpflichtung auf die Privaten das staatliche Gewaltmonopol zu beachten.[1733]

Im Ergebnis kommt es bei der Ausgestaltung einer Vorratsdatenspeicherung darauf an, dass auf die Anbieter keine unternehmensfremden Aufgaben übertragen werden und der Staat die Organisationshoheit behält, denn nur dann handelt es sich um eine grundsätzlich rechtfertigungsfähige Indienstnahme. Eine andere Frage, ist ob die Übertragung der Kostenlast zumutbar ist.

9.2.2.1.4 Zumutbarkeit der Kostenübertragung

Das *Bundesverfassungsgericht* hat festgestellt, dass die Kostenübertragung auf die Telekommunikationsanbieter grundsätzlich gerechtfertigt sei, solange nicht substantiiert vorgetragen werde, dass diese eine erdrosselnde Wirkung habe.[1734] Die Verfassungsmäßigkeit der Überbürdung der Kosten war zuvor vielfach bestritten worden.[1735] Die Verpflichtung zur Vorratsdatenspeicherung ist nicht die erste und einzige kostenträchtige Indienstnahme Privater.[1736]

[1730] *OVG Berlin-Brandenburg*, Urt. v. 2.12.2009; MMR 2010, 269.

[1731] *OVG Berlin-Brandenburg*, Urt. v. 2.12.2009; MMR 2010, 269.

[1732] BVerfGE 125, 260 (361).

[1733] Zu diesem, vgl. oben Kap. 9.2.1.1.

[1734] BVerfGE 125, 260 (362) „Dass die Kostenlasten in dieser Weise erdrosselnde Wirkungen haben, ist weder substantiiert vorgebracht noch erkennbar". *Heun* betont die Möglichkeit, dass unter Umständen bei einer künftigen Gesetzgebung die Beurteilung der Übertragung der Kostenlast anders ausfallen könnte, *Heun*, CR 2010, 247, 248 ff.

[1735] Dazu *Gausling* 2010, 150 ff. m. w. Nachw.; auch in der Rechtsprechung wurde auf Grund der Kostenübertragung die Verpflichtung zur Vorratsdatenspeicherung zum Teil als unverhältnismäßig bewertet: *VG Berlin*, Beschl. v. 17.10.2008, Az. *VG* 27 A 232.08; a.A. O*VG Berlin*, Urt. v. 2.12.2009, Az.: S 81.08 (MMR 2010, 269 ff.); die Kritik an der Heranziehung Privater zur Gefahrenabwehr allein auf Grund einer Sach- und Verantwortungsnähe, wurde auch im Rahmen der Auslandskopfüberwachung diskutiert, für eine Übertragbarkeit dieser auf die VDS Berger, CR 2008, 557, 560 ; vgl. dazu auch *Heckmann*, jurisPR-ITR 2010, Anm. 1.

[1736] Kosten werden auch übertragen auf Private im Rahmen von § 16 EEG (Vergütung von Betreibern von Anlagen Erneuerbarer Energien); Pharmaunternehmen werden verpflichtet, Apotheken einen Abschlag zu gewähren für die Krankenkassen mit dem Ziel das Krankenversicherungssystem zu stabilisieren, §§ 130, 130a SGBV. Eine ausführliche Darstellung diverser kostenträchtiger Indienstnahmen findet sich bei *Schirra* 2002, 14 ff.; grundlegend aus der Rspr. des *BVerfG* E 30, 292

Im Urteil zur Vorratsdatenspeicherung führt das *Bundesverfassungsgericht* aus, dass der Gesetzgeber einen „weiten Gestaltungsspielraum" dabei habe, „welche Pflichten zur Sicherstellung von Gemeinwohlbelangen er Privaten im Rahmen ihrer Berufstätigkeit" auferlege.[1737] Dabei könne er grundsätzlich auch Lasten, „die als Folge kommerzieller Aktivitäten regelungsbedürftig sind, den entsprechenden Marktakteuren auferlegen, um die damit verbundenen Kosten auf diese Weise in den Markt und den Marktpreis zu integrieren". Der Gesetzgeber sei „nicht darauf beschränkt, Private nur dann in Dienst zu nehmen, wenn ihre berufliche Tätigkeit unmittelbar Gefahren auslösen kann oder sie hinsichtlich dieser Gefahren unmittelbar ein Verschulden trifft". Es genüge vielmehr eine „hinreichende Sach- und Verantwortungsnähe" zwischen der beruflichen Tätigkeit und der auferlegten Verpflichtung.[1738]

Diese Konstruktion, nach der eine kostenpflichtige Indienstnahme allein mit einer Kausalitätsprüfung und Sach- und Verantwortungsnähe begründet wird, ist wenig überzeugend, wenn man die kostenpflichtige Indienstnahme als umgekehrte Gebührenkonstellation betrachtet:[1739] Gebühren sind Gegenleistungen für eine Amtshandlung oder für die Inanspruchnahme einer öffentlichen Einrichtung.[1740] Sie werden erhoben für eine staatliche Leistung, wenn diese von einem Bürger veranlasst wurde oder ihm zurechenbar ist.[1741] Bei einer Indienstnahme ist hingegen Leistungserbringer nicht der Staat sondern der Grundrechtsträger. Potentieller Gebührenschuldner wäre dementsprechend der Staat. Wenn man diesem Grundsatz folgt, müsste folglich der Staat nur dann die entstehenden Kosten nicht vergüten, wenn die Kosten durch den Grundrechtsträger selbst veranlasst wurden. Die Rechtfertigung kann insoweit dann in der (Mit-)Verantwortung des Grundrechtsträgers für das Entstehen der Kosten gesehen werden.[1742] Ein solcher allgemeiner Rechtsgedanke kann unserer Rechtsordnung entnommen werden: Gesetzliche, mit Kostenlasten verbundene Freiheitsbeschränkungen können dann gerechtfertigt werden, wenn den Grundrechtsträger Verantwortung für die Folgen trifft, die seine eigene Freiheitsausübung für ein bestimmtes Gemeinwohl-

(Mineralölbevorratung); die entschädigungslose Inanspruchnahme im Rahmen des Kontenabrufverfahrens erachtet *Hoffmann,* WM 2010, 193, 199 f. mit überzeugenden Argumenten als verfassungswidrig.

[1737] BVerfGE 125, 260 (339 f.; 361).

[1738] BVerfGE 125, 260 (362).

[1739] *Starck*, in *Mangoldt/Klein/Starck,* GG 2010, Art. 3 Rn. 389.

[1740] *Starck*, in *Mangoldt/Klein/Starck,* GG 2010, Art. 3 Rn. 117. Sie unterscheidet sich insofern vom Steuerbegriff, als eine Gebühr durch eine „Gegenleistung" gekennzeichnet und zwar sowohl in Bezug auf die Austauschgerechtigkeit, eine Erscheinungsform der Gleichheit, als auch auf die verhältnismäßige Gleichheit unter den Gebührenschuldnern. Gebühren werden nach dem Kostendeckungsprinzip und dem Äquivalenzprinzip bestimmt. Gebührenpflichtiger ist der, der eine Einrichtung des öffentlichen Rechts benutzt oder Begünstigter oder Veranlasser einer Amtshandlung ist.

[1741] *Starck*, in *Mangoldt/Klein/Starck,* GG 2010, Art. 3 Rn. 119.

[1742] Dieser Rechtsgedanke, dass soweit eine (Mit-)Verantwortlichkeit gegeben ist eine kostenträchtige Indienstnahme gerechtfertigt werden kann, findet sich auch im Polizei-, allgemeinem Verwaltungs-, Finanzverfassungs- und Staatshaftungsrecht.

gut hat.[1743] Dies zeigt sich auch im Grundsatz der Steuerstaatlichkeit und der staatsbürgerlichen Lastengleichheit.[1744]

Insofern ist die Übertagung der Kostenlast bei einer Indienstnahme problematisch, wenn das unternehmerische Handeln nicht bereits per se gefährlich ist, sondern lediglich die Voraus-setzungen dafür schafft, dass Dritte zu einem späteren Zeitpunkt in gefährdender Weise daran anknüpfen,[1745] wie es auch bei der Verpflichtung zur Vorratsdatenspeicherung der Fall ist.

Entscheidend für die Frage der Zumutbarkeit der Kostenübertragung ist schließlich die Frage, wie die Verantwortungsbeziehung ausgestaltet sein muss. Genügt eine Kausalität oder muss die Gefährdung dem Unternehmen zurechenbar sein?

In der Literatur wird zum Teil eine vollumfängliche Folgenverantwortung verlangt. Das Kosten verursachende Verhalten müsse dem vermeintlichen Kostenschuldner unmittelbar zurechenbar sein. Denn nur so könnte eine Lastengleichheit gewährleistet werden, ansonsten drohe eine willkürliche Verteilung der Kosten, die an sich im Interesse der Allgemeinheit entstehen.[1746]

Nach der Theorie von der objektiven Zurechnung ist ein Erfolg nur dann zurechenbar, wenn der Täter eine rechtlich missbilligte Gefahr geschaffen hat, die sich im tatbestandlichen Erfolg realisiert.[1747] Die Telekommunikationsanbieter schaffen jedoch mit dem Angebot von Telekommunikationsdienstleistungen keine rechtlich missbilligte Gefahr. Vielmehr ist das Angebot von Telekommunikationsdienstleistungen wesentlich für die Prosperität der modernen Gesellschaft.[1748]

Zum Teil wird die Zurechnung damit begründet, dass die Netzbetreiber die „Tarnkappe" für die Begehung von Straftaten liefern.[1749] Dagegen spricht jedoch, dass so letztlich eine Verantwortlichkeit allein damit begründet wird, dass die Überwachung in diesem gesellschaftlichen Bereich aufwendiger ist.[1750] Zudem kann gegen diese Tarnkappenargumentation angeführt werden, dass sie letztlich jedes technische Leistungsangebot, das von Kriminellen missbräuchlich genutzt werden kann, diskreditiert.[1751] Schließlich spricht dagegen, dass sich keine sachliche Verantwortung der Telekom-

---

[1743] Dem geht *Kube* ausführlich nach und untersucht dabei die polizeirechtliche Nichtstörerdogmatik, die Grundsätze des Staatshaftungsrechts, das verwaltungsrechtliche Kopplungsverbot und das Finanzverfassungsrecht, *Kube*, JZ 2010, 265, 267 f.

[1744] Zu diesen ausführlich oben Kap. 9.2.1.2.

[1745] *Schirra* 2002, 125.

[1746] Dazu *Waechter*, VerwArch 1996, 68, 75; zur Kritik an der Argumentation mit dem Begriff „Sachnähe", *Ders*., 77.

[1747] Diese wurde im Strafrecht begründet, BGHSt 14, 193 (Jauchegrubenfall).

[1748] Vgl. dazu oben Kap.1.1.3.3; zur Bedeutung der Telekommunikationsfreiheit für die Freiheitsausübung insgesamt, vgl. oben Kap. 2.1.3.3.

[1749] Die Tarnkappentheorie geht zurück auf *Waechter*, VerwArch 1996, 68, 81 f. . Wer eine „Tarnkappe" in den Verkehr bringt, müsse für Zwecke der Strafverfolgung entschädigungslos eine Reidentifizierungsmöglichkeit bereitstellen.

[1750] *Sievers* 2002, 149.

[1751] *Scholz*, Archiv PT 1995, 169, 185.

munikationsdiensteanbieter für strafbare Inhalte besteht und sie insofern gerade nicht verantwortlich sind, wenn ihr Angebot zu kriminellen Zwecken genutzt wird.[1752]

Nicht wegen des In-Verkehr-Bringens einer Tarnkappe, sondern auf Grund einer „Tropfentheorie" begründet *Mansen* die Verantwortungsbeziehung, die die Übertragung der Kostenlast rechtfertigen könne. Derjenige, der den „guten Tropfen" ernte – im Fall der Vorratsdatenspeicherung die Möglichkeit der wirtschaftlichen Betätigung im Telekommunikationssektor –, müsse dafür auch den „schlechten Tropfen" übernehmen und damit die notwendigen Kosten für staatliche Überwachungsmaßnahmen.[1753]

Dem folgt im Ergebnis das *Bundesverfassungsgericht,* wenn es zur Begründung der Kostenübertragung ausführt: „So wie die Telekommunikationsunternehmen die neuen Chancen der Telekommunikationstechnik zur Gewinnerzielung nutzen können, müssen sie auch die Kosten für die Einhegung der neuen Sicherheitsrisiken, die mit der Telekommunikation verbunden sind, übernehmen und in ihren Preisen verarbeiten".[1754]

Historisch lässt sich jedoch entgegen der Auffassung des Verfassungsgerichts die Verantwortung nicht begründen. Denn zum Zeitpunkt der Liberalisierung des Telekommunikationssektors bestand keine Pflicht zur Vorratsdatenspeicherung, so dass auch die Feststellung, dass die Kosten *entsprechend* in den Markt integriert würden,[1755] fehl geht.[1756] Wenn man dieser Argumentation folgt, könnten letztlich auch die Kosten der Autobahnsicherheit den Autoherstellern auferlegt werden.

Gegen die Übertragung der Kosten auf die Telekommunikationsanbieter spricht schließlich, dass die Erforderlichkeit der Verpflichtung der Anbieter zur Speicherung darauf zurückgeht, dass auf Grund der Entwicklung von Flatrate-Tarifen nicht mehr ausreichend Daten zur Verfügung stehen. Diese Entwicklung ist letztlich jedoch aus datenschutzrechtlicher und somit auch unter verfassungsrechtlichen Gesichtspunkten begrüßenswert. Insofern erscheint es widersinnig, wenn den Anbietern Kosten aufer-

---

[1752] *Gausling* 2010, 155 f.

[1753] *Manssen*, Archiv PT 1998, 236, Rn. 242; krit. dazu: *Braun*, K&R 2009, 386, Rn. 389; kritisch dazu: *VG Berlin* v. 2.7.2008 – Az: VG 27 A 3.07.

[1754] BVerfGE 125, 260 (362).

[1755] „Der Gesetzgeber verlagert auf diese Weise die mit der Speicherung verbundenen Kosten entsprechend der Privatisierung des Telekommunikationssektors insgesamt in den Markt. So wie die Telekommunikationsunternehmen die neuen Chancen der Telekommunikationstechnik zur Gewinnerzielung nutzen können, müssen sie auch die Kosten für die Einhegung der neuen Sicherheitsrisiken, die mit der Telekommunikation verbunden sind, übernehmen und in ihren Preisen verarbeiten", BVerfGE 125, 260 (362).

[1756] *Gausling* 2010, 154 führt aus, dass der Gesetzgeber einen weiten Gestaltungsspielraum hat, solange die Annahme einer Sachnähe nicht willkürlich erscheint. Anders *Schirra* 2002, 126, der grundsätzlich die Tarnkappen-Theorie *Waechter*s bestätigt. Er führt aus, dass eine Tarnkappe schon im Zeitpunkt seiner Markteinführung als per se gefährlich einzustufen sei. Tarnkappen seien aber nicht die Regel. Und das Risiko neuer Entwicklungen zu kriminellen Zwecken bestünde generell. Diese Risiken würden aber durch die positive Auswirkung neuer Entwicklungen auf den Lebensstandard, die wirtschaftliche Prosperität und das Wohlergehen der Allgemeinheit in aller Regel aufgewogen. Es sei ungerecht, wenn der unmittelbare Nutzen der Gesamtbevölkerung zu Gute kommt, während die Privaten für mittelbare Gefährdungen haften.

legt werden, die aus sicherheitsrechtlichen Gründen nur entstehen, weil es eine aus Perspektive der Grundrechte begrüßenswerte Entwicklung gab. Letztlich beruht das Entstehen der (vermeintlichen) Datenlücke darauf, dass sich die Telekommunikationsanbieter verfassungs- und datenschutzkonform verhalten.

Im Ergebnis sprechen zahlreiche Gründe gegen eine Zumutbarkeit der Kostenübertragung auf die Telekommunikationsanbieter.

Auch spricht für eine Kostenverantwortlichkeit des Staates, der Grundsatz der Steuerstaatlichkeit.[1757] Denn die Budgetverantwortung führt letztlich auch zu einer sorgsameren Prüfung der Frage, ob dieses Instrument tatsächlich erforderlich ist und wie es ausgestaltet werden soll.

Dennoch ist auch zu berücksichtigen, dass im Grundgesetz auch die Sozialpflichtigkeit des Eigentums in Art. 14 Abs. 2 GG normiert ist. Darauf gründet die Argumentation, dass wer die Gewinnchancen einer neuen Technik nutzt, auch die finanzielle Verantwortung für die damit einhergehenden Sicherheitsrisiken übernehmen muss.[1758] Im Sinne eines optimierten Ausgleichs ist daher eine anteilige Übertragung der Kosten auf die Telekommunikationsanbieter denkbar.

9.2.2.1.5 Erdrosslungsverbot

Auch wenn die kostenpflichtige Indienstnahme der Telekommunikationsanbieter im Rahmen der Vorratsdatenspeicherung grundsätzlich gerechtfertigt ist, ist sie dennoch nicht grenzenlos rechtfertigungsfähig. So macht auch das *Bundesverfassungsgericht* deutlich, dass dies nur gilt, solange die Vorratsdatenspeicherung keine erdrosselnde Wirkung hat.[1759]

Das Erdrosslungsverbot ist der Rechtsprechung zum Steuerrecht entlehnt. Hier geht das *Bundesverfassungsgericht* davon aus, dass eine Besteuerung grundsätzlich nicht in die Berufsfreiheit eingreift, es sei denn, dass die Steuer dem Steuerpflichtigen die berufliche Tätigkeit „unmöglich" macht – sie also erdrosselnde Wirkung hat.[1760]

Im Beschluss zum Einkommensteuertarif (bzw. zur Höhe des Grundfreibetrags) konkretisierte das *Bundesverfassungsgericht* erstmals, wann eine solche erdrosselnde Wirkung einer steuerlichen Belastung anzunehmen ist.[1761] Die geschützten Freiheits-

---

[1757] Vgl. oben Kap. 9.2.1.2.

[1758] BVerfGE 125, 260 (362).

[1759] „Ein Gesetz, das die Berufsausübung in der Weise regelt, dass es Privaten bei der Ausübung ihres Berufs Pflichten auferlegt und dabei regelmäßig eine Vielzahl von Personen betrifft, ist nicht bereits dann unverhältnismäßig, wenn es einzelne Betroffene unzumutbar belastet, sondern erst dann, wenn es bei einer größeren Betroffenengruppe das Übermaßverbot verletzt. Dass die Kostenlasten in dieser Weise erdrosselnde Wirkungen haben, ist weder substanziiert vorgebracht noch erkennbar. Insofern ist nicht weiter zu prüfen, ob hinsichtlich besonderer Fallgruppen oder Sondersituationen aus dem Gesichtspunkt der Verhältnismäßigkeit Härteregelungen geboten sind", BVerfGE 125, 260 (362 f.).

[1760] BVerfGE 38, 61 (102); 70, 219 (230); 78, 232 (243); 82, 159 (190); „wirtschaftlich unmöglich macht", so BVerfGE 17, 135 (137); vgl. dazu auch ausführlich *Wernsmann* in *Hübschmann/Hepp/Spitaler,* AO/FGO, § 4 AO, Rn. 552.

[1761] BVerfGE 87,153 (169).

rechte dürfen nur so weit beschränkt werden, dass dem Steuerpflichtigen ein Kernbestand des Erfolgs seiner wirtschaftlichen Betätigung in Gestalt der grundsätzlichen Privatnützigkeit des Erworbenen und der Verfügungsbefugnis über die geschaffenen vermögenswerten Rechtspositionen erhalten bleibt.[1762] Eine erdrosselnde Wirkung ist demnach dann gegeben, „wenn die betroffenen Berufsangehörigen in aller Regel und nicht nur in Ausnahmefällen wirtschaftlich nicht mehr in der Lage sind, den gewählten Beruf ganz oder teilweise zur Grundlage ihrer Lebensführung“ zu machen.[1763] Das *OVG Münster* geht davon aus, dass keine erdrosselnde Wirkung vorliegt, wenn keine Veränderung am Markt erkennbar ist.[1764]

Im Rahmen von Art. 14 GG wird eine erdrosselnde Wirkung dann angenommen, wenn der Einzelne „übermäßig belastet“ und seine Vermögensverhältnisse „grundlegend beeinträchtigt“ werden.[1765]

Dass die Verpflichtung zur Vorratsdatenspeicherung in Gestalt einer kostenpflichtigen Indienstnahme erdrosselnde Wirkung haben könnte, ist nicht generell auszuschließen. In Anbetracht der hohen Anforderungen an die Datensicherheit ist es durchaus vorstellbar, dass insbesondere für sehr kleine Anbieter die Vorratsdatenspeicherung erdrosselnd wirken kann.[1766]

9.2.2.1.6 Schutz der Berufsfreiheit durch Europäische Grundrechte

Die Berufsfreiheit und die wirtschaftliche Betätigungsfreiheit werden in Art. 15 und 16 EU-GRCh. geschützt. Der Schutzumfang der Berufsfreiheit geht zum Teil über jenen von Art. 12 GG hinaus,[1767] allerdings wird die freie ökonomische Betätigung von juristischen Unternehmen nur durch Art. 16 EU-GRCh. schützt.[1768] Der *Europäische Gerichtshof* hat die Berufsfreiheit als „allgemeinen Grundsatz des Gemeinschaftsrechts“ anerkannt.[1769]

[1762] *Arndt*/ *Schumacher*, NJW 1995, 2603, 2604.

[1763] BVerfGE 13, 181 (187); 30, 292 (314) in Bezug auf die erdrosselnde Wirkung von Steuern: *BVerwG*, Beschl. v. 7.1. 1998, Az. 8 B 228.97; *BFH* v. 29.3.2006, Az. II R 59/04; so dann auch O*VG Münster* v. 4.12.2008, Az. 14 A 4006/04 (zum Betrieb von Spielautomaten/ Spielautomatensteuer); so dann auch *OVG Münster*, v. 15.11.2010, Az. 14a A 2292/09.

[1764] Dies sei dann der Fall, wenn in den letzten Jahren und nicht nur über einen kurzen Zeitraum, die Zahl der Spielhallen annähernd gleich geblieben ist, so *OVG Münster*, v. 4.12.2008 - 14 A 4006/04.

[1765] *Papier,* in: *Maunz/Dürig,* GG 2011, Art. 14, Rn. 165, mit zahlreichen Nachw. aus der Rspr Fn. 1.

[1766] *Hornung/Schnabel*, DVBl. 2010, 824, 833; Erforderlich ist dann ein substantiierter Vortrag, dass die Maßnahme erdrosselnde Wirkung hat. Dafür wären Sachverständigen-Gutachten einzuholen - dazu auch BVerfGE 125, 260 (363) „Solange die Einschätzung des Gesetzgebers nur durch Vermutungen und Behauptungen in Frage gestellt wird, kann das *BVerfG* dieser Frage nicht nachgehen.“

[1767] Etwa in Bezug auf Arbeitsbedingungen oder subjektive Rechte für ausländische Unionsbürger, *Wieland*, in: *Dreier*, GG 2004, Art. 12, Rn. 22.

[1768] *Ruffert,* in: *Calliess*/*Ruffert*, EUV/AEUV, 2011, Art. 15 Rn. 8.

[1769] *EuGH*, Rs. 4/73, Nold ./. Kommission, Slg. 1974, 491 ff.; *EuGH*, Rs. 44/79, Hauer ./. Land Rheinland-Pfalz, Slg. 1979, 3727 ff.; *EuGH*, Rs. C-280/93, Deutschland ./. Rat, Slg. 1994, I-4973 Tz. 78 ff.; *EuGH*, Rs. C-122/95 Deutschland *./. Rat*, Slg. 1998, I-973 Tz. 74 ff.; *EuGH*, Rs. C-210/03, Swedish Match AB ./. *Secretary of State for Health,* Slg. 2004, I-11893 Tz. 72 ff.

Die Europäische Menschenrechtskonvention selbst enthält keine spezielle Bestimmung über die Berufsfreiheit. Der *Europäische Gerichtshof für Menschenrechte* neigt aber zu einer extensiven Interpretation der in Art. 1 Zusatzprotokoll 1 gewährleisteten Eigentumsgarantie und subsumiert Verhaltensweisen darunter, die nach deutschem Grundrechtsverständnis der Berufsfreiheit unterfallen.[1770]

Der *Europäische Gerichtshof* hat den Begriff der wirtschaftlichen Betätigungsfreiheit bislang nicht eindeutig definiert. Aus den Erläuterungen des Präsidiums des Grundrechtskonvents ergibt sich, dass es sich bei der wirtschaftlichen Betätigungsfreiheit vornehmlich um eine Ausprägung der Berufsfreiheit handelt.[1771] Geschützt wird mithin jede Wirtschafts- oder Geschäftstätigkeit eines Unternehmens,[1772] also jede dem Erwerb dienende Tätigkeit, die auf Dauer angelegt ist.[1773] Dieser Schutzbereich wird durch die Verpflichtung der Telekommunikationsdiensteanbieter zur Speicherung der Telekommunikationsverkehrsdaten betroffen.[1774] Eine Pflicht zur Vorratsdatenspeicherung verursacht zwar keinen unmittelbaren Nachteil. Dies ist auch nicht der Zweck der Regelung. Faktisch wirkt sie sich aber stark auf die Unternehmensfreiheit der Telekommunikationsdiensteanbieter aus. Wobei auch europarechtlich anerkannt ist, dass selbst wenn ein Rechtsakt lediglich mittelbar oder auch faktisch auswirkt, ein Eingriff vorliegt.[1775] Da eine Vorratsdatenspeicherung bei den Telekommunikationsanbietern erhöhten Verwaltungsaufwand und Kosten für die Anschaffung und Bereithaltung der Infrastruktur verursacht, ist darin eine mittelbare Verkürzung des Schutzbereichs von Art. 16 EU-GRCh. zu sehen, mithin also ein Eingriff.[1776] Eingriffe und Einschränkungen der wirtschaftlichen Betätigungsfreiheit können gem. Art. 52 Abs. 1 EU-GRCh. gerechtfertigt werden.[1777]

Entsprechend der Argumentation bezüglich des Eingriffs in Art. 12 GG bestehen in Bezug auf die Vereinbarkeit einer Vorratsdatenspeicherung mit dem gemeinschaftsrechtlichen Grundsatz der Freiheit der wirtschaftlichen Betätigung Zweifel.[1778] Diese

---

[1770] *Richter*, EMRK/GG, Kap. 9, Rn. 41.
[1771] So *Derksen* 2011, 10.
[1772] Grundrechtsträger sind alle natürlichen und juristischen Personen sowie Personenvereinigungen *Bernsdorff*, in: *Meyer*, EU-GRCh., Art. 16 Rn. 16. Zwar sind die Grundrechte der Charta nicht grundsätzlich auch auf juristische Personen anwendbar. Die Anwendbarkeit von Art. 16 EU-GRCh. ist aber in der Rspr des *EuGH* anerkannt und zwar unabhängig davon ob sie in privatrechtlichen oder öffentlich-rechtlichen Formen agieren.
[1773] *Derksen* 2011, 10.
[1774] *Derksen* 2011, 10.
[1775] *EuGH* Urt. v. 29.1.1998, Rs. T-113/96 (Dubois et fils./. Rat u. Kommission), Slg 1998, II-125, Rn. 75; Urt. v. 30.7.1996, Rs. C84/95 („Boshporus"), Slg. 1996, I-3953, Rn. 22 ff.
[1776] *Derksen* 2011, WD-3000-18/11, 12.
[1777] *Derksen* 2011, WD-3000-18/11, 13.
[1778] *Derksen* 2011, WD-3000-18/11, 21. So wird in einem Bericht des Wissenschaftlichen Dienstes des Bundestags ausgeführt: „Vorbehaltlich der noch ausstehenden Bewertung der Kommission, die vermutlich tragfähige Daten über die Erfolgsaussichten der Vorratsspeicherung enthalten wird, könnte die Regelung in ihrer momentanen Ausgestaltung unangemessen in das Gemeinschaftsgrundrecht der berufs- und wirtschaftlichen Betätigungsfreiheit zu Lasten der TK-Anbieter eingreifen. Gemessen an dem derzeitigen Diskussionsstand zur Richtlinie 2006/24/EG und zur Auslegung der EU-GRCh. sowie der bestehenden Umsetzungsspielräume der Mitgliedstaaten lässt

lassen sich nur bei einer Ausgestaltung einer Verpflichtung zur Vorratsdatenspeicherung ausräumen, bei der eine Kostenerstattung vorgesehen ist.

9.2.2.2 Allgemeine Handlungsfreiheit

Von der Verpflichtung zur Speicherung und Übermittlung von Verkehrsdaten auf Vorrat ist auch die allgemeine Handlungsfreiheit der Telekommunikationsanbieter betroffen, die dem Wesen nach auf die Telekommunikationsanbieter anwendbar ist (Art. 2 Abs. 1 i.V.m. Art. 19 Abs. 3 GG). Da die Berufsfreiheit in besonderem Maß der Entfaltung der Persönlichkeit dient, ist die Garantie der allgemeinen Handlungsfreiheit subsidiär gegenüber Art. 12 Abs. 1 GG soweit dieser von seinem persönlichen und sachlichen Schutzbereich her einschlägig ist.[1779] Dies gilt auch für den mit der Verpflichtung zur Vorratsspeicherung erfolgten Eingriff in die Berufsfreiheit der Telekommunikationsdiensteanbieter. Art. 2 Abs. 1 GG tritt also zurück.

9.2.2.3 Eigentumsgarantie

Da die Dienstanbieter verpflichtet werden die Infrastruktur für die Speicherung der Verkehrsdaten zu schaffen, berührt die Vorratsdatenspeicherung auch die Eigentumsgarantie. Das Grundgesetz schützt mit Art. 14 das Eigentum.

Eigentum in diesem Sinne ist kein statischer Begriff und auch nicht deckungsgleich mit dem zivilrechtlichen Eigentumsbegriff, orientiert sich an jenen durch das einfache Recht gezogenen Konturen des Eigentumsbegriffs.[1780] Nach ständiger Rechtsprechung des *Bundesverfassungsgerichts* umfasst die Eigentumsgarantie all das, was in einfachen Gesetzen als vermögenswerte private Rechtspositionen anerkannt ist.[1781] Die Eigentumsfreiheit umfasst aber nicht die mit einer gewerblichen Tätigkeit verbundenen Erwerbs- und Verdienstchancen, sondern nur die vermögenswerten Güter, die in ihrem Bestand bereits vorhandenen sind.[1782]

---

sich zweifelsfrei keine Ausgestaltung dieser Richtlinie umschreiben, die eine Vereinbarkeit mit der EU-GRCh. sicherstellte."

[1779] *Manssen* in *Mangoldt/Klein/Starck,* GG 2010, Art. 12 Rn. 274.

[1780] *Schirra* 2002, 95.

[1781] BVerfGE 83, 201 (209); 89, 1 (6); 95, 34 (348).

[1782] *Papier* in Maunz/Dürig, GG 2011, Art. 14, Rn. 95, 222; Auch wird faustformelartig danach abgegrenzt, dass Art. 14 Abs. 1 GG das Erworbene, Art. 12 Abs. 1 GG den Erwerb schützt, *Manssen* in *Mangoldt/Klein/Starck,* GG 2010, Art. 12 Rn. 289; Das *BVerfG* führt in diese Richtung schon im Jahr 1952 aus, dass „die Sach- und Rechtsgesamtheit, als die sich der Gewerbebetrieb darstellt, dem reinen Sacheigentum gelichzustellen sei", BVerfGE 1, 264 (277). Demnach genieße ein Unternehmen den gleichen verfassungsrechtlichen Schutz wie das Eigentum. Seit der 1960er Jahren zeigt sich die Rspr des *BVerfG* bezüglich des verfassungsrechtlichen Unternehmensschutzes zurückhaltender. Der Schutz erstrecke sich nicht auf Chancen und Verdienstmöglichkeiten, BVerfGE 51, 193 (222). Diese Einschränkung des Schutzes der Unternehmensfreiheit durch Art. 14 Abs. 1 GG ist in der Literatur teilw. auf Kritik gestoßen. Das Gericht würde die Bedeutung des Gewerbebetriebs als wirtschaftliche Fundament des Unternehmereigentums verkennen, da das Sacheigentum wertlos wäre, wenn es nicht genutzt werden könne, *Schirra* 2002, 96 f., Fn. 361-363 m. zahlreichen w. Nachw. *Schirra* betont hier zutreffend, dass die Begrenzung der Eigentumsfreiheit auf das Erworbene dazu dient den Schutzumfang von Art. 14 zu begrenzen. Den Erwerb schützt Art. 12 GG – insofern besteht ein hinlänglicher Schutz durch die Berufsfreiheit.

Die Verpflichtung der Telekommunikationsdiensteanbieter zur Speicherung der Verkehrsdaten auf Vorrat greift in Art. 14 GG ein, soweit von ihr die Vorhaltung und der Betrieb der erworbenen oder die Um- und Aufrüstung der im Bestand des Betriebs bereits vorhanden Geräte betroffen sind.[1783] Insofern handelt es sich bei der Vorratsdatenspeicherungsverpflichtung um einen hoheitlichen Eingriff, der in die wirtschaftliche Betätigungsfreiheit der Telekommunikationsdiensteanbieter sowohl objektbezogen (Eigentumsgarantie) als auch tätigkeits- und erwerbsbezogen (Berufsfreiheit) eingreift. In dieser Konstellation sind die Grundrechte nebeneinander anwendbar.[1784] Da die Schrankenregelungen beider Grundrechte eine weitgehende Identität aufweisen, liegt in einer zulässigen Beschränkung der Berufsausübungsfreiheit im Allgemeinen auch eine den Eingriff in die Eigentumsgarantie rechtfertigende Inhalts- und Schrankenbestimmung im Sinne von Art. 14 Abs. 1 S. 2 GG.[1785] Gerade bei Indienstnahmen sind die Prüfungen im Rahmen der Berufsfreiheit und der Eigentumsgarantie deckungsgleich.[1786] Es wird allein die Verhältnismäßigkeit geprüft. Es kann daher auf die Ausführung zur Rechtfertigung des Eingriffs in Art. 12 Abs. 1 GG verwiesen werden.[1787]

Europarechtlich wird das Eigentumsrecht durch Art. 17 EU-GRCh. geschützt. Auch hier ist anerkannt, dass Einschränkungen bei der Verfügung über das Vermögen gerechtfertigt sind, wenn sie für das Wohl der Allgemeinheit erforderlich sind.[1788]

Die Europäische Menschenrechtskonvention gewährt einen Schutz des Eigentums gemäß Art. 1 ZP 1 auch „unabhängig von einer nachweisbaren, innerstaatlich anerkannten Rechtsposition“ und zwar insbesondere die faktische Existenz eines Unternehmens, das jemand durch eigene Leistung aufgebaut hat, für das er sich einen Kundenstamm erschlossen hat und das einen Vermögenswert darstellt.[1789] Daraus hat der *Europäische Gerichtshof für Menschenrechte* einen Schutz der beruflichen Betätigung entwickelt,[1790] wobei er bei der Auslegung dieser den Mitgliedstaaten einen Beurteilungsspielraum zugesteht.[1791]

9.2.2.4 Gleichheitsgebot

Eine Verpflichtung zur Vorratsdatenspeicherung kann auch, soweit kleine und große Anbieter von Telekommunikationsdienstleistungen unterschiedslos betroffen sind, zu

---

[1783] *Gausling* 2010, 151; Denn auch der eingerichtete und ausgeübte Gewerbebetrieb genießt einen verfassungsrechtlichen Eigentumsschutz, *Papier* in *Maunz/Dürig,* GG 2011, Art. 14, Rn. 95 f.

[1784] Sie stehen dann in Idealkonkurrenz zueinander, *Hofmann* in *Schmidt-Bleibtreu/Klein*, GG 2011, Art. 12 Rn. 98; *Scholz* in *Maunz/Dürig*, GG 2011, Art. 12 Rn. 143 ff, bzgl. der Indienstnahme insbes. Rn. 148.

[1785] BVerfGE 50, 290 (364).

[1786] *v. Hammer*stein, MMR 2004, 222, Rn. 223 f.

[1787] Vgl. oben S. 303 ff.

[1788] Art. 17 Abs. 1 S. 3 EU-GRCh.; ähnlich auch Art. 1 Abs. 2 ZP Nr. 1 zur EMRK.

[1789] *Cremer*, EMRK/GG , Kap. 22, Rn. 48.

[1790] Dazu schon oben S. 313; aus der Rspr des *EGMR* etwa Van Marle ./. Niederlande, v. 26.6.1986, Series A Nr. 101, § 39 f.; Hoerner Bank GmbH ./. Deutschland, v. 20.4.1999, Rep. 1999, 281.

[1791] *Peukert,* in: *Frowein/Peukert,* EMRK 2009, Art. 1 ZP 1 Rn. 44.

nicht rechtfertigungsfähigen Ungleichbehandlungen führen.[1792] Denn die Kosten entwickeln sich nicht proportional zur Unternehmensgröße.[1793]

Der Gleichheitssatz ist als allgemeines rechtsstaatliches Prinzip bei Eingriffen in die Berufsfreiheit und das Eigentum zu beachten.[1794] Freiheits- und Gleichheitsrechte sind grundsätzlich nebeneinander anwendbar, allerdings ist, soweit eine gleichheitswidrige Behandlung durch die öffentliche Hand zur Beeinträchtigung der Berufsfreiheit führt, primär diese als Prüfungsmaßstab heranzuziehen, was aber nicht bedeutet, dass Art. 3 Abs. 1 GG als Prüfungsmaßstab verdrängt wird.[1795]

Der allgemeine Gleichheitssatz verlangt keine absolute „Gleichheit" der Belastung, sondern wird im Rahmen von finanziellen Belastungen durch das *Bundesverfassungsgericht* bei den Freiheitsrechten geprüft. Das Gericht nimmt nur dann eine Verletzung des Gleichheitsgebots an, wenn für einzelne Betroffene die Grenze der Zumutbarkeit überschritten wird. Lange Zeit wurde der Gleichbehandlungsgrundsatz als ein reines Verbot gesetzlicher Willkür verstanden. Erst seit 1980 prüft das *Bundesverfassungsgericht*, ob „eine Gruppe von Normadressaten im Vergleich zu anderen Normadressaten anders behandelt wird, obwohl zwischen beiden Gruppen keine Unterschiede von solcher Art und solchem Gewicht bestehen, dass sie die ungleich Behandlung rechtfertigen können".[1796]

Damit führt das *Bundesverfassungsgericht* in der Pflichtteilsentscheidung aus, dass dem Verleger nicht die „erheblich überdurchschnittlichen Herstellungskosten für ein Pflichtexemplar" aufgebürdet werden könnten.[1797] Dies widerspreche zunächst „dem verfassungsrechtlichen Gebot die Belange des betroffenen Eigentümers mit denen der Allgemeinheit in einen gerechten Ausgleich zu bringen und einseitige Belastungen zu vermeiden".[1798] Sodann verletze es den im Rahmen des Art. 14 Abs. 2 GG zu beachtenden Gleichheitssatz. Der Gleichheitssatz geböte in diesem Fall die Elemente der inhaltsbestimmenden Regelung so zu ordnen, dass der „unterschiedlichen Inanspruchnahme" der Betroffenen und „dem unterschiedlichen Gewicht ihrer Belange hinreichend differenziert Rechnung getragen" wird. „Einseitige Belastungen" müssten vermieden werden.[1799] Dies gilt auch für die Ausgestaltung einer Vorratsdatenspeicherung. Auch hier darf es nicht zu einseitigen Belastungen kommen. Zudem sind im Sinne der neuen Formel keine solchen Unterschiede erkennbar, die eine unterschiedlich hohe Kostenbelastung[1800] dieser Gruppen rechtfertigen können.

Der Gleichbehandlungsgrundsatz verlangt daher, dass die Vorratsdatenspeicherung so ausgestaltet wird, dass alle Telekommunikationsanbieter gleichermaßen, das heißt

[1792] Der folgende Abschnitt lehnt sich an einen Auszug aus dem bereits in *Knierim* 2011b erschienen Text an.
[1793] Vgl. oben S. 303.
[1794] BVerfGE 58, 137 (148).
[1795] *Manssen,* in: v. *Mangoldt/Klein*/*Starck*, 2010, Art. 12 Rn. 276.
[1796] BVerfGE 55, 72 (88); seitdem stRspr BVerfGE 87, 234 (255); 88, 5 (12); 95, 39 (45); siehe hierzu auch *Roßnagel*, DuD 2010, 544.
[1797] BVerfGE 58, 137 (150).
[1798] BVerfGE 58, 137 (150).
[1799] BVerfGE 58, 137 (150 f.).
[1800] Dies gilt nur solange und soweit keine Kostenerstattung vorgesehen ist.

proportional entsprechend ihrer Größe, belastet werden. Die Verpflichtung zur Vorratsdatenspeicherung würde Art. 3 Abs. 1 GG verletzen, wenn alle Telekommunikationsanbieter gleichermaßen verpflichtet werden, da dann kleine und mittlere Anbieter proportional stärker belastet werden.[1801] Es bedarf somit, um eine Verletzung von Art. 3 Abs. 1 GG zu vermeiden, entweder einer Ausnahme von kleinen Anbietern von der Speicherungsverpflichtung oder einer umfassenden Kostenerstattung.

Auch aus europarechtlicher Perspektive ist eine Kostenerstattungsregelung zu fordern, und zwar in Gestalt einer einheitlichen Regelung der Frage der Kostenerstattung im Rahmen der Richtlinie. In Anbetracht der Zielsetzung der Richtlinie den Binnenmarkt zu harmonisieren ist es widersinnig, die Frage der Kostenerstattung nicht zu regeln.[1802] Um Wettbewerbsverzerrungen zu vermeiden, die drohen solange in manchen Staaten eine Kostenerstattung erfolgt und in anderen nicht, ist es erforderlich europarechtlich die Kostenerstattung zu regeln. Auch sollte bezüglich der einzuhaltenden Sicherheitsstandards europaweit eine einheitliche Regelung geschaffen werden, da die Sicherheitsanforderungen wesentlich die Höhe der entstehenden Kosten beeinflussen und zum anderen so ein europaweit einheitlicher (Grundrechts-)Standard erreicht werden kann.[1803]

9.2.2.5 Rechtssicherheit und Bestimmtheitsgebot

Auch in der Dimension Staat-Wirtschaft gilt es im Interesse der von der Regelung betroffenen Telekommunikationsanbieter, Rechtssicherheit zu gewähren.[1804] Die Telekommunikationsunternehmen verpflichtenden Normen müssen so klar und bestimmt sein, dass mit Hilfe juristischer Auslegung zweifelsfrei feststellbar ist, wer zur Speicherung verpflichtet sein soll.

9.2.2.6 Optimierter Interessenausgleich aus Perspektive der TK-Industrie

Bei der Ausgestaltung der Indienstnahme der Telekommunikationsanbieter ist zu beachten, dass diese nur mit dem Gewaltmonopol des Staates in Einklang steht, wenn keine weitergehenden Ermittlungsmaßnahmen auf die Privaten übertragen werden und der Staat die Organisationshoheit behält. Es ist von zentraler Bedeutung, dass auch bei der Speicherung bei den Unternehmen sichergestellt ist, dass alle rechtsstaatlichen Garantien eingehalten werden.

Gegen die Zumutbarkeit der Übertragung der Kosten auf die Telekommunikationsanbieter sprechen zwar zahlreiche, gute Gründe. Schließlich wird sie gerechtfertigt auf Grund der wirtschaftlichen Betätigung der Anbieter − allerdings nur soweit sie nicht erdrosselnd wirkt. Dies droht indes für kleine Anbieter. Erforderlich ist daher eine Ausnahmeregelung für Kleinanbieter. Dies gebietet auch Art. 3 GG. Im Sinne eines

---

[1801] *Gausling* 2010, 155

[1802] Im Vereinigten Königreich ist bspw. eine Kostenerstattung vorgesehen. Auch der Kommissionsbericht stellt fest, dass das Ziel einer Harmonisierung aufgrund der unterschiedlichen Regelungen zur Kostenerstattung nicht erreicht wurde, EU Kom (2011), 225, 33; vgl. dazu auch schon oben S.

[1803] *Roßnagel*, DuD 2010, 544.

[1804] Zur verfassungsrechtlichen Begründung von Rechtssicherheit und den einzelnen Anforderungen, siehe auch oben S. 294.

optimierten Interessenausgleichs ist eine umfassende Kostenerstattung geboten, wobei die Anbieter anteilig an den Kosten beteiligt werden sollten.

9.2.3 Elemente eines Interessenausgleichs

Wesentlich für den Interessenausgleich in der Dimension Staat – Wirtschaft ist die Ausgestaltung zweier Elemente: Erstens, wer wird verpflichtet, also die Adressaten der Speicherungsverpflichtung, und zweitens, ob die Kosten übertragen werden.

9.3 *Staat – Staat*

Auch staatliche Interessen kollidieren bei der Vorratsspeicherung von Telekommunikationsverkehrsdaten. So ist es nicht nur im staatlichen Interesse Sicherheit zu gewährleisten, sondern ist es auch originär staatliches Interesse eine freiheitliche Grundordnung zu sichern. Inwiefern diese Interessen im Rahmen der Vorratsdatenspeicherung kollidieren, wird im Folgenden untersucht. Damit wird die dimensionsorientierte Untersuchung des Spannungs-verhältnisses zwischen Sicherheits- und Freiheitsinteressen vervollständigt.

9.3.1 Staatliche Sicherheitsinteressen

Im Interesse des Staates ist es, Sicherheit zu gewährleisten.[1805] Dafür ist nicht nur eine einzige Behörde zuständig. Vielmehr unterscheidet die Verfassung der Bundesrepublik Deutschland zwischen Gefahrenabwehrbehörden, Strafverfolgungsbehörden und Nachrichtendiensten.[1806] Um ein möglichst hohes Maß an Sicherheit durch eine Vorratsspeicherung zu ermöglichen, ist es staatliches Interesse die Daten zwischen den Behörden austauschen zu können. Die informationelle Kooperation ist insoweit in der Dimension Staat – Staat ein weiteres, Sicherheitsinteresse. Auch europa- und völkerrechtlich besteht ein Interesse an Zusammenarbeit. Dies ganz besonders für den Bereich der Bekämpfung des internationalen Terrorismus und der organisierten Kriminalität.

9.3.1.1 Innerstaatliche Kooperation

Wesentlich dafür, dass die Vorratsdatenspeicherung einen möglichst großen Beitrag zur Sicherheit leistet, ist, dass die Daten den unterschiedlichen Sicherheitsbehörden zur Verfügung stehen. Für die Erfüllung der Staatsaufgabe Sicherheit sind in der Bundesrepublik verschiedene Behörden zuständig.[1807] Dabei sind den Behörden jeweils spezifische Aufgaben zugewiesen. Damit die Vorratsdatenspeicherung einen möglichst hohen Beitrag zur Sicherheit leistet ist es erforderlich, dass die mit der Vorratsdatenspeicherung gewonnen Erkenntnisse auch zwischen den Behörden ausgetauscht werden können. Dieses Erfordernis besteht sowohl zwischen den verschiedenen Behörden (Polizei, Nachrichtendienste, Verfassungsschutz) als auch in Hinsicht auf eine gelungene Zusammenarbeit über die Grenzen der Bundesländer hinweg. Entscheidend kommt es insoweit darauf an, wann und unter welchen Voraussetzungen die Daten an

[1805] Zur verfassungsrechtlichen Grundlage und dem Umfang des staatlichen Sicherheitsinteresses generell, oben Kap. 2.2; speziell in Bezug auf die Vorratsdatenspeicherung Kap. 9.1.1.
[1806] Vgl. dazu oben Kap. 2.2.5.
[1807] Zu den verschiedenen Behörden, die mit Sicherheitsaufgaben betraut sind, oben Kap. 2.2.5, S. 116 ff.

eine andere öffentliche Stelle übermittelt werden können. Dies gilt es genauer zu betrachten, da die Bundesrepublik keine (informationelle) Funktionseinheit bildet.[1808]

Die Ermittlungen bezüglich der rechtsterroristischen Vereinigung NSU haben gezeigt, welch Schaden die innere Sicherheit nehmen kann, wenn die Kooperation und die Kommunikation wesentlicher Erkenntnisse zwischen den unterschiedlichen Behörden und über Landesgrenzen hinweg versagt.[1809]

Im Grundgesetz ist in Art. 35 Abs. 1 GG die allgemeine Pflicht zur Amts- und Rechtshilfe[1810] normiert. Auch die „Informationshilfe" ist Amtshilfe.[1811] Art. 35 Abs. 1 GG ist eine Spezialregelung, die die grundsätzlich ausschließliche Kompetenzverteilung zwischen Bund- und Landesbehörden modifiziert.[1812] Art. 35 GG durchbricht damit die Gewaltenteilung, wie sie in Art. 20 Abs. 2 GG vorgesehen ist – in ihr zeigt sich die „Einheit der Staatsgewalt" und der kooperierende Föderalismus.[1813]

Die Wurzel für diese Durchbrechung der Gewaltenteilung liegt darin, dass in Folge dieser verschiedene Aufgaben auf unterschiedliche Behörden verteilt sind und zudem noch eine föderale Aufgabentrennung besteht. Es ist daher notwendig, um die Verfolgung der Staatszwecke sicherzustellen, dass die Gewaltenteilung dann durchbrochen werden kann, wenn dies zur Verfolgung der Staatszwecke erforderlich ist.[1814]

Art. 35 Abs. 1 GG kann als Rahmenvorschrift betrachtet werden, während sich die Verfahren und der materielle Umfang von Rechts- und Amtshilfe sich (primär) aus einfach gesetzlich geregelten Verfahrensvorschriften ergeben.[1815]

Dabei sind Rechts- und Amtshilfe jeweils ausschließlich in dem jeweils geltenden Rechts- und Kompetenzrahmen zulässig ist. So darf eine Behörde sich nicht im Wege der Amts- oder Rechtshilfe über die Inanspruchnahme einer anderen Behörde Befugnisse verschaffen, die ihr selbst nicht zu kommen.[1816] Dies gebietet auch das Rechtsstaatsprinzip.

Grundsätzlich ist bei der Rechts- und Amtshilfe nach Art. 35 Abs. 1 GG zu beachten, dass weder Weisungsabhängigkeit, Delegation, Mandat noch Organleihe vorliegen darf. Sie ist nur für ein außerordentliches, punktuelles und eben nicht für ein regelmäßiges Zusammenwirken zulässig. Dabei muss sie zur rechtmäßigen Aufgabenerfüllung

---

[1808] *Pieroth/Schlink/Kniesel* 2012, § 2, Rn. 2; vgl. dazu auch schon oben S. 120, Fn. 758.

[1809] *Dpa,* Augsburger Allgemeine v. 26.4.2012, abrufbar unter: http://www.augsburger-allgemeine.de/politik/Mangelnde-Behoerden-Zusammenarbeit-bei-der-Aufklaerung-der-Neonazi-Morde-id19786926.html

[1810] Umfassend zum Wesen der Amtshilfe *Gärditz* 2003, 420 ff.

[1811] *Scholz*/*Pitschas* 1984, 116 ff.

[1812] *Pieroth*, in: *Pieroth/Schlink*, GG Komm 2011, Art. 35 Rn. 1; Strg. ist, ob sie nur im Verhältnis von Bundes- und Landesbehörden und von Behörden verschiedener Länder oder ob sie auch zwischen Bundesbehörden und zwischen Behörden desselben Landes gilt.

[1813] *Sannwald,* in: *Schmidt-Bleibtreu/Klein*, GG 2012, Art. 35 Rn. 1.

[1814] *Sannwald,* in: *Schmidt-Bleibtreu/Klein*, GG 2012, Art. 35 Rn. 2.

[1815] *Epping* in Beck O-K, 2012, Art. 35 Rn. 7; *Sannwald,* in: *Schmidt-Bleibtreu/Klein*, GG 2012, Art. 35 Rn. 4.

[1816] *Epping* in Beck-OK, 2012, Art. 35 Rn. 8.

„erforderlich“ sein und darf nicht anderweitig in einer sondergesetzlichen Aufgabenzuweisung normiert sein.[1817]

Die Pflicht zur Amtshilfe der Verwaltungsbehörden beruht auf § 4 VwVfG beziehungsweise dem jeweiligen landesrechtlichen Pendant. Dabei wird die Pflicht zur Amtshilfe durch das Datenschutzrecht beschränkt.[1818]

Einschlägig sind bei der Datenverarbeitung durch öffentliche Stellen im Wesentlichen die Landesdatenschutzgesetze. In § 2 Abs. 1 BDSG ist zwar auch die Verarbeitung durch öffentliche Stellen geregelt. Das Bundesdatenschutzgesetz ist jedoch nach § 1 Abs. 2 Nr. 1 BDSG nur hinsichtlich des Umgangs mit personenbezogenen Daten durch öffentliche Stellen des Bundes anzuwenden, während solange öffentlichen Stellen der Länder personenbezogene Daten verarbeiten, nur dann der Regelungsbereich des Bundesdatenschutzgesetzes eröffnet ist, wenn gem. § 1 Abs. 2 Nr. 2 BDSG der Datenschutz nicht durch die Länder geregelt ist.

Dennoch sollen hier zunächst kurz die Regeln des Bundesdatenschutzgesetzes dargelegt, da den dort benannten einzelnen Anforderungen überwiegend jene der Landesdatenschutzgesetze entsprechen. § 3 Abs. 4 Nr. 3 BDSG definiert das Übermitten als „das Bekanntgeben gespeicherter oder durch Datenverarbeitung gewonnener personenbezogener Daten an einen Dritten“ in der Weise, dass die Daten an den Dritten weiter gegeben werden oder dieser die bereitgehaltene Daten einsieht oder abruft. Dritter ist jede Person oder Stelle, die nicht die ursprünglich speichernde oder verarbeitende, also die im Sinne von § 3 Abs. 3 BDSG verantwortliche, Stelle ist. Dadurch wird der Datenfluss zwischen Behörden sowohl in organisatorischer als auch in funktionaler Hinsicht begrenzt.[1819]

Keine Bedeutung hat die Art der Datenübermittlung, also ob diese mündlich, schriftlich oder elektronisch erfolgt.[1820] Es kommt allein darauf an, dass Informationen an einen Dritten weitergegeben werden. [1821] Dritter ist nach der Legaldefinition in § 3 Abs. 8 S. 2 BDSG „jede Person oder Stelle außerhalb der verantwortlichen Stelle“.

Gemäß § 15 Abs. 1 BDSG ist eine Datenübermittlung zulässig, wenn sie „zur Erfüllung der in der Zuständigkeit der übermittelnden Stelle oder des Dritten an den die Daten übermittelt werden, liegenden Aufgaben erforderlich ist“ und zweitens „die Voraussetzungen vorliegen, die eine Nutzung nach § 14 BDSG zulassen würden“. Erforderlich ist die Übermittlung dann, wenn die ersuchende Behörde die Aufgabe nicht auf anderem Weg ohne gegen die Rechtsordnung zu verstoßen, erfüllen kann. Sie muss insofern für die Aufgabenerfüllung unverzichtbar sein.[1822] Wichtig ist auch, dass sich der Umfang des Abrufs gemäß § 3a BDSG auf das geringstmögliche Maß an Daten be-

[1817] *Pieroth,* in: *Pieroth/Schlink,* GG Komm 2011, Art. 35 Rn. 4.
[1818] *Petri,* in: *Lisken/Denninger,* 2012, G, Rn. 437.
[1819] *Petri,* in: *Lisken/Denninger,* 2012, G, Rn. 435.
[1820] *Wank* in ErfKomm ArbR, 2012, § 28 BDSG, Rn. 14; *Petri,* in: *Lisken/Denninger,* 2012, G, Rn. 434.
[1821] *Petri,* in: *Lisken/Denninger,* 2012, G, Rn. 434.
[1822] *Ambs,* in: *Erbs/Kohlhaas,* StR Komm, 2012, § 12 BDSG, Rn. 7.

schränken muss. Darüber hinaus sind auch alle anderen für die Datenerhebung und -speicherung geltenden Zulässigkeitsvoraussetzungen zu beachten: so müssen Zweckbindungsgrundsatz und Transparenzgebot berücksichtigt werden. Schließlich ist in organisatorischer Hinsicht bestimmt, dass im Fall eines Übermittlungsverlangens, die ersuchende öffentliche Stelle der ersuchten den Verwendungszweck mitzuteilen hat.[1823] Ob dieser Verwendungszweck zur Übermittlung ermächtigt, ist sodann durch die ersuchte Stelle zu prüfen.

Denn nach den allgemeinen Übermittlungsregeln ist die Stelle für die Rechtmäßigkeit der Datenübermittlung verantwortlich, die die Weitergabe der Informationen veranlasst hat.[1824] In inhaltlicher Hinsicht ist davon die Prüfung des konkreten Übermittlungszwecks erfasst, sowie in organisatorischer Hinsicht die Prüfung der Zuständigkeit: ist die ersuchende Stelle tatsächlich für die angegebene Aufgabe zuständig und auch im konkreten Fall zur Verwendung der Daten ermächtigt?[1825]

Neben der Ermächtigung zur Informationshilfe im Wege der Amtshilfe, können Daten für Zwecke der Gefahrenabwehr und der Strafverfolgung übermittelt werden. Die Übermittlung zu polizeiliche Zwecken richtet sich nach den Polizeigesetzen von Bund- und Ländern. Eine Datenübermittlung an die Staatsanwaltschaft erfolgt nach §§ 161, 163 StPO. Zu präventiven Zwecken (Gefahrenabwehr, Gefahrenvorsorge) ermächtigen die §§ 481, 483 StPO zur Datenübertragung.

Für die Datenübermittlung von der Polizei finden sich sodann Regelungen in den Polizeigesetzen. In Hessen wird die polizeiliche Übermittlung personenbezogener Daten in den §§ 21 ff. HSOG geregelt.[1826] Als allgemeine Regel bestimmt § 21 Abs. 1 HSOG, dass die Datenübermittlung nur zu dem Zweck zulässig ist, zu dem die Daten erlangt wurden. Der Verwendungszweck ist festzuhalten. In § 21 Abs. 5 HSOG ist die Pflicht die Zulässigkeit der Übermittlung zu prüfen normiert. Sodann wird auch klargestellt, dass Daten nur zu dem Zweck verarbeitet werden dürfen, zu dem sie übermittelt worden sind. Die Übermittlung zwischen öffentlichen Stellen wird in § 22 HSOG geregelt. Nach Abs. 1 ist eine Übermittlung zwischen Polizeibehörden (auch verschiedener Länder und des Bundes, S. 2) zulässig, soweit die Daten für die Aufgabenerfüllung der ersuchenden Behörde benötigt werden und die Datenübermittlung „erforderlich" ist. Zwischen den oder an die für die Gefahrenabwehr zuständigen Behörden „können personenbezogene Daten übermittelt werden, soweit die Kenntnis dieser Daten zur Erfüllung der Aufgaben der empfangenden Stelle erforderlich erscheint". Einige wenige spezielle Abruftatbestände werden in § 22 Abs. 2 HSOG benannt.

Gemäß § 24 HSOG können Daten mit automatisiertem Abrufverfahren übermittelt werden.

[1823] *Ambs,* in: *Erbs/Kohlhaas,* StR Komm, 2012, § 12 BDSG, Rn. 7.
[1824] vgl. § 487 Abs. 3 StPO, § 10 Abs. 8 BKAG, § 33 Abs. 1 BPolG; § 21 Abs. 5 HSOG; dazu *Petri,* in: *Lisken/Denninger,* 2012, G, Rn. 459.
[1825] *Petri,* in: *Lisken/Denninger,* 2012, G, Rn. 460.
[1826] Hier werden nur exemplarisch die einschlägigen Normen des HSOG benannt.

Für die Übermittlung von auf Vorrat gespeicherten Verkehrsdaten, gilt zunächst generell das was auch für alle durch die öffentliche Verwaltung verarbeiteten Daten gilt: Eine Datenübermittlung zwischen staatlichen Stellen ist nur soweit möglich, wenn die datenschutzrechtlichen Anforderungen beachtet werden, insbesondere die Zweckbindung der Daten gewährleistet ist, sowie die Voraussetzungen für den Abruf der Daten beim Anbieter auch bei der ersuchenden Stelle vorliegen.[1827]

Für die Gewährleistung der Zweckbindung von Vorratsdaten ist es erforderlich, dass auch die im Wege der Analyse der Verkehrsdaten gewonnen Informationen nur unter den für die Datenübermittlung und die Amts- und Rechtshilfe geltenden Voraussetzungen übermittelt werden dürfen. Ansonsten würde der Zweckbindungsgrundsatz allein durch einen zwischengeschalteten Verarbeitungsschritt unterlaufen.

9.3.1.2 Europäische und internationale Zusammenarbeit

Die Vorratsdatenspeicherung ist als europäische Richtlinie verabschiedet worden. Auch wenn die Richtlinie technisch ein Instrument zur Harmonisierung des Binnenmarktes ist, entstand sie unter dem Eindruck der Anschläge von London und Madrid und insofern als Instrument zur Bekämpfung des internationalen Terrorismus. Ihr Ziel ist insofern auch sicherzustellen, dass für diesen Zweck Daten zur Verfügung stehen. So wird in den Erwägungsgründen unter anderem darauf verwiesen, dass der Rat in einer Erklärung vom 13. Juli 2005 die Terroranschläge von London verurteilt hat und „nochmals auf die Notwendigkeit hingewiesen" hat, „so rasch wie möglich gemeinsame Maßnahmen zur Vorratsspeicherung von Telekommunikationsdaten zu erlassen".[1828] Auch wird als Ziel der Richtlinie in Erwägungsgrund 21 neben der Harmonisierung „die Gewährleistung, dass diese Daten zum Zwecke der Ermittlung, Feststellung und Verfolgung von schweren Straftaten, wie sie von jedem Mitgliedstaat in seinem nationalen Recht bestimmt werden, zur Verfügung stehen" genannt. Dies zeigt, dass das Ziel Sicherheit zu gewährleisten, bei der Verabschiedung der Richtlinie von hoher Bedeutung war.

Für die Bekämpfung schwerer Straftaten, insbesondere des internationalen Terrorismus, aber eine funktionsfähige und effektive Zusammenarbeit zwischen verschiedenen Staaten erforderlich. Zu den Anforderungen an die Übermittlung der auf Vorrat gespeicherten Verkehrsdaten in andere Mitgliedstaaten finden sich keine Vorgaben in der Richtlinie.[1829] Nichtsdestotrotz besteht ein sicherheitsrechtliches Interesse, die Daten grenzüberschreitend zu übermitteln.

Dieses Interesse wird verfassungsrechtlich gestärkt durch die Völkerrechts- und Europarechtsfreundlichkeit der Verfassung.[1830] Das *Bundesverfassungsgericht* betont, dass das Grundgesetz die deutsche öffentliche Gewalt „programmatisch auf die internationale

[1827] BVerfGE 125, 260 (333).
[1828] Erwägungsgrund 10 der RL 2006/24/EG.
[1829] Solche Regelungen hätten auch in der damaligen dritten Säule, also im Rahmen der polizeilichen und justiziellen Zusammenarbeit verabschiedet werden müssen. Zur Entstehungsgeschichte der Richtlinie und warum sie gerade nicht als Rahmenbeschluss i.R.d. Polizeilichen und Justiziellen Zusammenarbeit verabschiedet wurde, vgl. oben Kap. 4.2.1.
[1830] BVerfGE 111, 307 (317). Auch wird der Bundesrepublik eine „offene Staatlichkeit" bescheinigt. *Wahl,* JuS 2003, 1145.

Zusammenarbeit (Art. 24 GG) und auf die europäische Integration (Art. 23 GG) festgelegt" habe. Dies zeigt sich im Vorrang des Völkerrechts vor einfachem Gesetzesrecht gemäß Art. 25 Abs. 2 GG; der Einordnung des Völkervertragsrechts in das System der Gewaltenteilung durch Art. 59 Abs. 2 GG, in der mit Art. 24 Abs. 2 GG eröffneten Möglichkeit der Einbindung in Systeme gegenseitiger kollektiver Sicherheit, in dem in Art. 24 Abs. 3 GG erteilten Auftrag zur friedlichen Beilegung zwischenstaatlicher Streitigkeiten im Wege der Schiedsgerichtsbarkeit und schließlich in der Verfassungswidrigkeit einer Friedensstörung nach Art. 26 Abs. 1 GG.[1831] „Mit diesem Normenkomplex zielt die deutsche Verfassung, auch ausweislich ihrer Präambel, darauf ab, die Bundesrepublik Deutschland als friedliches und gleichberechtigtes Glied in eine dem Frieden dienende Völkerrechtsordnung der Staatengemeinschaft einzufügen", so das *Bundesverfassungsgericht*.[1832] Ebenso ist das Ziel an der Verwirklichung der Europäischen Einheit und der Entwicklung der Europäischen Union mitzuwirken, ausdrücklich in Art. 23 Abs. 1 GG normiert.[1833]

Allerdings ist die Öffnung für völkerrechtliche und europarechtliche Bindungen nicht endlos. Dies zeigt sich schon darin, dass Völkervertragsrecht nicht unmittelbar, also ohne Zustimmungsgesetz, anwendbar ist. Auch Völkergewohnheitsrecht, das zwar gemäß Art. 25 GG Bestandteil des Bundesrechts ist, hat keinen Verfassungsrang. Darin kommt „die klassische Vorstellung" zum Ausdruck „dass es sich bei dem Verhältnis des Völkerrechts zum nationalen Recht um ein Verhältnis zweier unterschiedlicher Rechtskreise handelt und dass die Natur dieses Verhältnisses aus der Sicht des nationalen Rechts nur durch das nationale Recht selbst bestimmt werden kann (…). Die Völkerrechtsfreundlichkeit entfaltet Wirkung nur im Rahmen des demokratischen und rechtsstaatlichen Systems des Grundgesetzes".[1834] Europarecht ist zwar als supranationales Recht zum Teil unmittelbar wirksam.[1835] Allerdings ist auch der Überlagerung nationalen Rechts durch europäisches Recht durch den Identitätsvorbehalt eine Schranke gesetzt.[1836]

Es zeigt sich, dass die Bundesrepublik sowohl an europarechtliche und völkerrechtliche Verträge gebunden ist und zur Mitwirkung an einer guten Zusammenarbeit verpflichtet ist. Auf der anderen Seite ist sie auch verpflichtet die Grundrechte, Rechtsstaats- und Demokratieprinzip, insbesondere die „Identität der Verfassung", zu wahren.

Die Übermittlung von auf Vorrat gespeicherten Verkehrsdaten innerhalb Europas richtet sich nach vertraglichen Vereinbarungen. Es wurden für einen erleichterten Informationsaustausch mehrere Abkommen zur Übermittlung von personenbezogenen Daten innerhalb der *Europäischen Union* geschlossen.[1837]

[1831] Vgl. *Scholz,* in: *Maunz/Dürig,* GG 2011, Art. 23 Rn. 54.
[1832] BVerfGE 63, 343(370); 111, 307 (318).
[1833] Dazu *Scholz,* in: *Maunz/Dürig,* GG 2011, Art. 23 Rn. 54.
[1834] BVerfGE 111, 307 (318).
[1835] Vgl. zum Verhältnis nationales Recht – Europarecht, oben S. 47 ff., 224 ff.
[1836] Dazu schon ausführlich oben, S. 158 f.
[1837] In Bezug auf die zwischenstaatliche Zusammenarbeit sind zu nennen: EuRhÜbk v. 20.4.1959; ZP – EuRhÜbk v. 17.3.1978; SDÜ v. 14.6.1990; EU-RhÜbk v. 29.5.2000; ZP-EU-RhÜbk v.

Ein weitgehender Vorstoß wurde mit einem von der Kommission im Jahr 2005 eingebrachten Vorschlag für einen Rahmenbeschluss verfolgt. Damit sollte der Grundsatz der Verfügbarkeit (principle of availability) eingeführt werden.[1838] Ziel war, dass der Austausch von strafverfolgungsrelevanten Informationen in der gesamten Union nach einheitlichen Bedingungen erfolgt. Dieser Vorstoß ist jedoch auf heftige Kritik gestoßen[1839] und wurde schließlich vom Rat nicht unterstützt.

Zum Teil schlägt sich jedoch der Ansatz des Prinzips der Verfügbarkeit in dem ebenfalls im Jahr 2005 geschlossenen Prümer Vertrag nieder.[1840] Dieser wurde in weiten Teilen mit dem RB 2008/615/JI[1841] in Unionsrecht überführt.[1842] Der Rahmenbeschluss sieht vor, dass Polizei- und Staatsanwaltschaften direkten Zugriff auf die Datenbanken der anderen Vertragsstaaten haben.[1843] Sie beziehen sich jedoch nur auf bestimmte explizit genannte, behördliche Datenbanken[1844] und erfassen nicht die auf Vorrat gespeicherten Telekommunikationsverkehrsdaten. Eine Übertragung dieses Konzepts auf diese auf Vorrat gespeicherten Daten scheidet zudem schon deshalb aus, da bei der Vorratsdatenspeicherung kein unmittelbarer Zugriff der Staaten auf die Datenbanken vorgesehen ist. Ein solcher wäre auch mit dem deutschen Verfassungsrecht nicht vereinbar.[1845]

Neben dem Prümer Vertrag wurde mit der sogenannten „Schwedischen Initiative" eine Vereinfachung des Informationsaustausches zwischen Strafverfolgungsbehörden vereinbart.[1846] Diese verpflichtet die Mitgliedstaaten an die grenzüberschreitende Übermittlung personenbezogener Daten innerhalb der Union keine höheren Anforderungen zu stellen, als auf nationaler Ebene für den Datenaustausch zwischen Polizei- und Strafverfolgungsbehörden gelten (Prinzip des gleichberechtigten Zugangs).[1847] Die Mitgliedstaaten müssen gewährleisten, dass innerhalb bestimmter Fristen[1848] Informationen und Erkenntnisse an die zuständigen Strafverfolgungsbehörden anderer Mit-

---

14.10.2001; RB 2006/960/JI v. 18.12.2006 (schwedische Initiative); zu Abkommen der EU mit Drittstaaten, siehe auch *Brodowski* ZIS 2011, 940.

[1838] KOM (2005) 490 - Vorschlag v. 12.10.2005; dazu *Böse* 2007, 46 ff.; *Meyer*, NStZ 2008, 188, 190 f.

[1839] Unter anderem, da dieser ein unterschiedlich hohes datenschutzrechtliches Level zulässt, so *Böse* 2007, 86; *Weichert* 2006.

[1840] Vgl. Nachw. in Fn. 397.

[1841] RB 2008/615/JI v. 23.8.2008; Abl. EU L 210/1.

[1842] *Weichert* 2006.

[1843] Darin ist ein Paradigmenwechsel in der grenzüberschreitenden Zusammenarbeit zu erkennen, denn ein vorheriges Ersuchen ist nach Prüm nicht mehr erforderlich, dazu ausführlich *Zöller*, ZIS 2011, 64, 66 ff.

[1844] DNA-Analyse-Dateien; daktyloskopische Daten und Kennungen; Daten aus Fahrzeugregistern; sowie die Übermittlung von Namen und Geburtsdaten von Personen, die im Verdacht stehen eine terroristische Straftat zu begehen.

[1845] BVerfGE 125, 260 (321 f.)

[1846] RB 2006/960/JI v. 18.12.2006.

[1847] Es sind also die gleichen Anforderungen an die Übermittlung an andere Mitgliedstaaten zu stellen, wie bei innerstaatlichen Verfahren. Art. 3 RB 2006/960/JI.

[1848] Innerhalb von 8 Stunden, sofern die Daten der Behörde unmittelbar verfügbar sind; ansonsten max. 14 Tage, Art. 4 RB 2006/960/JI.

gliedstaaten übermittelt werden. Die Umsetzungsfrist des Rahmenbeschlusses ist am 19. Dezember 2006 abgelaufen. Eine Umsetzung in deutsches Recht für den Zugriff auf die Daten für polizeiliche Aufgaben der Gefahrenabwehr ist etwa in § 22 Abs. 1 S. 2 HSOG[1849] erfolgt.

Für den Informationsaustausch im Rahmen des Strafverfahrens gibt es bislang keine eigenständige nationale Regelung. Ein erster Gesetzentwurf der Bundesregierung wurde am 17. März 2011[1850] vorgelegt. Während das Bundeskriminalamt den Entwurf lobte, stieß er insbesondere im Hinblick auf den Datenschutz auf Kritik. Die vorgesehene Übermittlung von personenbezogenen Daten greife „massiv in das Recht auf informationelle Selbstbestimmung" eingreife. „Das gilt umso mehr, weil der Grundrechtsschutz im Falle der Datenübermittlung an Strafverfolgungsbehörden innerhalb der EU bei realistischer Betrachtungsweise nicht gewährleistet werden kann, nicht zuletzt weil die Einhaltung grundrechtsschützender Begrenzungen seitens des Empfängerstaates sich einer effektiven Kontrolle entzieht. Während personenbezogene Daten Grenzen in Sekundenschnelle überwinden, sind sie für nationale Kontrollbefugnisse nahezu unüberwindbar."[1851] Es bestünden erhebliche Zweifel ob der Entwurf verfassungsrechtlichen Ansprüchen genüge.[1852] Die Kritik floss in eine Überarbeitung des Entwurfs ein, der schließlich am 8. März 2012 mit den Stimmen der CDU/CSU und FDP-Fraktion angenommen wurde.[1853] Die Opposition hatte weiterhin Kritik im Hinblick auf den Datenschutz geübt.[1854]

Fraglich ist aber auch, ob das Umsetzungsgesetz mit dem Recht auf informationelle Selbstbestimmung vereinbar ist. Denn die Tatsache, dass der Rahmenbeschluss umgesetzt wurde ändert nichts an der Tatsache, dass bis heute kein adäquater Individualschutz bei der Informationsverarbeitung im Rahmen der polizeilichen und justiziellen Zusammenarbeit auf europäischer Ebene gegeben ist.[1855] Dies führt dazu, dass der hohe Schutzstandard, der an sich in Deutschland verfassungsrechtlich vorgegeben ist, auf Grund des Anwendungsvorrangs des Unionsrechts keine Wirkung entfaltet.[1856] Informationskooperation ist jedoch auf Grund der Bindung aller Gewalten an die im

[1849] Abk. für Hessisches Gesetz über die öffentliche Sicherheit und Ordnung; Gesetzesänderung vom 23.12.2009.
[1850] BT-Drs. 17/5096.
[1851] *Putzke* 2007, 8 f.
[1852] *Putzke* 2007, 11.
[1853] BT Drs. 17/8870; BT Plenarprotokoll 17/165, 19659; BR Drs. 117/12.
[1854] BT Plenarprotokoll 17/165, 19656 (D) ff.
[1855] Ausführlich dazu *Boehm* 2011; Dies würde sich jedoch durch die Verabschiedung der Richtlinie „zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Aufdeckung, Untersuchung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr" ändern, KOM (2012) 10, vgl. dazu oben S. 91 f.
[1856] *Zöller*, ZIS 2011, 64, 67; Die Europäische Datenschutzrichtlinie nimmt ausdrücklich die ehemals dritte Säule aus. Der RB v. 27.12.2008 über den Schutz personenbezogener Daten, die im Rahmen der polizeilichen und justiziellen Zusammenarbeit in Strafsachen verarbeitet werden (RB 2008/977/JI), bietet auch keine Abhilfe, da Rechtsakte wie der Prümer Ratsbeschluss ausdrücklich von ihr ausgenommen sind; Abhilfe verspricht hier jedoch der RL-E v. 25.1.2012 i. R. d. DS-GVO-E (KOM (2012) 10). Allerdings sollen laut Art. 3 Abs. 3 b) Datenverarbeitungen durch Organe und Einrichtungen der EU von der VO ausgenommen werden.

Grundgesetz garantierten Grundrechte nur möglich, solange und soweit ein adäquater Grundrechtsschutz gewährleistet wird. Insoweit bestehen Bedenken gegen die Vereinbarkeit des Gesetzes mit der informationellen Selbstbestimmung.[1857]

Wenn in Bezug auf die auf Vorrat gespeicherten Verkehrsdaten sichergestellt ist, dass der Zugriff und insofern dann auch die Übermittlung der Daten in andere Mitgliedstaaten unter Richtervorbehalt steht, ist es möglich so die Sachleitungsbefugnis der Staatsanwaltschaft[1858] zu wahren.[1859] Bedenken gegen die Übermittlung bestehen aber weiter, hinsichtlich der Wahrung informationeller Selbstbestimmung, solange kein einheitlicher datenschutzrechtlicher Standard gewährleistet ist. Da das Umsetzungsgesetz dies nicht sicherstellt unterläuft die Regelung das nationale Verfassungsrecht. Dies würde sich auch nicht mit dem Inkrafttreten der Datenschutz-Grundverordnung in Kraft treten ändern. Zwar wurde mit der Datenschutz-Grundverordnung auch ein Entwurf für eine Richtlinie formuliert.[1860] Selbst wenn diese angenommen würde, würde sie im Bereich der polizeilichen und justiziellen Zusammenarbeit aber noch kein einheitliches datenschutzrechtliches Niveau erzeugen.[1861]

Da die Vorratsdaten auf Grund ihrer hohen Aussagekraft und der vielfältigen Analysemöglichkeiten sowie dem bestehenden Missbrauchsrisiko besonders geschützt werden müssen, ist zum Schutz der informationellen Selbstbestimmung grundsätzlich zu verlangen, dass die Daten nur nach voriger richterlicher Überprüfung übermittelt werden dürfen.

9.3.1.3 Anforderungen aus Perspektive staatlicher Sicherheitsinteressen

Wichtig ist in Bezug auf die Gewährleistung von Sicherheit in jeglichem zwischenstaatlichen Verhältnis, dass der Austausch der Daten möglichst klar und eindeutig geregelt ist.

Es bedarf insofern einheitlicher Regelungen für die Übermittlung von auf Vorrat gespeicherten Verkehrsdaten ins innereuropäische Ausland. Dabei ist von zentraler Bedeutung, dass die datenschutzrechtlichen Grundsätze beachtet werden. Die Übermittlung in andere Mitgliedstaaten der Europäischen Union ist unter Richtervorbehalt zu stellen.

[1857] Selbst wenn man einen Verstoß gegen das Recht auf informationelle Selbstbestimmung annimmt, führt dies nicht zur Verfassungswidrigkeit der Regelung, da diese aufgrund der „Solange" Rechtsprechung keiner verfassungsrechtlichen Prüfung am Maßstab der Grundrechte zugänglich ist, vgl. zur Solange-Rechtsprechung des *BVerfG,* oben S. 57, Fn. 264; S. 170 ff.

[1858] Vgl. § 152 Abs. 1 GVG; § 161 Abs. 1 S. 2 StPO.

[1859] *Böse* 2007, 128 fordert hier, dass bei grenzüberschreitender Übermittlung von sensitiven Daten die Entscheidung der Justiz überlassen werden müsse.

[1860] Mit dem Vorschlag für eine „Richtlinie zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Aufdeckung, Untersuchung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr" vorgelegt und damit auch der Bereich der Datenverarbeitung im Bereich der polizeilichen und justiziellen Zusammenarbeit miteinbezogen, KOM (2012) 10; vgl. zur Gesamtstrategie auch KOM (2012) 9.

[1861] Zum Entwurf der Datenschutz-Grundverordnung, vgl. oben S. 91 f.

9.3.2 Staatliches Freiheitsinteresse

Staatliches Interesse ist nicht nur die Gewährleistung von Sicherheit. Vielmehr wurde schon in Kap. 3 aufgezeigt, dass die Verfassung das Verhältnis von Freiheit und Sicherheit im Sinne der „Sicherheit als Diener der Freiheit" konzipiert hat.[1862] Das Bekenntnis der Verfassung zu einer freiheitlichen Grundordnung kommt nicht nur in den Grundrechten der Betroffenen (Dimension Staat – Bürger) und jener der Telekommunikationsunternehmen (Dimension Staat – Wirtschaft) zum Ausdruck, sondern auch in staatsorganisationsrechtlichen Regelungen, die die freiheitliche Grundordnung schützen. Dem dient unter anderem die Verteilung von Zuständigkeiten und Befugnissen zur Gewährleistung der inneren wie äußeren Sicherheit auf Polizei, Geheimdienste und Militär sowie die Aufteilung zwischen Bundes- und Landesbehörden. Es sind Bundesstaats-, Rechtsstaats- und Demokratieprinzip, die das staatliche Freiheitsinteresse im Grundgesetz widerspiegeln. Sie verpflichten den Staat zur Gewährleistung informationeller Gewaltenteilung, einer Trennung von Polizei und Nachrichtendiensten sowie dazu, den gesamten Sicherheitsapparat transparent zu gestalten.

9.3.2.1 Informationelle Gewaltenteilung

Auf der einen Seite steht das staatliche Interesse, dass möglichst jede Behörde möglichst umfassend die ermittlungstechnisch interessanten Daten erhält. Auf der anderen Seite ist die informationelle Gewaltenteilung als Instrument der Freiheitssicherung zu beachten.

Das Prinzip der Gewaltenteilung ist einer der fundamentalen Verfassungsgrundsätze, der in seinem Kerngehalt änderungsfest im Grundgesetz verankert ist.[1863] Es wird dabei zwischen funktionaler und institutioneller Gewaltenteilung unterschieden. Das Gewaltenteilungskonzept des Grundgesetzes zeichnet sich durch „gegenseitige Kontrolle, Hemmung und Mäßigung der Gewalten" aus.[1864] Das Grundgesetz garantiert als Ausprägung und Ausdehnung der klassischen Gewaltenteilung auf die öffentliche Verwaltung auch die informationelle Gewaltenteilung.[1865] In diesem Sinne betont das *Bundesverfassungsgericht*: „aus der Einheit der Gemeindeverwaltung folgt keine informationelle Einheit".[1866] Vielmehr müsse die informationelle Gewaltenteilung gewährleistet werden. Dass es eben keine informationelle Einheit der Staatsgewalt gibt zeigt sich in Art. 35 Abs. 1 GG, der eine Regelung zur Rechts- und Amtshilfe trifft, die nur aus dem Grund notwendig ist, weil eben auch in informationeller Hinsicht, eine Trennung zwischen den verschiedenen Behörden besteht.[1867] Daneben ist die informationelle Gewaltenteilung auch Ausfluss des Zweckbindungsgrundsatzes. Dieser verlangt, dass

---

[1862] Vgl. oben Kap. 3.3.

[1863] *Di Fabio,* in: *Isensee/Kirchof,* HStR II, 2004, § 27, Rn. 1, 4.

[1864] BVerfGE 34, 52 (59); „Seine Bedeutung liegt in der politischen Machtverteilung, dem Ineinandergreifen der drei Gewalten und der daraus resultierenden Mäßigung der Staatsherrschaft", BVerfGE 3, 225 (247); 95, 1 (15) sowie stRspr BVerfG; dazu auch *Sommermann,* in *Mangoldt/Klein/Starck,* GG 2010, Art. 20 Rn. 212.

[1865] *Forgó/Krügel/Rapp* 2006, 49; *Podlech*, 1973, 9.

[1866] *BVerfG*, Beschl. v. 18.12.1987 – 1 BvR 962/87, NJW 1988, 959.

[1867] Art. 35 Abs. 1 GG enthält eine Regelung zur Rechts- und Amtshilfe. Darin kommt zum Ausdruck, dass es eben keine (informationelle) Einheit der Staatsgewalt gibt; dazu auch *Tinnefeld/Ehmann/Gerling* 2005, 151.

die Zwecke einer Datenverwendung und damit auch die Entscheidung, wer wie die Daten verwerten darf, ausdrücklich und eindeutig geregelt sein müssen.[1868] Der Gewährleistung (informationeller) Gewaltenteilung dient auch das Bundesstaatsprinzip. Informationelle Gewaltenteilung meint die interne wie externe Daten-Abschottung, nach der die Zweckbindung bei der Verarbeitung personenbezogener Daten durch staatliche Stellen gewährleistet werden muss: sowohl bei der Übermittlung zwischen verschiedenen Stellen als auch bei der Verarbeitung von einer Stelle zu verschiedenen Zwecke.[1869]

Die informationelle Gewaltenteilung muss auch bei der Ausgestaltung der Vorratsdatenspeicherung, insbesondere bei den Zugriffs-, Weitergabe- und Verwendungsregelungen gewahrt werden.

9.3.2.2 Bundesstaatlichkeit

Die Ordnung Deutschlands in einem föderalistischen System[1870] ist Ausdruck der vertikalen Gewaltenteilung. Ziel dieser ist, wie auch der horizontalen Gewaltenteilung, eine gegenseitige Machtbegrenzung, um eine übermächtige Staatsgewalt zu verhindern.[1871] Dies muss auch bei einer Neuregelung der Vorratsdatenspeicherung berücksichtigt werden und ist insbesondere in Bezug auf die Gesetzgebungskompetenzen von Bedeutung.

Denn im Bereich der Gefahrenabwehr und der Strafverfolgung ist die Gesetzgebungskompetenz zwischen dem Landes- und dem Bundesgesetzgeber föderal aufgeteilt: Für die Gefahrenabwehr sind grundsätzlich gemäß Art. 70 Abs. 1 GG die Länder zuständig. Eine Ausnahme bildet der Art. 73 Abs. 1 Nr. 9a GG, der die Zuständigkeit des Bundesgesetzgebers für den Bereich der Abwehr von (konkreten) Gefahren des internationalen Terrorismus begründet.[1872] Infolge dessen wurden dem Bundeskriminalamt im Bereich der Abwehr von Gefahren durch den internationalen Terrorismus Befugnisse zugewiesen, die bis dato nur den Polizeien der Länder zustanden. Die Gesetzgebungskompetenz für die Zusammenarbeit von Bund und Ländern im Bereich der Bekämpfung organisierter Kriminalität und Terrorismus liegt nach Art. 73 Abs. 1 Nr. 9a und 10 sowie Abs. 2 GG beim Bund. Für das Strafrecht und das Strafverfolgungsrecht hat der Bundesgesetzgeber von der ihm in konkurrierender Gesetzgebung gemäß Art. 74 Abs. 1 Nr. 1 GG zugewiesenen Kompetenz abschließend Gebrauch gemacht. Auch für das Telekommunikationsrecht besitzt der Bundesgesetzgeber die Regelungskompetenz nach Art. 73 Abs. 1 Nr. 7 GG.

[1868] Vgl. ausführlich zum Zweckbindungsgrundsatz, oben S. 87 f.

[1869] Zum Prinzip der informationellen Gewaltenteilung auch *Petri,* in: *Lisken/Denninger,* 2012, G, Rn. 435.

[1870] Der Aufbau Deutschlands in einem föderalistischen System ist durch die Bezeichnung in Art. 20 Abs. 1 GG als demokratischer und sozialer Bundesstaat und die von der Ewigkeitsgarantie umfasste „Gliederung des Bundes in Länder" eindeutig festgelegt, *Jestadt* in HStR II, § 29 Rn. 15 u. 19.

[1871] Vgl. zum Grundsatz der Gewaltenteilung, schon oben Kap. 2.1.4.3, S. 107 f.

[1872] Dieser weist dem Bund die ausschließliche Gesetzgebungskompetenz für Fälle zu, in denen eine länderübergreifende Gefahr vorliegt, die Zuständigkeit einer Landesbehörde nicht erkennbar ist oder die oberste Landesbehörde um eine Übernahme ersucht.

Dieser bildet die Kompetenzgrundlage für die Anordnung einer Speicherungsverpflichtung der Telekommunikationsverkehrsdaten auf Vorrat, da diese das Telekommunikationsrecht betrifft. Darüber hinaus obliegen auch die Gewährleistung der Datensicherheit und die normenklare Begrenzung der Zwecke der möglichen Datenverwendung „als untrennbare Bestandteile der Anordnung der Speicherungsverpflichtung dem Bundesgesetzgeber".[1873] Der Grund dafür liegt darin, dass, so das *Bundesverfassungsgericht* überzeugend, Speicherung und Zweckbindung bei einer Vorratsdatenspeicherung untrennbar verknüpft sind. Auf Grund des Verbots einer Datenspeicherung zu unbestimmten Zwecken[1874] stünden die Speicherungsverpflichtung und die Regelung der Verwendungszwecke in einem „unaufhebbaren verfassungsrechtlichen Zusammenhang (…). Eine Speicherung kann nicht als solche abstrakt gerechtfertigt werden, sondern nur insoweit, als sie hinreichend gewichtigen, konkret benannten Zwecken dient." Es sei unzulässig einen Datenpool zu schaffen, „dessen Nutzung je nach Bedarf und politischem Ermessen der späteren Entscheidung verschiedener staatlicher Instanzen überlassen bleibt".[1875] Die materielle Verknüpfung von Speicherung und Verwendungszweck als „maßgebliches Bindeglied zwischen Eingriff und Rechtfertigung" dürfe so auch „im Zusammenspiel von Bund und Ländern nicht aufgebrochen werden".[1876] Der Bundesgesetzgeber müsse die qualifizierten Voraussetzungen für die Verwendung der Daten zum Zwecke der Strafverfolgung, der Gefahrenabwehr und der Gefahrenprävention treffen, ebenso wie die „notwendigen Regelungen zur Aufrechterhaltung der Zweckbindung bei der weiteren Verwendung der Daten, insbesondere in Form von Kennzeichnungs- und Protokollierungspflichten".[1877]

Nicht der Regelungskompetenz des Bundesgesetzgebers unterfalle hingegen die Regelung, „ob und wieweit" im Rahmen der von ihm festzulegenden Zwecke „tatsächlich" auf die Daten zurückgegriffen werden darf. Die Normierung der Abrufregelungen richte sich vielmehr nach den allgemeinen Gesetzgebungskompetenzen und muss daher nach den oben genannten Grundlagen erfolgen. Für den Bereich der Gefahrenabwehr und die Regelung der Zugriffsrechte liegt sie demnach bei den Ländern, lediglich zur Abwehr von Gefahren des internationalen Terrorismus liegt die Regelungskompetenz beim Bundesgesetzgeber.

Zu unterscheiden von der Frage der Gesetzgebungskompetenz ist, wer die jeweiligen Aufgaben ausführt. Hier gilt gemäß Art. 83 GG der Grundsatz des Landesvollzugs. Allein in den in §§ 4, 4a BKAG genannten Fällen, verfügt das Bundeskriminalamt über die Kompetenz zur Abwehr von Gefahren und zur Strafverfolgung. Grundsätzlich ist jedenfalls die Landesjustiz (§§ 74, 24, 142 Abs. 1 Nr. 2 und 3 GVG) originär für die Verfolgung von Straftaten und die Gefahrenabwehr zuständig und somit auch für den Abruf und die darauf folgende behördeninterne Speicherung, Verwaltung und Löschung der Daten.

[1873] BVerfGE 125, 260 (LS 3; 344 f.).
[1874] Vgl. zu diesem oben S. 139.
[1875] BVerfGE 125, 260 (345).
[1876] BVerfGE 125, 260 (346).
[1877] BVerfGE 125, 260 (346).

9.3.2.3 Trennung von Polizei und Nachrichtendiensten

Neben der föderalen Aufteilung sowohl von Gesetzgebung als auch Aufgabenverteilung, sieht das Grundgesetz eine strikte Trennung zwischen den Aufgaben der Polizei und der Nachrichtendienste vor.[1878] Ausdrücklich ist dieses Trennungsgebot nicht im Grundgesetz normiert. Es schlägt sich aber in der Funktionentrennung in Art. 87 Abs. 1 S. 2 GG nieder.[1879] Das Trennungsgebot wird zudem durch die organisationsrechtliche Aufteilung der Zuständigkeiten für Gefahrenabwehr auf die Länder und für die Nachrichtendienste und Abwehr „militärischer" Gefahren auf den Bund untermauert und kann schließlich historisch begründet werden. Hintergrund ist, dass die Verfassungskonstitution unter dem Eindruck der Übermacht der Geheimpolizei im Dritten Reich das Ziel verfolgte eine solche zukünftig zu verhindern. Dazu diente die Trennung zwischen nachrichtendienstlichen und polizeilichen Befugnissen.[1880] Ob das Trennungsgebot Verfassungsrang besitzt ist umstritten.[1881] Unabhängig von diesem Streit ist jedoch evident, dass das Grundgesetz eine Trennung von Nachrichtendiensten und Polizei organisationsrechtlich vorsieht. Diese grundlegenden Verfassungsnormen gilt es auch bei der Ausgestaltung der Vorratsdatenspeicherung zu beachten.

Der Erkenntnisaustausch zwischen dem Bundesamt für Verfassungsschutz und anderen Behörden, die für den Bundesnachrichtendienst und den Militärischen Abschirmdienst teilweise entsprechend gelten, sind in §§ 17 bis 26 BVerfSchG geregelt. Zur Koordinierung bei der Bekämpfung internationalen Terrorismus, wurde im Jahr 2004 das Gemeinsame Terrorismusabwehrzentrum (GTAZ) und nach diesem Vorbild 2012 das Gemeinsame Abwehrzentrum gegen Rechtsterrorismus (GAR) geschaffen.[1882] Nicht nur an diesen, sondern auch in Bezug auf die Novelle des Bundeskriminalamtgesetzes aus dem Jahr 2008 und anderen Neuerungen wurde vielfach und zutreffend kritisiert, dass das Trennungsgebot durch intensiven Datenfluss, Ausweitung der polizeilichen Befugnisse im Gefahrenvorfeld sowie die Ausweitung nachrichtendienstlicher Befugnisse aufgeweicht werde.[1883] Diese Tendenz läuft den verfassungsrechtlichen Vorgaben zuwider. Eine strikte Trennung der Aufgaben von Polizei und Nachrichtendiensten verlangt die Verfassung und ist im Hinblick auf die Sicherung einer freiheitlichen Grundordnung auch geboten. Gegenläufige Tendenzen einer immer stärkeren Zusammenarbeit der Behörden und der Verlagerung von Kompetenzen widerspricht der Verfassung der Bundesrepublik, die darauf angelegt ist eine übermächtige Polizeibehörde zu verhindern.

[1878] Vgl. ausführlich zum Trennungsgebot, *Klee* 2010, 51 ff..

[1879] *Roggan/Bergemann*, NJW 2007, 876; zum Teil wird es auch mit dem Rechtsstaatsprinzip begründet, so etwa: *Denninger*, ZRP 1981, 231, 232.

[1880] Dazu *Nehm,* NJW 2004, 3289, 2390.

[1881] Ausführlich mit dieser Frage und den Ansichten in der Literatur befasst sich *Klee* 2010, 51 ff., der im Ergebnis den Verfassungsrang ablehnt (S. 64).

[1882] Ausführlich mit der Rechtsform und den Rechtsproblemen, die durch die Begründung der GATZ entstanden sind, *Weisser*, NVwZ 2011, 142; vgl. dazu auch schon oben S. 64.

[1883] *Gusy*, ZRP 2008, 36; *Weisser*, NVwZ 2011, 142; *Roggan/Bergemann,* NJW 2007, 876; *Baum, Schantz,* ZRP 2008, 137.

Es gilt daher bei der Ausgestaltung der Vorratsdatenspeicherung, insbesondere bei der Regelungen zum Zugriff und der Weitergabe von gewonnen Informationen, das Trennungsgebot zu bewahren.

9.3.2.4 Transparente Staatsgewalt

Die Verfassung sieht eine freiheitliche Grundordnung vor.[1884] Dabei ist dem Staat das Gewaltmonopol übertragen.[1885] Dabei dient diese dazu dem Bürger Freiheit vor Willkür zu gewähren. Es muss insofern sichergestellt sein, dass die Arbeit der Polizeibehörden nicht willkürlich verläuft. Wesentlich dafür ist die Kontrollierbarkeit und Kontrolle der Polizeiarbeit – also ihre Transparenz.

Die Verpflichtung zu einer transparenten Polizei spiegelt sich auch in der im Grundgesetz angelegten Sicherheitsarchitektur der Bundesrepublik.[1886] Zunächst ist die Exekutive an die Verfassung gebunden.[1887] Die einzelnen Polizeibehörden und die Nachrichtendienste unterstehen in einer Weisungskette den Innenministerien. Außerdem unterliegen die Polizeibehörden der gerichtlichen Kontrolle und die Nachrichtendienste unterstehen der parlamentarischen Kontrolle.[1888]

Gerade weil weit streuende Überwachungsmaßnahmen umgesetzt werden, kommt der Transparenz der Ermittlungsarbeit von Polizei und Nachrichtendiensten eine besonders hohe Bedeutung zu – denn eine geheime Staatspolizei „erschüttert das Vertrauen der Bürger“ in den Staat.[1889] Daher steht es im staatlichen Freiheitsinteresse, dass die Vorratsdatenspeicherung so ausgestaltet wird, dass diese möglichst transparent erfolgt.

9.3.3 Elemente eines Interessenausgleichs

Anknüpfungspunkte zur Auflösung des Spannungsverhältnisses zwischen staatlichen Sicherheits- und Freiheitsinteressen bieten die Zugriffsregelungen und die Bestimmungen über die Weitergabe der Vorratsdaten bzw. der aus ihnen gewonnen Informationen. Dabei konnten in jeder Dimension Ansätze identifiziert werden, welche für die Beeinträchtigung der betroffenen Interessen wesentlich sind und deren Gestaltung somit für einen Interessenausgleich genutzt werden kann. Wesentlich sind so dann rechtliche, technische und organisatorische Maßnahmen um sicherzustellen, dass sich insgesamt keine umfassende gesamtgesellschaftliche Überwachung realisiert.

[1884] Vgl. oben S. 108 ff.
[1885] Vgl. oben Kap. 2.2.1.
[1886] Vgl. oben Kap. 2.2.5.
[1887] Art. 1 Abs. 3 GG.
[1888] Sämtliche Nachrichtendienste unterstehen der parlamentarischen Kontrolle, die zuletzt mit Gesetz v. 29.7.2009 gestärkt wurde (Gesetz zur Fortentwicklung der parlamentarischen Kontrolle der Nachrichtendienste (BGBl. 2009 I, 2346), PKGrG; dazu *Huber*, NVwZ 2009, 1321.
[1889] *Albrecht* 16.2.2012.

10 Gestaltungsvorschläge für einen optimierten Interessenausgleich

Mittels der Analyse der verschiedenen von der Vorratsdatenspeicherung betroffenen Dimensionen[1890] konnten verschiedene Elemente identifiziert werden, die als Anknüpfungspunkte für die Optimierung des Interessenausgleichs dienen können. Es wurden sodann die Anforderungen identifiziert, die es für eine verfassungsverträgliche Ausgestaltung der Vorratsdatenspeicherung zu berücksichtigen gilt. [1891]

Für die Entwicklung von optimierten Gestaltungsvorschlägen, ist zunächst zwischen der Ebene der Datenerhebung und jener der Datenverwendung zu unterscheiden. In Bezug auf die Ausgestaltung der Datenerhebung, also der Speicherungsverpflichtung eigenen sich insbesondere Regelungen zu den erfassten Datenkategorien, dem Speicherzeitraum, den Adressaten der Speicherung, dem Speicherort, der Datensicherheit, der Frage der Kostentragung, einem Schutz von Vertrauensbeziehungen und schließlich dem Verfahren der Datenübertragung, dazu den Interessenausgleich zu optimieren.

Anknüpfungspunkte auf der Ebene der Datenverwendung sind sodann die Zugriffsregelungen, der Umfang des Datenabrufs, die Frage der Proliferation der abgerufenen Daten an andere Stellen und ob die Daten mittelbar zu anderen Zwecken genutzt werden können sowie das Abrufverfahren, die Bedingungen der Datenspeicherung bei staatlichen Stellen und schließlich die Datenübermittlung zwischen verschiedenen innerstaatlichen Stellen sowie in andere Staaten.

Neben den Ebenen der Datenerhebung und -verwendung kann ein Interessenausgleich durch Regelungen zu Transparenz und Rechtsschutz und schließlich der Wahrung des Verbots einer umfassenden gesamtgesellschaftlichen Überwachung, also durch Vorkehrungen zur Durchführung der Überwachungs-Gesamtrechnung erzielt werden.

Es wurden in allen Dimensionen verschiedene Anforderungen jeweils aus Perspektive der Sicherheits- wie der Freiheitsinteressen, die für eine verfassungsverträgliche Ausgestaltung zu berücksichtigen sind, ermittelt. Diese Anforderungen sollen hier nicht vorab, sondern jeweils konkret bei den einzelnen Gestaltungselementen wiederholt werden. Im Folgenden wird nun umfassend für jedes einzelne Gestaltungselement erörtert, welche Vorgaben sich aus der Vorratsdatenspeicherungsrichtlinie und aus der Verfassung ergeben, welche Gestaltungsanforderungen zu beachten sind und wie sich die Interessenkollision im Einzelnen auswirkt.

Daran schließt sich eine Folgenabschätzung an: Welche Einbußen und welche Vorteile bringt die jeweilige Ausgestaltung für Freiheits- und Sicherheitsinteressen? Sodann

[1890] Staat-Bürger, S. 264 ff.; Staat-Wirtschaft, S. 296 ff.; Staat-Staat, S. 319 ff.

[1891] Die entwickelten Gestaltungsvorschläge beruhen auf den Ergebnissen des Forschungsprojekts INVODAS, welche gemeinsam mit *S. Schweda* (EMR; Saarbrücken) unter der Leitung von Prof. *Roßnagel* entwickelt wurden. Die Ergebnisse des Projekts und so auch die hier dargestellten Gestaltungsvorschläge wurden ebenfalls im Forschungsbericht *Roßnagel/Moser-Knierim/Schweda,* 2013, S. 123 ff. veröffentlicht.

A. Moser-Knierim, *Vorratsdatenspeicherung,* DuD-Fachbeiträge,
DOI 10.1007/978-3-658-04156-4_10, © Springer Fachmedien Wiesbaden 2014

wird jeweils ein Gestaltungsvorschlag vorgestellt, der im Hinblick auf die ermittelte Interessenkollision und ihre Gewichte es vermag ein möglichst hohes Maß an Kohärenz zu erzeugen.

10.1 Datenerhebung – Ausgestaltung der Speicherungsverpflichtung

Das Wesen der Vorratsdatenspeicherung besteht darin, dass flächendeckend ohne Anlass von jedem Bürger Telekommunikationsverkehrsdaten für einen bestimmten Zeitraum vorgehalten werden, und zwar für den Fall, dass eventuell ein berechtigtes staatliches Interesse besteht, auf diese Daten zuzugreifen. Es handelt sich bei der Datenspeicherung um einen besonders schweren Grundrechtseingriff.[1892] Die Datenerhebung und -speicherung bildet die Grundlage der Vorratsdatenspeicherung. Ihre Ausgestaltung beeinflusst den Interessenausgleich im Rahmen einer Vorratsdatenspeicherung grundlegend.

10.1.1 Datenkategorien

Die Auswahl der Datenkategorien ist geeignet das Eingriffsgewicht zu reduzieren − und zwar sowohl für den Bürger als auch für die betroffenen Unternehmen. Wenn weniger Daten gespeichert werden, verringern sich nicht nur die Analysemöglichkeiten und damit auch die Aussagekraft der Daten, sondern auch der Umfang der zu speichernden Daten und damit auch die Pflege und Sicherung der gespeicherten Daten für die verpflichteten Unternehmen.

Zu speichern sind gemäß Art. 5 Abs. 1 VDS-RL die Daten die zur Bestimmung, wer, wann mit wem, wie und von wo aus kommuniziert hat.[1893] Inhaltsdaten dürfen gem. Art. 1 Abs. 2 S. 2 VDS-RL nicht gespeichert werden. Die Speicherpflicht bezieht sich nur auf Daten, die bei den Telekommunikationsanbietern ohnehin anfallen. In Bezug auf die zu speichernden Datenkategorien ist der den Mitgliedstaaten verbleibende Gestaltungsspielraum minimal. Mit den dort genannten Kategorien wird das Telekommunikationsverhalten nahezu vollständig erfasst.[1894]

Nach der hier vertretenen Ansicht handelt es sich bei einer Verpflichtung zur Speicherung der Telekommunikationsverkehrsdaten auf Vorrat um kein unverzichtbares und auch um kein alternativloses Instrument. Insofern sollte im Sinne eines optimierten Interessensausgleichs auf die Maßnahme verzichtet werden, da es grundrechtsschonendere Alternativen gibt und die Gewährleistung von Sicherheit ohne eine Vorratsdatenspeicherung nicht in Frage gestellt wird. Die Vorratsdatenspeicherung ist keineswegs unentbehrlich zur Verfolgung und Aufklärung von schweren Straftaten im digitalen Zeitalter.[1895]

[1892] Vgl. oben S. 274 ff.
[1893] Eine ausführliche Darstellung des Regelungsgehalts der VDS-RL in Bezug auf die Datenkategorien findet sich in Kap. 4.1.2; S. 143 f.
[1894] Zu den Ausnahmen, vgl. oben S. 143 ff.
[1895] Vgl. dazu oben Kap. 4.4.2, insbes. S. 203 ff.

Die Richtlinie verlangt jedoch aktuell eine Umsetzung. Insofern ist die Frage, wie im Rahmen der Richtlinie ein möglichst optimierter Interessenausgleich erzeugt werden kann, zu beantworten.

Verfassungsrechtlich zwingend gefordert ist im Hinblick auf die Interessen der Bürger, dass die Telekommunikationsfreiheit grundsätzlich gewahrt bleibt. Auch sind der Kernbereich privater Lebensgestaltung, die Berufsfreiheit von Berufsgeheimnisträgern wie Seelsorgern, und Ärzten und die Pressefreiheit zu schützen. Schließlich ist im Hinblick auf die Erforderlichkeit und Geeignetheit oder auf die Unverzichtbarkeit und Alternativlosigkeit der Vorratsdatenspeicherung sowohl im Hinblick auf die Freiheitsinteressen der Bürger als auch die staatlichen Sicherheitsinteressen zu fragen, wie groß die Rolle einzelner Datenkategorien für die Sicherheit ist. Auch der datenschutzrechtliche Grundsatz der Erforderlichkeit[1896] gebietet es, dass der Speicherumfang auf das unbedingt erforderliche Maß reduziert wird.

Im Interesse der Telekommunikationsanbieter ist sodann die Formulierung einer eindeutigen und abschließenden Regelung. Dabei ist von Bedeutung, dass keine Verpflichtung zur Speicherung von Daten besteht, die nicht ohnehin erhoben und verarbeitet werden.

10.1.1.1 Keine Speicherung von Inhaltsdaten

Eine umfassende Speicherung der Inhalte der Telekommunikation würde den Wesensgehalt von Art. 10 GG verletzen. Insofern ist sicherzustellen, dass die Vorratsdatenspeicherung keine Inhalte erfasst.[1897]

Als Inhaltsdaten können auch Daten gewertet werden, die „nur“ Aufschluss über den Inhalt eines Kommunikationsvorgangs erlauben – wie es etwa bei der Kommunikation mit Berufsgeheimnisträgern der Fall ist.[1898] Daten, die Vertrauensbeziehungen mit Berufsgeheimnisträgern betreffen sind jedenfalls von der Verpflichtung zur Vorratsdatenspeicherung auszunehmen.

10.1.1.2 Differenzierung zwischen verschiedenen Datentypen

Das Interesse der Ermittlungsbehörden an den auf Vorrat gespeicherten Verkehrsdaten ist nicht an allen Datentypen gleich hoch. So werden IP-Adressen deutlich häufiger abgefragt als andere Verkehrsdaten. Auf der anderen Seite werden diese Daten vielfach auch für niederschwellige Delikte angefragt.[1899]

So wie sich das Interesse an den Daten und an der Verpflichtung zur Vorratsdatenspeicherung je nach Datentyp unterscheiden, so lassen sich auch Unterschiede im Eingriffsgewicht feststellen. Es kann zwischen IP-Zugangsdaten, Mail- und Telefonverbindungsdaten und Funkzellendaten unterschieden werden:

[1896] Vgl. oben Kap. 2.1.3.1.3.2, S. 88.
[1897] Vgl. dazu oben, S. 277.
[1898] Vgl. dazu oben S. 289.
[1899] Vgl. oben S. 168 f, 268.

- Die Speicherung der *IP-Adressen*, ihre Zuordnung zu einem Nutzer verknüpft mit dem Zeitpunkt ermöglichen die Auskunft darüber, in welchem Zeitraum eine IP-Adresse welchem Nutzer zugeordnet war. Der Aussagegehalt einer Speicherung von IP-Zugangsdaten ist jedoch begrenzt. So kann, selbst dann, wenn alle gespeicherten IP-Zugangsdaten zu einer Person für den gesamten Speicherzeitraum mitgeteilt werden, kein Profil der Internetnutzung erstellt werden. Nur in Kombination mit den bei Seitenbetreibern gespeicherten Informationen über ihre Besucher, könnte inhaltlich das Verhalten im Netz nachvollzogen werden. Insofern kann IP-Adressen aber unmittelbar eine inhaltliche Aussage entnommen werden, sodass der Eingriff durch eine Speicherung durchaus schwer wiegt.[1900]

  IP-Adressen werden insbesondere für die Verfolgung von Informations- und Kommunikationskriminalität benötigt. Im Bereich der IP-Datenspeicherung hat das Max-Planck-Institut eine Schutzlücke diagnostiziert, da hier die Daten häufig auf Grund von Flatrate-Tarifen nicht gespeichert würden.[1901]

- *Verbindungsdaten über Telefon- und Mailverkehr* beinhalten Informationen über Zeiten und Partner der Kommunikation. Daraus lässt sich teilweise unmittelbar auf den Inhalt der Kommunikation schließen. Die Analyse sämtlicher Verbindungsdaten über einen längeren Zeitraum ermöglicht es zudem, Kommunikations-, Beziehungs- und Interessenprofile des Nutzers zu erstellen.[1902] Es lassen sich aus diesen Daten „tiefe Einblicke in das soziale Umfeld und die individuellen Aktivitäten" jedes Einzelnen gewinnen und „bis in die Intimsphäre hineinreichende inhaltliche Rückschlüsse ziehen".[1903] Sie ermöglichen es schließlich, „detaillierte Aussagen zu gesellschaftlichen oder politischen Zugehörigkeiten sowie persönlichen Vorlieben, Neigungen und Schwächen" zu treffen.[1904] Auch lassen sich Organisationsstrukturen von Verbänden ermitteln.[1905]

  Mail- und Telefonverbindungsdaten können für unterschiedlichste Delikte relevant sein.[1906] Gerade im Bereich der Aufklärung von Kapitalverbrechen aber auch zur Aufdeckung der Strukturen terroristischer Organisationen, können die Verbindungsdaten als Verdachtsgewinnungsinstrument dienen.

  Verkehrsdaten werden trotz überwiegend vorhandener Flatrate-Tarife dennoch überwiegend für mindestens sieben Tage gespeichert.[1907]

[1900] Vgl. dazu auch oben S. 281 ff.
[1901] Vgl. oben S. 196.
[1902] Ausführlich zu den Analysemöglichkeiten, vgl. oben Kap. 4.4.1.1, S. 182 f.
[1903] BVerfGE 125, 260 (319).
[1904] BVerfGE 125, 260 (319).
[1905] BVerfGE 125, 260 (319).
[1906] Vgl. dazu oben, S. 188 ff.
[1907] Vgl. dazu oben Abbildung, S. 1520271.

- Als dritte Kategorie sind *Funkzellendaten* zu nennen. Durch die Auskunft über eine Funkzelle kann keine exakte Ortung erfolgen. Sie ermöglicht aber eine grobe Ortsbestimmung und so auch die Erstellung von Bewegungsprofilen, wie das Beispiel *Spitz* zeigt.[1908] Die Genauigkeit der Funkzellenauswertung hängt davon ab, wie häufig kommuniziert wird, da nur dann die Funkzellendaten erhoben werden. Für die Aussagekraft ist hier relevant, wo sich eine Person bewegt, da diese von der Funkzellendichte im jeweiligen Gebiet abhängt.[1909] Neben der Möglichkeit, individuelle Bewegungsprofile zu erstellen, ermöglicht die Auswertung der Bewegungsprofile vieler Telekommunikationsnutzer es auch, Begegnungen und damit soziale Strukturen und Beziehungen auch jenseits konkreter Telekommunikations-verbindungen zu ermitteln.[1910]

Die Darstellung zeigt, dass die verschiedenen Datenkategorien deutliche Unterschiede sowohl in der Eingriffsintensität aufweisen als auch hinsichtlich der Bedeutung für die Arbeit der Strafverfolgungs- und Gefahrenabwehrbehörden.

Zu betonen ist jedoch, dass es sich bei jeglicher Speicherung auf Vorrat – auch von nur einer einzelnen dieser Datenarten – um einen besonders schwerwiegenden Grundrechtseingriff handelt. Er wird zwar graduell durch die Reduzierung auf einzelne Daten abgemildert, es handelt sich aber in jedem Fall bei einer Verpflichtung zur Speicherung auf Vorrat um eine infrastrukturelle Überwachungsmaßnahme neuer Qualität.

Schon auf Grund der Tatsache, dass eine Verpflichtung zur Vorratsdatenspeicherung als anlasslose und verdachtsunabhängige Maßnahme zur Strafverfolgungsvorsorge mit klassischen Grundsätzen des Datenschutzes kollidiert, ist eine solche Speicherung (etwa allein der IP-Zugangsdaten) nur als Ausnahme zulässig.[1911] Auch bleibt es bei einem besonders schweren Grundrechtseingriff, so dass daraus besonders hohe Anforderungen an eine verhältnismäßige Ausgestaltung erwachsen.[1912]

Dennoch ist die hier aufgezeigte Differenzierung zwischen dem Eingriffsgewicht der einzelnen Speicherungsverpflichtungen von großer Wichtigkeit. Denn gerade wegen der Schwere des Eingriffs ist es erforderlich, dass die Ausgestaltung dem besonderen Gewicht des Eingriffs Rechnung trägt.[1913] Dem würde es entsprechen, für die drei genannten Datenkategorien unterschiedliche Speicherzeiträume und Verwendungsregelungen vorzusehen.

So könnte auch den verschiedenen Anforderungen an die Speicherungsverpflichtung aus ermittlungstechnischer Sicht genügt werden. Es wurde aufgezeigt, dass sich das

[1908] Vgl. dazu oben S. 183.
[1909] Vgl. dazu oben S. 31 ff.
[1910] BVerfGE 125, 260 (319).
[1911] Anlasslose und flächendeckende Überwachungsmaßnahmen nur als Ausnahme, dazu oben Kap. 7.2.
[1912] Vgl. dazu oben Kap. 9.1.2.1.3.2, S. 275 f.
[1913] BVerfGE 125, 260 (324, 316).

Abfrageverhalten je nach Datenart unterscheidet.[1914] Wenn eine Regelung zur Vorratsspeicherung dieser Erkenntnis Rechnung trägt, sind die Einbußen für die Arbeit der Ermittlungsbehörden gering, während die Reduzierung der Eingriffsintensität aus Sicht der Bürger und der Telekommunikationsdiensteanbieter zu begrüßen ist.

Allerdings ist zu beachten, dass die Vorratsdatenspeicherungsrichtlinie auf Grund der Mindestspeicherfrist von sechs Monaten in nationales Recht nicht mit differenzierenden Speicherzeiträumen umgesetzt werden kann. Eine solch differenzierende Lösung, wäre aber im Sinne eines optimierten Interessenausgleichs wünschenswert. Dafür ist es erforderlich die Richtlinie entsprechend zu ändern.

10.1.1.3 Speicherung von Portinformationen

Schwierig gestaltet sich in technischer Hinsicht die Speicherung der Verkehrsdaten, soweit der Zugang über NAT[1915] erfolgt – wie etwa bei der Nutzung des Internets mit Mobiltelefon oder TabletPC, soweit diesen keinen feste IPv6-Adresse zugewiesen ist.

Bei einem Zugang über NAT ist es für eine nachträgliche Rückverfolgung erforderlich, dass mehrere Daten gespeichert werden, nämlich die private IP-Adresse, der Port der Verbindung, die öffentliche IP-Adresse sowie der exakten Zeitpunkt der Nutzung. Port und IP-Adressen werden jedoch nur temporär und häufig nur für einen sehr kurzen Zeitraum vergeben. Dies führt dazu, dass bereits kurze Zeit, vielfach nur wenige Sekunden später, ein anderer Kunde über den Port und die öffentliche IP-Adresse das Internet nutzt. Hier scheitert eine eindeutige Identifikation, sobald die Portinformationen nicht gespeichert werden.[1916]

Entsprechend fordern auch Vertreter von Polizei und Staatsanwaltschaft, dass diese Daten bei einer Neueinführung der Vorratsdatenspeicherung von der Speicherungsverpflichtung mit erfasst werden sollten.[1917] Selbst wenn dies der Fall ist, scheidet aber vielfach eine genaue Zuordnung zu einem bestimmten Nutzer aus, da die Adressen in Sekundenschnelle neu vergeben werden und so auch trotz Speicherung der Portinformationen eine exakte Zuordnung scheitert. Die Folgen eines Verzichts auf die Speicherung von Portinformationen sind also letztlich begrenzt. Dies gilt insbesondere in Anbetracht der Tatsache, dass moderne mobile Endgeräte vielfach bereits IPv6 nutzen und daher (soweit keine Privacy-Extension aktiviert wurden) eine Identifikation auch ohne Speicherung von Portinformationen möglich ist.

Darüber hinaus würde eine Verpflichtung zur Speicherung der Portinformationen über die Vorgaben der Richtlinie hinausschießen. Denn es handelt sich um keine Daten, die ohnehin bei den Telekommunikationsanbietern anfallen. Verletzt würde insofern auch das Gebot einer grundrechtsschonenden Umsetzung der ohnehin besonders eingriffsgewichtigen Verpflichtung zur Vorratsdatenspeicherung.

[1914] Vgl. oben S. 186 ff.
[1915] Vgl. zu NAT schon oben S. 25 ff.
[1916] Vgl. dazu schon ausführlich oben S. 34, 144.
[1917] Vgl. oben S. 196.

10.1.1.4 Empfehlung

Dem europäischen Gesetzgeber wird empfohlen Reduzierung der Eingriffsintensität eine Beschränkung der Datenkategorien auf ein Minimum empfohlen. Soweit überhaupt eine Entscheidung für eine Speicherung gefällt wird, sollte zwischen verschiedenen Datenkategorien differenziert, Daten über die Kommunikation mit Berufsgeheimnisträgern und Vertrauenspersonen von der Speicherung ausgenommen und schließlich keine Verpflichtung zur Speicherung von Port-Informationen eingeführt werden.

10.1.2 Speicherzeitraum

Der Speicherzeitraum wird zum einen bestimmt durch die Speicherfrist und zum anderen durch die vorgegebenen Löschfristen.

10.1.2.1Speicherfrist

Nach den Vorgaben der Vorratsdatenspeicherungsrichtlinie sind die Daten für mindestens sechs und maximal 24 Monate zu speichern.[1918] Das *Bundesverfassungsgericht* hat in einer sechsmonatigen Speicherung die Obergrenze für eine verfassungsrechtlich vertretbare Speicherung der Telekommunikationsverkehrsdaten auf Vorrat gesehen.[1919] Näher begründet hat das Gericht dies nicht. Es kann nur vermutet werden, dass der Grund für die Beschränkung des Speicherzeitraums darin liegt, dass je länger dieser ist, desto genauere und aussagekräftigere Persönlichkeitsprofile erstellt werden können.[1920]

Momentan ist aufgrund der Vorgaben der Richtlinie und der verfassungsrechtlichen Vorgaben kein Gestaltungsspielraum vorhanden: die Speicherfrist ist auf sechs Monate festzulegen.

Die Bemessung des Speicherzeitraums wäre jedoch geeignet, um den Interessenausgleich zu optimieren. Dies gilt insbesondere in Anbetracht der Tatsache, dass die Anzahl der Abfragen mit der Dauer der Speicherung sinkt und somit ihre Relevanz für die Ermittlungsarbeit nachlässt. Insofern könnte ohne gravierende Einbußen für die Arbeit der Ermittlungsbehörden der Speicherzeitraum reduziert und damit auch das Eingriffsgewicht verringert werden. Eine Möglichkeit den Interessenausgleich zu optimieren, bestünde darin, die Speicherfrist auf das unbedingt erforderliche Maß zu beschränken. Zur Bestimmung des erforderlichen Maßes sollten empirische Untersuchungen berücksichtigt werden. Eine solche Lösung ist letztlich auch unter datenschutzrechtlichen Gesichtspunkten geboten – denn auch diese gebieten es, die Speicherung auf das unbedingt erforderliche Maß zu reduzieren.[1921]

Es wurde aufgezeigt, dass die verschiedenen Datenkategorien unterschiedliches Eingriffsgewicht aufweisen, aber auch von unterschiedlicher Bedeutung für die Strafver-

[1918] Ausführlich zu den Anforderungen der RL in Bezug auf den Speicherzeitraum, vgl. oben S. 144.
[1919] BVerfGE 125, 260 (322).
[1920] Vgl. zur Kritik an dieser Forderung, oben S. 128 ff.
[1921] Zum Grundsatz der Erforderlichkeit und zum Grundsatz der Datenvermeidung und -sparsamkeit, vgl. oben S. 88 f.

folgung und Gefahrenabwehr sind.[1922] Vorstellbar ist insofern für IP-Zugangsdaten eine relativ kurze Speicherfrist vorzusehen, den Zugriff aber auch für niederschwellige Delikte zu eröffnen. Während für sonstige Verbindungs- und Standortdaten ein längerer Speicherzeitraum vorgegeben wird, der Zugriff auf diese aber auf besonders schwere Straftaten begrenzt wird. Alternativ könnte auch nur für IP-Adressen eine Speicherverpflichtung vorgegeben werden, da nur hier nachweislich Schutzlücken bestehen. Dafür spricht auch, dass bei Verbindungsdaten und Standortdaten, das Risiko einer Profilbildung besteht. Das Ermittlungstechnische Interesse an einer Vorratsdatenspeicherung dieser Datenkategorien ist sodann geringer, da diese Daten ohnehin für einen gewissen Zeitraum bei der Mehrzahl der Anbieter gespeichert werden.

Um eine solche Differenzierung im Rahmen der Speicherungsverpflichtung zu ermöglichen, müsste im Rahmen der Überarbeitung der Richtlinie zur Vorratsdatenspeicherung die Mindestspeicherfrist verkürzt oder idealerweise gänzlich aufgehoben werden, um den Mitgliedstaaten einen entsprechenden Gestaltungsspielraum einzuräumen.

10.1.2.2 Löschfrist

Für den Speicherzeitraum sind auch die Bestimmungen über die Löschfristen relevant. Die Vorratsdatenspeicherungsrichtlinie schreibt in Art. 7 d) vor, dass die Daten – außer jenen, die abgerufen und gesichert wurden - am Ende der Frist zu vernichten sind.

Der ehemalige § 113a Abs. 11 TKG sah vor, dass die Daten innerhalb von einem Monat gelöscht werden müssen. Auf diese Weise wurde die Speicherfrist faktisch auf sieben Monate erweitert.[1923]

Auch wenn das *Bundesverfassungsgericht* die Ausdehnung der Speicherfrist durch eine weiche Löschfrist nicht beanstandet hat, ist aus Perspektive der betroffenen Bürger eine unverzügliche Löschung zu fordern.[1924] Denn nur so kann dem Recht des Bürgers entsprochen werden, zu wissen, welche Daten über ihn gespeichert werden.[1925] Bei der Regelung der Löschfrist sind auch die Interessen der betroffenen Unternehmen zu berücksichtigen. Diese müssen in der Lage sein, die Löschung in der vorgegebenen Frist durchzuführen. Eine unmittelbare Löschung[1926] nach Ablauf des Speicherzeitraums ist in Anbetracht der großen Datenmengen und der technischen Rahmenbedingungen kaum zu realisieren. Aus Perspektive der betroffenen Unternehmen ist insoweit die Möglichkeit einer Löschung in bestimmten Intervallen zu fordern. Denkbar ist insofern, eine wöchentliche Löschung nach Ablauf des Speicherzeitraums vorzuschreiben. Jedenfalls muss sichergestellt werden, dass die Daten erfolgreich gelöscht wurden und

[1922] S. hierzu Kap. 186 ff., insbes. 188 ff., 203 f.
[1923] *Szuba* 2011, 138; *Hoeren*, JZ 2008, 668, 669.
[1924] Vorgesehen ist eine „unverzügliche Löschung“ etwa in § 96 Abs. 1 TKG. Darunter wird ein „sehr zeitnahes Löschen“ verstanden. Soweit möglich und nicht unverhältnismäßig, sind die Daten „unmittelbar“ nach dem Ende der Verbindung zu löschen, *Eckhardt,* in: *Spindler/Schuster* 2011, § 96 TKG Rn. 6; *Graf* 2011, § 96 TKG Rn. 6.
[1925] Ausführlich zum Recht auf informationelle Selbstbestimmung, vgl. oben Kap. 2.1.3.1, S. 81 ff.
[1926] *Szuba* 2011, 253 fordert etwa eine „unverzügliche Löschung“ der Daten.

eine Wiederherstellung der Dateien nicht möglich ist. Erforderlich ist dafür das mindestens einmalige Überschreiben der Daten mit Zufallsdaten.[1927]

10.1.2.3 Empfehlung

Empfohlen wird die Speicherfrist so kurz wie möglich zu bemessen und dabei zwischen verschiedenen Datenkategorien zu unterscheiden. Bezüglich einer Löschfrist wird empfohlen eine unmittelbare und vollständige Löschung der Daten (innerhalb von einer Woche) nach Ablauf der Speicherfrist zu verlangen.

10.1.3 Adressaten

Auch die Auswahl der Adressaten der Speicherungsverpflichtung bietet einen Anknüpfungspunkt für die Optimierung des Interessenausgleichs im Hinblick auf die Interessen der Telekommunikationsanbieter, aber auch unter datenschutzrechtlichen Gesichtspunkten.

Gemäß Art. 1 Abs. 1 VDS-RL sind die Anbieter „öffentlich zugänglicher elektronischer Kommunikationsdienste oder Betreiber eines öffentlichen Kommunikationsnetzes" zur Vorratsdatenspeicherung zu verpflichten. In Deutschland wurden in § 113a Abs. 1 S. 1 TKG a.F. diejenigen verpflichtet, „die öffentlich zugängliche Telekommunikationsdienste für Endnutzer" erbringen.[1928] Wer konkret von dieser Regelung erfasst wurde, war zum Teil umstritten.[1929] Unter dem Gesichtspunkt der Rechtssicherheit ist eine eindeutige Nennung der Adressaten zu fordern, die sich an den im Telekommunikationsgesetz gebräuchlichen Wendungen orientieren sollte.[1930]

Zu berücksichtigen sind bei der Auswahl der Speicherungsverpflichteten aus Perspektive der Bürger der Grundsatz der Datensparsamkeit[1931] und aus Perspektive der verpflichteten Telekommunikationsdiensteanbieter das Erdrosslungsverbot[1932] sowie das Gleichbehandlungsgebot.[1933]

Der Grundsatz der Datensparsamkeit gebietet, dass eine doppelte Speicherung von Verkehrsdaten zu verhindern ist. Diesem Gebot entsprechend waren auch in den für

---

[1927] *Szuba* 2011, 253; *Roßnagel/Bedner/Knopp*, DUD 2009, 536 , 539; generell zum sicheren Löschen: *Fox*, DUD 2009, 110.

[1928] Telekommunikationsdienste wird in § 3 Nr. 24 TKG legal definiert als „in der Regel gegen Entgelt erbrachte Dienste, die ganz oder überwiegend in der Übertragung von Signalen über Telekommunikationsnetze bestehen, einschließlich Übertragungsdienste in Rundfunknetze".

[1929] Siehe ausführlich dazu *Gausling* 2010, 55 ff.; dazu auch *Zöller*, GA 2007, 392 ff., 405 f.; *Hornung*, MMR 2007, XIII.

[1930] So wurde etwa die in § 113a Abs. 3 TKG a.F. gebrauchte Wendung „Anbieter von Diensten der elektronischen Post" kritisiert, da sie nicht im TKG legal definiert ist und somit schon in sich zu unbestimmt, *Szuba* 2011, 136. Auch in Bezug auf die Formulierung, wer „öffentlich" Telekommunikationsdienste anbietet, war umstritten, ob etwa Arbeitgeber oder auch Universitäten zur Speicherung verpflichtet waren, *Grimm/Michaelis*, Der Betrieb 2009, 174; *Feldmann*, NZA 2008, 1398

[1931] Vgl. dazu schon oben S. 88.

[1932] Vgl. dazu oben S. 312 ff.

[1933] Vgl. dazu oben S. 316 f.

nichtig erklärten Regelungen nur die Dienstanbieter, die gegenüber dem Endkunden Dienste erbringen, zur Speicherung verpflichtet.

Verlangt wird jedenfalls dass sich eine Regelung entweder darauf beschränkt, entweder nur die Betreiber, die dem Endkunden Dienste erbringen, zu verpflichten oder allein die Netzbetreiber, die Daten, die sie als Host für die Telekommunikationsanbieter als ihre Kunden erheben, zur Speicherung zu verpflichten. Ansonsten würden Datensätze doppelt gespeichert werden.

Insofern ist aber zumindest in Bezug auf die Kommunikation über das Internet die Verpflichtung nur der Netzbetreiber eine denkbare Alternative, da auch bei diesen Informationen über die Kommunikation des Endkunden im Netz anfallen.[1934] Letztlich könnten so zwar nicht sämtliche Telekommunikationsverbindungen rekonstruiert werden, andererseits könnte auf diese Weise aber ein hoher Sicherheitsstandard garantiert werden. Denn es handelt sich überwiegend um sehr große Anbieter, die problemlos auch sehr hohe Sicherheitsvorkehrungen umsetzen können. Auch kann bei der Konzentration der Speicherungsverpflichtung auf nur wenige Netzbetreiber die Einhaltung der Datensicherheitsmaßnahmen überprüft werden. Verfassungsrechtlich gefordert ist jedenfalls eine bestimmte und normenklare Regelung.

Auch und gerade unter diesem Gesichtspunkt liegt es nahe die Adressaten nicht abstrakt zu bestimmen, sondern die Auswahl und Bestimmung der Adressaten jeweils durch Verwaltungsakt zu konkretisieren. So könnte sichergestellt werden, dass Rechtsklarheit herrscht, wer zur Vorratsdatenspeicherung verpflichtet ist. Zudem könnte durch die Übertragung der Auswahl der Adressaten auf eine zentrale Behörde, etwa die *Bundesnetzagentur,* die über erforderliches Wissen und Kenntnisse über die Netzstruktur in der Bundesrepublik verfügt, auch gewährleistet werden, dass bei der Auswahl der Adressaten der Grundsatz der Datensparsamkeit berücksichtigt wird und zugleich Sorge getragen wird, dass tatsächlich möglichst umfassend die Verkehrsdaten gespeichert werden. Diese könnte bei der Auswahl ebenfalls das Erdrosslungsverbot berücksichtigen.

Insbesondere in Bezug auf Anonymisierungsdienstanbieter und reine Geschäftskundenanbieter stellt sich die Frage, ob diese nicht von einer Speicherungsverpflichten auszunehmen sind. Da die Bedeutung dieser Daten für die Arbeit der Ermittlungsbehörden besonders gering ist. Auch ist eine Ausnahme von Kleinst- und Kleinanbietern von der Speicherungsverpflichtung zu erwägen.

10.1.3.1 Anbieter von Anonymisierungsdiensten

Die deutsche Regelung verpflichtete auch Anonymisierungsdienste.[1935] Die Richtlinie selbst sieht hingegen keine derartige Verpflichtung vor. Faktisch führt eine Verpflichtung zur Vorratsdatenspeicherung von Anonymisierungsdienstleistern überwiegend ins Leere.[1936] Denn hier wird den Nutzern eine private IP-Adresse zugewiesen, während

[1934] Vgl. oben S. 31.
[1935] Ausführlich dazu *Gausling* 2010, 78 ff.
[1936] *Gausling* 2010, 84; *Szuba* 2011, 136, 138 ff.

die Verbindung ins Internet über ein von mehreren Benutzern genutztes NAT oder eine öffentliche IP-Adresse des Anonymisierungsdienstes erfolgt.[1937] Ermöglicht wird bei einer Vorratsdatenspeicherung jeweils eine Rückverfolgung bis zum letzten Server einer Mixkaskade bzw. zum letzten einer Kette eines Tor-Servers. Eine Zuordnung einer einzelnen Aktivität zu einer bestimmten IP-Adresse scheidet hingegen vielfach aus.[1938] Jedenfalls solange nicht die Betreiber sämtliche Mixe einer Kaskade oder alle Server einer Tor-Route auf Vorrat speichern. Sobald bereits ein Betreiber nicht speichert, ist eine Deanonymisierung nicht mehr möglich. Zu beachten ist dabei, dass sobald ein Betreiber seinen Sitz im (außereuropäischen) Ausland hat – was häufig der Fall ist – dieser nicht zur Speicherung verpflichtet ist.[1939] Durch eine Ausnahme von Anonymisierungsdiensten von der Speicherungsverpflichtung werden zwar die Möglichkeiten die Vorratsdatenspeicherung zu umgehen erweitert, was unter sicherheitspolitischen Aspekten abzulehnen ist. Da jedoch letztlich der intelligente Straftäter auch die Vorratsdatenspeicherung umgehen kann (Nutzung ausländischer Provider, Internet-Cafés, Hot-Spots, Mobiles Internet) werden durch die Ausnahme von Anonymisierungsdienstleistern die Umgehungsmöglichkeiten nur geringfügig erweitert, insbesondere da vielfach auch trotz Speicherungsverpflichtung eine Reanonymisierung in den meisten Fällen ausscheiden dürfte. Eine Speicherungsverpflichtung von Anonymisierungsdienstanbieter ist im Ergebnis abzulehnen.

10.1.3.2 Geschäftskundenanbieter

Auch in Bezug auf reine Geschäftskundenanbieter (auch B2B-Betreiber) ist zu erwägen, ob diese nicht von einer Speicherungsverpflichtung ausgenommen werden sollten. Derartige Telekommunikationsanbieter verarbeiten zwar eine hohe Menge Verkehrsdaten, in aller Regel sind diese für die Bekämpfung und Verfolgung von internationalem Terrorismus, organisierter Kriminalität und Kinderpornographie aber nicht relevant. Sie werden nur in sehr wenigen Fällen abgerufen.

Die Auswahl, ob auch Geschäftskundenanbieter verpflichtet werden sollen, ist auch davon abhängig für welche (Straf-)Taten ein Zugriff auf die auf Vorrat gespeicherten Verkehrsdaten erlaubt werden soll. Sollte etwa ein Zugriff auch für Betrugsfälle und Wirtschafts- sowie Steuerdelikte ermöglicht werden, ist die Erforderlichkeit der Verpflichtung gegeben. Ansonsten kann die Erforderlichkeit der Verpflichtung in Frage gestellt werden.[1940] In diesem Fall spricht insbesondere der Grundsatz der Datensparsamkeit gegen eine Verpflichtung dieser Anbieter.

10.1.3.3 Kleinst- und Kleinanbieter

Zum Teil wird auch eine Ausnahme von Kleinst- und Kleinanbietern von der Speicherungsverpflichtung gefordert. Die hohen Anforderungen die zum Schutz der informationellen Selbstbestimmung bei einer neuen Umsetzung der Vorratsdatenspeicherung

---

[1937] Zur Funktionsweise von Anonymisierungsdiensten, oben Kap. 1.1.2.1.5, S. 29 f.

[1938] *Szuba* 2011, 136 ff.; vgl. zur technischen Funktionsweise *Hansen* 2003, 315; *Gietl*, K&R 2007, 545, 549.

[1939] Zahlreiche Knotenpunkte des Tor-Netzwerks befinden sich außerhalb des Geltungsbereichs des TKG, *Gausling* 2010, 84; dazu auch oben, S. 29.

[1940] *Knierim*, 2011b.

durch die Unternehmen zu beachten sind, führen zu einer deutlichen Steigerung des Aufwands und der Kosten. Insofern ist es wahrscheinlich, dass eine Neuregelung bei Kleinstanbietern erdrosselnd wirken würde und daher verfassungswidrig wäre.[1941] Zudem könnte bei einer kostenpflichtigen Verpflichtung von Klein- und Kleinstanbietern der Gleichheitssatz verletzt werden.[1942] Denn der Aufwand der Implementierung der Speicher- und Sicherheitsprozesse verursacht für kleine wie große Anbieter einen hohen finanziellen Aufwand, der sich nicht proportional zum Umsatz oder zur Größe eines Unternehmens verhält.[1943]

Durch eine Ausnahme von Klein- und Kleinstanbietern von der Verpflichtung zur Vorratsdatenspeicherung werden jedoch weitere Möglichkeiten, der Vorratsspeicherung von Verkehrsdaten zu entgehen, geschaffen. Dies birgt das Risiko, dass jedenfalls intelligente Straftäter zu kleinen Anbietern wechseln, die nicht von der Speicherungspflicht erfasst sind. In dieser Hinsicht erscheint eine vollständige Kostenerstattung die vorzugswürdige Alternative.

Eine generelle Ausnahme von Kleinst- und Kleinanbietern wäre dann geboten, wenn keine Kostenerstattung der Investitions- und Betriebskosten erfolgt. Soweit allerdings die Speicherung insgesamt auf wenige große Anbieter konzentriert wird und deren Auswahl durch die Bundenetzagentur erfolgt, ist weder eine grundsätzliche Ausnahme von Kleinstanbietern noch eine vollständige Kostenerstattung zwingend geboten.

10.1.3.4 Empfehlung

Empfohlen wird die Bestimmung der Adressaten auf die Bundesnetzagentur zu übertragen, die diese nach dem Grundsatz des „Cheapest Cost Avoider" auswählt und die Speicherungspflicht jeweils durch Verwaltungsakt begründet.

10.1.4 Speicherort

Die Richtlinie enthält keine Angaben über den Speicherort. Für das *Bundesverfassungsgericht* ist die Speicherung durch die Privaten „maßgeblich" für die Rechtfertigungsfähigkeit der Speicherungsverpflichtung.[1944] Grund dafür ist zum einen, dass so eine dezentrale Datensammlung entsteht, was das Missbrauchsrisiko senkt. Zum anderen soll dadurch das Gefühl des Überwachtwerdens verringert und Transparenz gefördert werden.[1945] In Betracht kommt daher grundsätzlich nur die Speicherung beim Anbieter. Dabei sind die Datenspeicher für die Vorratsdatenspeicherung getrennt von ihren operationalen Systemen zu halten.[1946]

Denkbar wäre darüber hinaus, dass die Anbieter die Speicherungsverpflichtung auf ein drittes Unternehmen auslagern. Dabei muss, um die Dezentralität der Speicherung zu

---

[1941] Vgl. oben S. 312 f.
[1942] Vgl. oben S. 316.
[1943] Vgl. oben S. 303.
[1944] BVerfGE 125, 260 (321); Treffend bezeichnen so *Eckhardt/ Schütze* die Speicherung durch die Privaten als „Schlüssel zur Zulässigkeit", CR 2010, 225, 227; vgl. dazu ausführlich oben S. 296.
[1945] BVerfGE 125, 260 (321 f.).
[1946] *Gausling* 2010, 144.

gewährleisten, verhindert werden, dass alle Verpflichteten die Speicherung auf ein einziges drittes Unternehmen übertragen und so letztlich doch eine zentrale Datenbank entsteht.[1947] Letztlich kann unter datenschutzrechtlichen Gesichtspunkten die Zulässigkeit der Auslagerung der Speicherungsverpflichtung auf einen Dritten insgesamt in Frage gestellt werden. Denn diese führt dazu, dass in aller Regel die Kontrollierbarkeit und die Organisationshoheit beschnitten und damit die Verfügbarkeit der Daten beeinträchtigt wird. Dies gilt umso mehr bei einer Speicherung im Ausland. Insofern ist für die Verpflichtung zur Vorratsdatenspeicherung zu erwägen, ob diese entgegen der allgemeinen datenschutzrechtlichen Regelungen, nicht auf einen anderen übertragen werden kann. Soweit die Kosten erstattet werden, ist es, um das Ziel einen besonders hohen Sicherheitsstandard zu erreichen, gerechtfertigt die Berufsfreiheit dahingehend einzuschränken indem die Datenverarbeitung allein innerhalb des jeweiligen Konzernverbundes für zulässig erklärt wird.[1948]

Nach dem Vorschlag, die Auswahl der Adressaten nach dem Grundsatz „Cheapest Cost Avoider" der Bundesnetzagentur zu übertragen, wird insgesamt nur eine geringe Anzahl an Unternehmen verpflichtet werden. Durch die Konzentration der Speicherung bei wenigen großen Anbietern wird zwar die Dezentralität verringert, jedoch kann so leichter ein hoher Sicherheitsstandard garantiert werden. In Anbetracht der empfohlenen vollen Kostenerstattung ist die Auslagerung der Speicherungsverpflichtung zu untersagen.

Empfohlen wird die Unternehmen durch Verwaltungsakt zu verpflichten die Vorratsdatenspeicherung im eigenen Konzern durchzuführen.

10.1.5 Datensicherheit

Der Sicherheit der Daten kommt zum einen eine hohe Bedeutung zu, um die informationelle Selbstbestimmung der betroffenen Bürger zu schützen,[1949] und zum anderen, da die Daten nur dann polizeilich verwerten werden können, wenn ihre Integrität gewährleistet ist. Für eine verhältnismäßige Ausgestaltung des Eingriffs in das Telekommunikationsgeheimnis sind spezielle Vorgaben zur Sicherung der Vorratsdaten zu

---

[1947] Soweit die Daten innerhalb der EU/EWR gespeichert werden sollen, ist § 11 BDSG anwendbar. Soweit die Daten außerhalb zu speichern wäre, ist § 4b BDSG anzuwenden, dazu *Spindler,* in: *Spindler/Schuster* 2011, § 11 BDSG, Rn. 14; Das BDSG geht davon aus, dass an eine Weitergabe zur Verarbeitung der Daten an einen Dritten keine grundlegend anderen Anforderungen zu stellen sind. Die Verantwortlichkeit und Verfügungsgewalt bleiben beim Auftraggeber. Im BDSG wird daher davon ausgegangen, dass auch bei einer Auftragsdatenverarbeitung ein gleichwertiger Datenschutz besteht. Dies gilt auch innerhalb der EU/EWR, dazu *Dammann*, in: *Simitis*, BDSG 2011, § 3 Rn. 246.

[1948] Insofern auch entgegen der Regelung zur Auftragsdatenverarbeitung in § 11 BDSG.

[1949] *Britz*, JA 2011, 81, 82 verweist darauf, dass durch die Sicherung der Daten gegen Missbrauch auch das das „diffus bedrohliche Gefühl des Beobachtetseins" verringert werden könne; in diesem Sinne auch die abweichende Meinung des Richters Schluckebier „Ist zudem das nach dem Stand der Technik mögliche angemessene Niveau der Datensicherheit gewährleistet, fehlt damit auch jede objektivierbare Grundlage für die Annahme eines eingriffsintensivierenden Einschüchterungseffekts oder eines - wie das Urteil formuliert - "Gefühls des ständigen Überwachtwerdens" und der "diffusen Bedrohlichkeit", BVerfGE 125, 260 (366).

treffen.[1950] Die Vorratsdatenspeicherungsrichtlinie gibt in Bezug auf Datenschutz und Datensicherheit lediglich in Art. 7 Mindestanforderungen vor sowie die Anforderung, dass eine regelmäßige und unabhängige Kontrolle der Datensicherheit vorgenommen werden muss.[1951]

Das *Bundesverfassungsgericht* führt aus, dass ein Standard an Datensicherheit garantiert werden müsse, „der unter spezifischer Berücksichtigung der Besonderheiten der durch eine vorsorgliche Telekommunikationsverkehrsdatenspeicherung geschaffenen Datenbestände ein besonders hohes Maß an Sicherheit gewährleistet".[1952] Dafür müsse eine Regelung getroffen werden, die sich zum einen am „Entwicklungsstand der Fachdiskussion" orientiert und „neue Erkenntnisse und Einsichten fortlaufend" aufnimmt. Zum anderen dürfe die Regelung nicht „unter dem Vorbehalt einer freien Abwägung mit allgemeinen wirtschaftlichen Gesichtspunkten" stehen.[1953] Das *Bundesverfassungsgericht* erwägt den Rückgriff auf die Rechtsfigur „Stand der Technik".[1954]

Stand der Technik, so ist es im Umweltrecht anerkannt, sind jene Techniken, Technologien und Produkte, die auch „grundsätzlich flächendeckend frei am Markt verfügbar".[1955] Die Berücksichtigung der Verhältnismäßigkeit zwischen Aufwand und Nutzen möglicher Maßnahmen ist dabei etwa für § 3 Abs. 6 BImSchG ausdrücklich im Anhang benannt, welcher die Kriterien zur Bestimmung des Stands der Technik auflistet. Die Kriterien der Verfügbarkeit und der wirtschaftlichen Vertretbarkeit führen dazu, dass auch bei der Ermittlung des Stands der Technik das Kosten-Nutzen-Verhältnis berücksichtigt werden muss.[1956] Der Begriff „Stand der Technik" ist jedoch von der „Regel der Technik" abzugrenzen, welches Kriterium in Energierecht ist.[1957] Regel der Technik ist im Gegensatz zum Stand der Technik, das was sich allgemein durchgesetzt hat. Insoweit ist der Begriff „Stand der Technik" enger: Es muss zwar auch grundsätzlich und allgemein auf dem Markt verfügbar sein, sowie der Einsatz im konkreten Fall verhältnismäßig sein, aber es muss der höchste allgemein verfügbare Standard gewählt werden. Geboten ist insofern die Orientierung an den aktuellen technischen Entwicklungen und nicht an dem, was bereits zum Regel der Technik, mithin zum Standard geworden ist.

[1950] *Roßnagel/Bedner/Knopp*, DUD 2009, 536, 538.

[1951] Art. 9 VDS-RL verlangt nach einer unabhängigen Kontrolle. Zur vollkommenen Unabhängigkeit des Datenschutzbeauftragten, dazu oben Fn. 867, S. 142; ausführlich zu den in der RL formulierten Anforderungen an die Datensicherheit, ebd.

[1952] BVerfGE 125, 260 (326).

[1953] BVerfGE 125, 260 (327).

[1954] BVerfGE 125, 260 (326).

[1955] *Müller-Kullmann,* in: *Danner/Theobald,* Energierecht 2012, § 5 EnEG Rn. 5; so auch für § 3 BImSchG *Schulte,* in: Beck-OK Umweltrecht 2012, § 3BImSchG Rn. 92 „Begrifflich wird das nach jeweiligem Entwicklungsstand technisch-praktisch realisierbare bezeichnet." Wobei die praktische Eignung auch eine wirtschaftliche Eignung im Rahmend es Verhältnismäßigkeitsgrundsatzes bedeutet. Geeignet sind demnach Maßnahmen nur dann, wenn ihr Ergebnis gegenüber dem wirtschaftlichen Aufwand vertretbar erscheint; so schon BT-Drs 7/179, 32; BVerwG NVwZ 2001, 1165.

[1956] *Breuer* 2011, 29.

[1957] *Müller-Kullmann,* in: *Danner/Theobald,* Energierecht 2012, § 5 EnEG Rn. 6.

Für die Vorratsdatenspeicherung ist von Bedeutung, dass die für den Stand der Technik einzuhaltenden technischen Vorgaben verbindlich konkretisiert werden. Systemkonform wäre es, die Bundesnetzagentur mit dieser Aufgabe zu betrauen. Das Bundesamt für Sicherheit in der Informationstechnik wäre bei Sachfragen miteinzubeziehen.

Vermutlich um zu verdeutlichen, dass ein besonders hoher Sicherheitsstandard tatsächlich besonders umfassende Maßnahmen erfordert, hat das Gericht in der Entscheidung zur Vorratsdatenspeicherung unter Verweis auf die sachverständigen Ausführungen besonders konkrete Angaben zur Datensicherheit gemacht.[1958] Erforderlich sei „eine getrennte Speicherung (…) auf auch physisch getrennten und vom Internet entkoppelten Rechnern, eine asymmetrische kryptografische Verschlüsselung unter getrennter Verwahrung der Schlüssel, die Vorgabe des Vier-Augen-Prinzips für den Zugriff auf die Daten verbunden mit fortschrittlichen Verfahren zur Authentifizierung für den Zugang zu den Schlüsseln, die revisionssichere Protokollierung des Zugriffs auf die Daten und deren Löschung sowie der Einsatz von automatisierten Fehlerkorrektur- und Plausibilitätsverfahren".[1959]

Die Bedeutung der Datensicherheit ist für den Interessenausgleich im Verhältnis *Staat − Bürger* hoch.[1960] Sie hat jedoch starke Rückwirkungen auf das Kollisionsverhältnis *Staat − Wirtschaft*. Im Wesentlichen sind es Aspekte der Datensicherheit, die die Höhe der Investitions- und Betriebskosten bestimmen. Der Gestaltungsspielraum des Gesetzgebers ist in Bezug auf die Datensicherheit auf Grund der verfassungsrechtlichen Anforderungen stark reduziert. Schließlich ist das Missbrauchsrisiko bei auf Vorrat gespeicherten Telekommunikationsverkehrsdaten besonders hoch:[1961]

Hintergrund eines Teils der Missbrauchsszenarien ist die Kommerzialisierung personenbezogener Daten. „Die Identität von Personen wird mehr und mehr zum Handelsgut".[1962] Die Telekommunikationsverkehrsdaten sind zudem von hoher Aussagekraft und daher von besonders hohem wirtschaftlichem Wert.[1963] Auch das *Bundesverfassungsgericht* erkennt, dass die „Gefahr eines illegalen Zugriffs auf die Daten groß" sei, denn „angesichts ihrer vielseitigen Aussagekraft können diese für verschiedenste Akteure attraktiv sein".[1964]

So ergeben sich Risiken zunächst aus der Speicherung unmittelbar bei den privaten Anbietern.[1965] Diese ist zwar verfassungsrechtlich geboten, damit die Daten auf viele Einzelunternehmen verteilt sind und dem Staat als Gesamtheit nicht unmittelbar zur Verfügung stehen,[1966] allerdings führt diese dezentrale Speicherung bei den Anbietern

[1958] BVerfGE 125, 260 (325 ff.).
[1959] BVerfGE 125, 260 (326).
[1960] Vgl. oben S. 274 f.
[1961] Vgl. dazu schon oben S. 184 f.
[1962] *Roßnagel* 2009, 100.
[1963] Vgl. dazu oben S. 184 f.
[1964] BVerfGE 125, 260 (325).
[1965] *Ziebearth* ist der Ansicht, dass es grundrechtsschonender wäre, wenn nicht die Anbieter selbst die Verkehrsdaten speichern würden aufgrund des dadurch entstehenden erheblichen Missbrauchsrisikos. Er erinnert an die Datenschutzskandale aus dem Jahr 2008, *Ziebarth*, DUD 2009, 25, 29.
[1966] BVerfGE 125, 260 (321).

zu einer Steigerung des Missbrauchsrisikos. Dieses besteht zunächst durch die Telekommunikationsdiensteanbieter selbst, die „grundsätzlich privatnützig" handeln und „nicht durch spezifische Amtspflichten gebunden" sind.[1967] Zum anderen bietet die Vielzahl der Speicherorte auch vielfältige Angriffspunkte. Ganz in diesem Sinne argumentiert das *Bundesverfassungsgericht:* „Schon angesichts der Anzahl der Speicherungsverpflichteten ist die Zahl derjenigen groß, die Zugriff auf solche Daten haben und haben müssen. Da die Speicherungspflicht kleinere Dienstanbieter mitbetrifft, stößt die Sicherung vor Missbrauch ungeachtet aller möglichen und erforderlichen Anstrengungen des Gesetzgebers auch in Blick auf deren Leistungsfähigkeit auf strukturelle Grenzen. Verstärkt wird dies dadurch, dass die Anforderungen an die Datenverwaltung und die Übermittlung der Daten an die Behörden ein hohes Maß an Technikbeherrschung sowie anspruchsvolle Software voraussetzen, womit sich zwangsläufig die Gefahr von Schwachstellen und das Risiko von Manipulationen durch interessierte Dritte verbinden."[1968] Außerdem bestehen, da die privaten Diensteanbieter „unter den Bedingungen von Wirtschaftlichkeit und Kostendruck handeln", „nur begrenzte Anreize zur Gewährleistung von Datensicherheit".[1969]

Der Ansatz der Konzentration der Speicherung auf wenige große Anbieter ermöglicht es diese Missbrauchsrisiken zu reduzieren. Dies gilt insbesondere da die Speicherung bei wenigen, besonders leistungsfähigen Speicherverpflichteten dazu führt, dass ein hoher Standard an Datensicherheit leichter umgesetzt und kontrolliert werden kann als bei einer Verpflichtung sämtlicher kleiner Dienstanbieter.

Durch die Übertragung der technischen Konkretisierung auf die Bundesnetzagentur kann sichergestellt werden, dass eine regelmäßige Überprüfung und Anpassung der sicherheitstechnischen Vorgaben erfolgt. Durch eine Zertifizierung technischer Lösungen könnte darüber hinaus Transparenz verstärkt und Rechtssicherheit für die speichernden Unternehmen erzeugt werden.

Im Einzelnen sind zur Gewährleistung eines besonders hohen Sicherheitsstandards erforderlich:

- Getrennte und vom Internet entkoppelte Speicherung

Die vom Billing-System getrennte und vom Internet entkoppelte Speicherung, um sicherzustellen, dass der Kreis der Zugriffsberechtigten auf die Vorratsdaten eng begrenzt wird. Die Entkoppelung vom Internet kann die Möglichkeiten des unberechtigten Zugriffs auf die Daten eindämmen. Durch die Trennung nach Dienst- oder Kommunikationsarten wird die Möglichkeit beschränkt, bei widerrechtlichem Zugriff auf die Daten umfassende Profile zu erstellen.[1970] Um Datenveränderungen zu erkennen, wird darüber hinaus der Einsatz kryptographisch sicherer Hashfunktionen empfohlen.[1971]

[1967] BVerfGE 125, 260 (325).
[1968] BVerfGE 125, 260 (320).
[1969] BVerfGE 125, 260 (325).
[1970] *Roßnagel/Bedner/Knopp*, DUD 2009, 536, 538.
[1971] *Pfitzmann/Köpsell*, DUD 2009, 542, 544.

- Anspruchsvolle Verschlüsselung der Daten bei Speicherung und Übermittlung

Mit Hilfe anspruchsvoller Verschlüsselungsverfahren kann die Integrität der Daten sichergestellt und ein Schutz vor Missbrauch erzeugt werden. Es sind sichere Algorithmen zu verwenden. Die dabei eingesetzte Hard- und Software sollte durch das Bundesamt für Sicherheit in der Informationstechnik oder die Datenschutzbeauftragten zertifiziert werden und regelmäßig im Hinblick auf die Sicherheit überprüft werden.[1972] Eine Verschlüsselung muss unmittelbar vor der ersten Speicherung auf einem Datenträger erfolgen. Es ist dabei sicherzustellen, dass die verwendeten Schlüssel so gespeichert werden, dass auf sie nur zum Zeitpunkt einer Auskunftserteilung nach geeigneter Authentifizierung zugegriffen werden kann und sie an einem physisch getrennten und besonders gesicherten Ort aufbewahrt werden.[1973]

- Fehlererkennungs- und Korrekturverfahren

Fehlererkennungs- und Fehlerkorrekturverfahren sind erforderlich, um die Wahrscheinlichkeit der Speicherung von Falschinformationen zu verringern.[1974] Denkbar ist insoweit zunächst eine syntaktische Prüfung der Vollständigkeit der Datenlieferungen über Sequenzzähler. Dadurch kann jedoch lediglich sichergestellt werden, dass die Datenzufuhr korrekt erfolgt ist. Darüber hinaus ist regelmäßig und automatisiert (zumindest stichprobenartig) zu überprüfen, ob Uhrzeiten stimmen, Kennungen so vergeben worden sein oder ob eine gespeicherte IP-Adresse zur zugewiesenen IP-Range gehört.[1975]

- Datenabruf

Durch die Möglichkeit, die Daten sortiert abzurufen, kann der Eingriff durch den Abruf auf das Erforderliche beschränkt werden.[1976] Eine falsche Wiedergabe von Nummern oder Uhrzeiten kann durch eine Verarbeitung bei der Ausgabe der Daten entstehen. Das Abrufverfahren muss sicherstellen, dass eine solche falsche Wiedergabe ausscheidet.[1977]
Neben diesen qualitätssichernden Vorkehrungen ist die Sicherheit des Datenabrufs durch ein hohes Authentifizierungsniveau zu gewährleisten.

- Datenzugang

Um den Kreis der Zugriffsberechtigten zu begrenzen und um den Schutz vor einer missbräuchlichen Nutzung zu erhöhen, ist die Anzahl der Mitarbeiter auf ein Minimum zu begrenzen. Die Auswahl sollte anhand von Zuverlässigkeitskriterien erfolgen.[1978] Diese sollten gemäß § 5 BDSG verpflichtet werden. Der Zugriff sollte nur er-

[1972] *Roßnagel/Bedner/Knopp*, DUD 2009, 536, 539.
[1973] *Pfitzmann/Köpsell*, DUD 2009, 542, 544 ff. Zur Speicherung der Schlüssel, sollten sog. „tamper resistant" Geräte verwendet werden, also solche, die im Fall eines Diebstahls zumindest einen gewissen Schutz bieten.
[1974] *Roßnagel/Bedner/Knopp*, DUD 2009, 536, 538; dazu auch *Szuba* 2011, 251.
[1975] *Roßnagel/Bedner/Knopp*, DUD 2009, 536, 538; *Szuba* 2011, 251.
[1976] *Roßnagel/Bedner/Knopp*, DUD 2009, 536, 538.
[1977] *Roßnagel/Bedner/Knopp*, DUD 2009, 536, 539.
[1978] *Roßnagel/Bedner/Knopp*, DUD 2009, 536, 540; *Szuba* 2011, 254.

möglicht werden, wenn mehrere Berechtigte zusammenwirken (Mehraugenprinzip). Dies kann mit der Verschlüsselung der Daten kombiniert werden.

- Kennzeichnung der Daten

Um die Herkunft der Daten erkennbar zu machen, damit sichergestellt wird, dass sie nur zu den gesetzlich vorgesehenen Zwecken verwendet werden, ist eine Kennzeichnung der Daten als Vorratsdaten erforderlich.[1979] Organisatorisch sollte die Kennzeichnung idealerweise schon vor der Übermittlung der Daten an die ersuchenden Behörden erfolgen. Außer der Kennzeichnung als Vorratsdaten sollte sie auch Angaben über die ersuchende Stelle, die verantwortliche Person, einen Verweis auf die richterliche Anordnung und den Zeitpunkt der Übermittlung enthalten.[1980] Die Kennzeichnung sollte soweit möglich der Daten untrennbar mit dem beauskunfteten Datum verknüpft werden.[1981]

- Kontrolle und Sanktionen

Die Wahrung der rechtlichen Anforderungen in Bezug auf die Datensicherheit muss auch in der Praxis sichergestellt werden. Dies kann durch Kontrolle und Sanktionen im Fall der Verletzung der Anforderungen zur Datensicherheit gewährleistet werden.
Die Kontrolle der Datensicherheitsstandards muss nach den Vorgaben der Richtlinie in Art. 8 Abs. 2 durch vollkommen unabhängige Behörden erfolgen.

Das *Bundesverfassungsgericht* führt aus, dass verfassungsrechtlich geboten „eine für die Öffentlichkeit transparente Kontrolle unter Einbeziehung des unabhängigen Datenschutzbeauftragten" ist.[1982] Die Unabhängigkeit der Datenschutzbeauftragten in der Bundesrepublik hatte der *Europäische Gerichtshof* in einem Urteil vom 9. März 2010 beanstandet.[1983]

Wichtig ist, damit die Kontrolle effektiv gestaltet werden kann, dass die mit dieser Aufgabe zu betrauenden Datenschutzbeauftragten nicht nur vollkommen unabhängig die Kontrollen durchführen, sondern auch tatsächlich so ausgestattet sind, dass sie die ihr übertragene Aufgabe wahrnehmen können. Wesentlich dafür ist, dass sie zur Erfüllung dieser Aufgaben über ausreichend Personal und Mittel verfügen, damit unter anderem regelmäßig Vor-Ort-Kontrollen durchgeführt werden können.

Die Kontrollierbarkeit wird zudem durch Informationspflichten verstärkt. Sollten die Anbieter Datensicherheitsanforderungen verletzen oder sollte ein Missbrauch festge-

---

[1979] *Jarass,* in: *Jarass/Pieroth,* GG 2011, Art. 10 Rn. 19; Auch gemäß § 101 Abs. 3 StPO sind die im Rahmen von verdeckten Ermittlungsmaßnahmen erlangten Daten besonders zu kennzeichnen.

[1980] *Roßnagel/Bedner/Knopp*, DUD 2009, 536, 539.

[1981] Denkbar wären hier eventuell digitale Wasserzeichen. Dies würde allerdings zu einer starken Beeinträchtigung des Work-Flows führen; dazu *Knierim* 2011a.

[1982] BVerfGE 125, 260 (327)

[1983] C 518/07 Kommission./.Deutschland; vgl. dazu auch schon oben Fn. 867; Für die Gewährleistung einer vollständig unabhängigen Prüfung besteht entsprechend des Judikats des *Europäischen Gerichtshofs* in Bezug auf die Unabhängigkeit des Bundesdatenschutzbeauftragten Nachbesserungsbedarf. Dieses wurde etwa im Antrag der Fraktion Bündnis 90/die Grünen v. 29.6.2011 gefordert, BT Drs. 17/6345.

stellt werden, muss der Dienstanbieter die betreffenden Kunden darüber informieren.[1984] Das *Bundesverfassungsgericht* fordert darüber hinaus „ein ausgeglichenes Sanktionensystem, das auch Verstößen gegen die Datensicherheit ein angemessenes Gewicht beimisst".[1985]

Es wird empfohlen die Anforderungen an die technischen Sicherheitsvorkehrungen klar und bestimmt vorzugeben, wobei sich der technische Sicherheitsstandard am Stand der Technik zu orientieren hat. Die Anforderungen sollten in technischen Richtlinien von der Bundesnetzagentur konkretisiert werden. Eine Prüfung und ggf. Anpassung im Hinblick auf aktuelle technische Entwicklungen sollte mindestens einmal im Kalenderjahr erfolgen.

10.1.6 Kostentragung

Die RL 2006/24/EG sieht keine Kostenerstattung vor. Auch die Regelung § 113a TKG i. V. m. § 110 Abs. 1 S. 1 Nr. 1 TKG (a.F.) sah keine Erstattung der Investitionskosten vor. Lediglich Abrufkosten wurden erstattet.[1986] Das *Bundesverfassungsgericht* hat dies im Urteil vom 2.3.2010 nicht beanstandet.[1987] Es sprechen jedoch zahlreiche gute Argumente gegen eine Kostenübertragung.[1988]

Bei dem Element der Kostentragung handelt es sich um ein zentrales Element für den Interessenausgleich primär in der Dimension Staat − Wirtschaft. Er ist jedoch auch für den Ausgleich in der Dimension Staat − Bürger von Bedeutung. Denn einerseits werden die Telekommunikationsunternehmen bei der Datenspeicherung die Auswahl der Sicherheitstechnologien auch daran ausrichten, ob sie selbst dafür aufkommen müssen oder ob sie die Kosten ersetzt bekommen. Andererseits kann auch das Abfrageverhalten der Behörden und damit die Datenverwendung beeinflusst werden, wenn dafür hohe Kosten anfallen.

Eine Neuregelung zur Vorratsdatenspeicherung wird aufgrund der hohen sicherheitstechnischen Anforderungen deutlich höhere Investitions- und Betriebskosten verursachen, als die in den Jahren 2008 bis 2010 bestehende Pflicht zur Vorratsspeicherung.[1989]

Um eine hohen Standard an Datensicherheit zu gewährleisten, aber auch um Wettbewerbsverzerrungen und eine Ungleichbehandlung[1990] der einzelnen Verpflichteten zu verhindern, sollten grundsätzlich sämtliche Investitions-, Betriebs-, und Abrufkosten

---

[1984] Vgl. § 42a BDSG.
[1985] BVerfGE 125, 260 (327); Welche Anforderungen im Einzelnen an ein ausgeglichenes Sanktionssystem zu stellen sind, wird im Folgenden auf S. 370 f. dezidiert erörtert.
[1986] § 23 Abs. 1 S. 1 Nr. 2 JVEG Erstattung bei Auskunftsanordnungen von Strafverfolgungsbehörden); gem. § 20 G10 beim Abruf durch Nachrichtendienste. Der hiernach mögliche Aufwendungsersatz erstreckte sich allein auf die Abrufkosten und nicht auf Betriebs- und Investitionskosten.
[1987] BVerfGE 125, 260 (360 ff.); geklagt hatte im Verfahren 1 BvR 256/08 eine Anonymisierungsdienstleisterin.
[1988] Vgl. dazu oben S. 292.
[1989] Vgl. oben S. 302.
[1990] Vgl. zum Gleichheitssatz, oben S. 316.

ersetzt werden. Auch ist eine Kostentragung auf Grund des Prinzips der Steuerstaatlichkeit und des Prinzips der staatsbürgerlichen Lastengleichheit geboten.[1991]

Lediglich zu einem kleinen Anteil sollten die Anbieter an den Kosten beteiligt werden, um deren Sparinteresse zu motivieren und so unnötig hohe Kosten zu verhindern. Dieses kann auch auf Grund der Sozialpflichtigkeit des Eigentums gerechtfertigt werden.[1992]

Auch unter dem Aspekt der Harmonisierung, die mit der Vorratsdatenspeicherungsrichtlinie verfolgt wird, ist kritisch zu hinterfragen, ob nicht in der Richtlinie eine einheitliche Regelung zur Kostenerstattung zu treffen ist, um dieses Ziel zu erreichen.

Empfohlen wird den verpflichteten Anbietern 80 Prozent der entstehenden Kosten zu ersetzen.

10.1.7 Schutz von Vertrauensbeziehungen

Ein Schutz von Vertrauensbeziehungen ist in der Vorratsdatenspeicherungsrichtlinie nicht vorgesehen. Sie steht einer solchen Regelung aber auch nicht entgegen. Die im Jahr 2010 für nichtig erklärten deutschen Regelungen sahen keinen ausdrücklichen Schutz vor. Das Grundgesetz verlangt jedoch einen besonderen Schutz von Vertrauensbeziehungen.[1993] In der StPO wird ein Schutz von Vertrauensbeziehungen durch das strikte Verbot von Ermittlungen gegenüber Geistlichen (über das, was ihnen in ihrer Eigenschaft als Seelsorger anvertraut worden oder bekanntgeworden ist), Strafverteidigern (in Bezug auf das, was ihnen in dieser Eigenschaft anvertraut worden oder bekanntgeworden ist) und Mitgliedern des Deutschen Bundestages, der Bundesversammlung, des Europäischen Parlaments aus der Bundesrepublik Deutschland oder eines Landtages (über Personen, die ihnen in ihrer Eigenschaft als Mitglieder dieser Organe oder denen sie in dieser Eigenschaft Tatsachen anvertraut haben, sowie über diese Tatsachen selbst) durch § 160a Abs. 1 S. 1 StPO[1994] garantiert. Gemäß Abs. 1 S. 2 StPO dürfen dennoch erlangte Erkenntnisse nicht verwertet werden. Zu beachten ist, dass dies nur für die Strafverfolgung gilt, also nicht für die Gefahrenabwehr und nicht für die Geheimdienste.

Für andere Geheimnisträger wie Rechtsanwälte, Steuerberater, Ärzte, psychologische Psychotherapeuten, Mitglieder von Schwangerschaftsberatungsstellen, Mitarbeiter von Suchtberatungsstellen sowie Journalisten gilt gemäß § 160a Abs. 2 StPO kein striktes Ermittlungs- und Verwertungsverbot in Bezug auf in ihrer Funktion erlangtes Wissen. Das Gesetz verlangt in § 160 Abs. 2 S. 1 StPO lediglich, dass die Eigenschaft als Geheimnisträger im Rahmen der Verhältnismäßigkeitsprüfung besonders berücksichtigt wird. Ein überwiegendes Strafverfolgungsinteresse verlangt in der Regel zumindest, dass das Verfahren eine Straftat von erheblicher Bedeutung betrifft.[1995] Satz 2 gebietet,

---

[1991] Dazu oben S. 299.
[1992] Dazu schon oben S. 306.
[1993] Dazu oben Kap. 9.1.2.4, S. 289.
[1994] § 160a eingef. durch Gesetz v. 21.12.2007 (BGBl. 2007 I, 3198); Abs. 1 S. 1 u. 5 neu eingef. durch Gesetz v. 22.12.2010 (BGBl. 2010 I, 2261).
[1995] § 160a Abs. 2 S. 1 StPO.

dass die „Maßnahme zu unterlassen oder, soweit dies nach der Art der Maßnahme möglich ist, zu beschränken“ ist.

Bei der Verpflichtung zur Vorratsdatenspeicherung handelt es sich noch um keine Ermittlungsmaßnahme. Es handelt sich vielmehr um eine für den eventuellen Fall zukünftiger Ermittlungen getroffene Regelung. Insofern gilt § 160a StPO nicht bereits für die Speicherungsverpflichtung, sondern findet erst im Fall einer Anfrage oder der Übermittlung der Daten Anwendung. Das hieße, Verkehrsdaten, die Informationen über das Vertrauensverhältnis zu Seelsorgern, Strafverteidigern und Mandatsträgern enthalten, dürfen gemäß § 160a Abs. 1 StPO grundsätzlich nicht übermittelt werden, während die Frage, ob Informationen in Bezug auf das Vertrauensverhältnis zu anderen Berufsgeheimnisträgern, wie Psychotherapeuten, Ärzten oder Journalisten, übermittelt werden dürfen, einer Abwägung zugänglich wären.

Dies genügt nicht dem für eine Datenspeicherung und nachfolgende Abfragen verfassungsrechtlich gebotenen Schutz von Vertrauensbeziehungen.[1996]

Es gibt heute einen großen Anteil der Seelsorgeberatung, aber auch der Drogen- und Suchtberatung, die über Telefon und Internet erfolgen. Auch Journalisten kommunizieren mit ihren Informanten über moderne Kommunikationsmittel und sind dabei besonders auf die Wahrung der Anonymität der Informanten angewiesen.[1997] Aus diesen Gründen ist jedenfalls für sämtliche in § 53 Abs. 1 StPO benannten Geheimnisträger ein striktes Übermittlungsverbot der Daten zu fordern.

Das *Bundesverfassungsgericht* erwägt ein Übermittlungsverbot für „Verbindungen zu Anschlüssen von Personen, Behörden und Organisationen in sozialen oder kirchlichen Bereichen, die grundsätzlich anonym bleibenden Anrufern ganz oder überwiegend telefonische Beratung in seelischen oder sozialen Notlagen anbieten und die selbst oder deren Mitarbeiter insoweit anderen Verschwiegenheitsverpflichtungen unterliegen“.[1998] Jedoch kann allein ein striktes Übermittlungsverbot nicht die einschüchternde Wirkung der Vorratsdatenspeicherung verhindern. Aufgrund des Charakters der Vorratsdatenspeicherung als gesamtgesellschaftliches Überwachungsinstrument ist daher ein vollumfänglicher Schutz der Vertrauensbeziehungen zu Berufsgeheimnisträgern verfassungsrechtlich zwingend erforderlich.

Dies ist auch geboten, da es sich bei Daten, die Informationen über die Kommunikation mit Berufsgeheimnisträgern enthalten, nicht lediglich um Verkehrsdaten handelt, sondern diese Daten in der Regel eine inhaltliche Aussage in sich tragen und daher auch auf Grund des Verbots der Speicherung von Inhaltsdaten nicht zu speichern sind.[1999]

Fraglich ist wie die Ausnahme von der Speicherungsverpflichtung realisiert werden kann. Denkbar ist den Schutz von Vertrauensbeziehungen in einem dreistufigen Verfahren sicherzustellen:

[1996] Vgl. zu diesem oben S. 288.
[1997] Dazu oben S. 292 f.
[1998] BVerfGE 125, 260 (334); vgl. § 99 Abs. 2 TKG.
[1999] Vgl. dazu oben S. 290.

Erste Stufe: Ausnahme von der Speicherung
Ähnlich wie beim Schutz von Kernbereichsdaten bei der Wohnraumüberwachung[2000] sollte auf der ersten Stufe soweit möglich die Speicherung der Daten ausgeschlossen werden. Diejenigen Kennungen, die einem Berufsgeheimnisträger zuzuordnen sind, wären von der Speicherungsverpflichtung auszunehmen. Denkbar ist etwa, dass Geheimnisträger ihre Kennung beim jeweiligen Anbieter auf eine Sperrliste setzen lassen, wie es auch in § 99 Abs. 2 TKG für Anbieter anonymer Seelsorgeleistungen sowie der in § 203 Abs. 1 Nr. 4, 4a StPO benannten Geheimnisträger vorgesehen ist.
Allerdings kollidiert die Übertragung dieser Aufgaben mit der Berufsfreiheit der Telekommunikationsdiensteanbieter. Die Verwaltung von Listen und der Abgleich dieser sowie die Implementierung von Löschalgorithmen sind unternehmensfremde Aufgaben, die bereits die Rechtfertigungsfähigkeit der Indienstnahme in Frage stellen.[2001] Zudem entstehen so bei den Anbietern höchst sensitive Listen über statische IP-Adressen, Telefonnummer und Mailadressen von Geheimnisträgern. Auch diese Listen sind missbrauchsgefährdet.

Zur Wahrung eines hohen Sicherheitsstandards und einer vertrauenswürdigen Verwaltung der Listen von Berufsgeheimnisträgern, sowie um die Telekommunikationsanbieter zu entlasten, sollte nicht das jeweilige private Telekommunikationsunternehmen mit der Verwaltung der Listen betraut werden, sondern eine staatliche Behörde. Dies gilt auch, um die erforderliche Geheimhaltung sicherzustellen. Denkbar wäre, dass Berufsgeheimnisträger mit einem amtlichen Nachweis über ihre Eigenschaft als Geheimnisträger (zum Beispiel von der zuständigen Berufskammer) eine Ausnahme von der Vorratsdatenspeicherung bei der Bundesnetzagentur beantragen, ähnlich wie im Rahmen des Verfahrens nach § 99 TKG. Hier führt die Bundesnetzagentur eine Liste auf die Geheimnisträger, wenn sie sich mit einem Nachweis über ihre Eigenschaft als Geheimnisträger registriert haben, auf Antrag gesetzt werden. Die Liste mit den Anschlussnummern wird zum Abruf im automatisierten Verfahren bereitgestellt. Telekommunikationsanbieter sind verpflichtet die Liste alle drei Monate abzurufen und ihr Abrechnungssystem entsprechend anzupassen.

Eine Schwierigkeit besteht in technischer Hinsicht bei der Filterung von Kennungen auf Grund der Tatsache, dass dies für die Kommunikation im Internet nur funktioniert, soweit der Berufsgeheimnisträger über eine statische IP-Adresse verfügt.

Zweite Stufe: Filterung/Übermittlungsverbot
Soweit möglich muss die Auskunftserteilung für alle die Fälle unterbunden werden, in denen sich die Tatsache, dass es sich um ein besonders geschütztes Vertrauensverhältnis handelt, erst im Zeitpunkt der Anfrage herausstellt.[2002] Da es sich bei der Filterung um eine unternehmensfremde Aufgabe handelt, deren Übertragung auf die Telekommunikationsanbieter den Eingriff in die Berufsfreiheit deutlich vertiefen würde, wäre

[2000] § 100c Abs. 4 bis 7 StPO.
[2001] Vgl. oben S. 307.
[2002] In diesem Sinne fordert auch das *Bundesverfassungsgericht*, dass „bei der Datenübermittlung Filter zwischengeschaltet werden, mit denen bestimmte Telekommunikationsverbindungen zum Schutz von besonderen Vertrauensbeziehungen ausgesondert werden“, BVerfGE 125, 260 (334).

die Filteraufgabe in erster Linie durch die anfragenden Stellen durchzuführen. Die Schwierigkeit besteht hier allerdings darin, dass sie zumindest für den Bereich dynamischer IP-Adressen nicht über das erforderliche Wissen verfügen, um die Filterung ohne Mitwirkung der Telekommunikationsanbieter durchzuführen. Es müssen insofern für die Filterung sowohl Telekommunikationsunternehmen als auch ersuchende Behörden aktiv werden.

Dritte Stufe: Beweisverwertungsverbot
Soweit sich erst nach der Übermittlung an staatliche Stellen herausstellt, dass es sich um Daten handelt, die Aufschluss über verfassungsrechtlich geschützte Vertrauensbeziehung geben, dürften die Daten nicht verwertet werden. Es greift insofern auf der dritten Ebene ein Beweisverwertungsverbot, wie es auch in § 160a Abs. 1 StPO normiert ist.[2003]

Eine solche dreistufige Lösung, ist derzeit der einzig ersichtliche Ansatz, um den verfassungsrechtlichen Anforderungen zu genügen und im Rahmen einer bestehenden Verpflichtung zur Einführung einer Vorratsdatenspeicherung den Interessenausgleich möglichst zu optimieren. Sie bringt aber neue erhebliche Risiken mit sich und bedeutet einen schweren Eingriff in die Berufsfreiheit der Telekommunikationsanbieter.

Eine solche Lösung ist insofern zwar ein mögliches Konzept, es ist aber keinesfalls eine ideale Lösung. Vertrauensbeziehungen sind durch eine Verpflichtung zur Vorratsdatenspeicherung stark gefährdet, selbst dann wenn durch ein dreistufiges Verfahren ein minimaler Schutz gewährleistet wird. Letztlich ist auch bei einer dreistufigen Lösung kein umfassender Schutz von Vertrauensbeziehungen möglich. In Anbetracht der betroffenen hohen Verfassungsgüter[2004] spricht dies grundsätzlich gegen die Einführung einer Vorratsspeicherung der Telekommunikationsverkehrsdaten.

Solange und soweit allerdings europarechtlich die Verpflichtung zur Einführung einer Vorratsdatenspeicherung besteht, ist im Interesse eines optimierten Interessenausgleichs der Schutz von Vertrauensbeziehungen durch ein dreistufiges Verfahren, wie es hier vorgeschlagen wurde, zu gewähren.

10.1.8 Datenübermittlung

Der Zugang zu den auf Vorrat gespeicherten Verkehrsdaten ist in der Vorratsdatenspeicherungsrichtlinie nicht ausdrücklich geregelt. Art. 4 bestimmt allein, dass die Mitgliedstaaten, Maßnahmen erlassen müssen, um sicherzustellen, „dass die auf Vorrat gespeicherten Daten nur in bestimmten Fällen und in Übereinstimmung mit dem innerstaatlichen Recht an die zuständigen Behörden“ weitergegeben werden. Die Regelung des Verfahrens und der Bedingungen des Zugangs zu den Daten wird insofern den Mitgliedsaaten überlassen.

[2003] Mit dem Unterschied, dass es sich nicht auf den Schutz von den in § 53 Abs. 1 S. 1 Nr. 1, 2 oder Nr. 4 genannten Personen beschränken dürfte.

[2004] Zur verfassungsrechtlichen Grundlage des Schutzes von Vertrauensbeziehungen, ausführlich oben S. 289 ff.

Aus verfassungsrechtlicher Sicht ist zu beachten, dass nicht nur die Speicherungsverpflichtung, sondern auch die Übermittlung der Daten in das Telekommunikationsgeheimnis eingreift.[2005] Es ist insofern auch bei den Regelungen zur Datenübermittlung, das Telekommunikationsgeheimnis und die informationelle Selbstbestimmung der Nutzer zu beachten.

Verfassungsrechtlich gefordert ist, dass die auf Vorrat gespeicherten Daten „dem Staat unmittelbar als Gesamtheit nicht zur Verfügung" stehen. [2006]

Die Regelung in § 113 Abs. 9 i. V. m. § 113b TKG a.F. sah allein eine Übermittlung als manuelle Auskunft nach § 113 TKG vor. Dieser Ansatz, dass staatlichen Behörde keinen unmittelbaren Zugriff auf die Daten zu gewähren, genügt der verfassungsrechtlich geforderten strukturellen Trennung zwischen Erhebung und Verwertung.[2007]

Das Potential, das Daten missbräuchlich genutzt werden, sowie das Risiko der Verfälschung der Daten auf dem Übermittlungsweg sind sehr hoch. Dies droht insbesondere, solange die Übermittlung auf vielfältige und vor allem höchst unsichere Wege verteilt ist (unverschlüsselte Daten-CD oder E-Mail, per Fax oder Post). Eine solche ist daher strikt zu verbieten.[2008]

Auch muss sichergestellt werden, dass die Daten den korrekten Empfänger erreichen und auf dem Weg dorthin weder geöffnet noch verändert werden können. Erforderlich ist insoweit zunächst eine eindeutige Authentifizierung der anfordernden Stelle. Für die Datenübermittlung ist sodann ein besonders hoher Sicherheitsstandard zu fordern.[2009] Denkbar wäre allein eine elektronische Übermittlung zuzulassen, da auf diesem Wege letztlich sehr hohe Sicherheitsstandards realisiert werden können.

Die Übermittlung von auf Vorrat gespeicherten Verkehrsdaten zwischen Telekommunikationsdiensteanbietern und ersuchenden Behörden könnte gänzlich über die „Elektronische Schnittstelle Behörden" (ESB) erfolgen. Diese wurde entwickelt, u. a. um das gesamte Verfahren zur Beantragung und Ausleitung von Verkehrsdaten voll elektronisch zu gewährleisten, es insgesamt zu vereinfachen und zu beschleunigen. Eingeführt werden soll die ESB laut eines Beschlusses der Innenminister der Länder vom 17. November 2006. Es fehlt aber bislang an einer entsprechenden verbindlichen Normierung.[2010] Sollte die ESB verbindlich eingeführt werden, ist dies grundsätzlich

---

[2005] BVerfGE 125, 260 (310).

[2006] BVerfGE 125, 260 (321); „Die Trennung von Speicherung und Abruf fördert strukturell zugleich die – durch gesetzliche Ausgestaltung näher zu gewährleistende – Transparenz und Kontrolle der Datenverwendung".

[2007] Eine Vorratsspeicherung in einer zentralen staatlichen Datensammlung wäre nicht mit dem Gedanken einer freiheitlich demokratischen Grundordnung zu vereinen, vgl. dazu oben S. 276.

[2008] *Szuba* 2011, 254.

[2009] BVerfGE 125, 260 (325); dazu auch *Gausling* 2010, 144 ff.; dies ist gem. § 110 Abs. 3 TKG Aufgabe der Bundesnetzagentur, internationale Standards werden durch die ETSI vorgegeben. Vgl. dazu auch schon oben S. 277 .

[2010] *Wirth* (LKA Bayern), Stellungnahme zum Gesetzentwurf zur Neuregelung der TKÜ, v. 22.8.2007, abrufbar unter: http://www.gesmat.bundesgerichtshof.de/gesetzesmaterialien/16_wp/telekueberw/stellung_ra_wirth_at.pdf.

in Bezug auf eine verkürzte Übermittlungszeit aus sicherheitsrechtlicher Perspektive zu begrüßen. Soweit für die ESB hohe technische und organisatorische Sicherheitsvorkehrungen vorgesehen sind, ist dies auch unter dem Gesichtspunkt informationeller Selbstbestimmung zu begrüßen.

Damit Auskunftsersuchen und Antworten sicher, schnell und den gesetzlichen Anforderungen entsprechend übermittelt werden, bietet es sich an, das Verfahren zu zentralisieren. Dafür müsste die ersuchende Behörde jeweils ihre Anfrage an eine zentrale Stelle übermitteln, die sie dann an das betreffende Unternehmen richtet. Auch wenn dies als Umweg erscheint, könnte so in der Praxis das Verfahren schneller werden, da die Informationen über zuständige Ansprechpartner bereits gebündelt bei einer Behörde vorlägen und nicht durch jede Behörde neu recherchiert werden müssten. Wichtig ist in diesem Zusammenhang auch, dass es in jedem Unternehmen eine allein und ausdrücklich zuständige Stelle gibt, die für die Bearbeitung der Anfragen zuständig ist.

Vom Unternehmen werden die angeforderten Verkehrsdaten, nachdem sie aus dem Gesamtdatenbestand herausgefiltert wurden, auf demselben Kommunikationsweg, idealerweise über die ESB, übertragen. Dieses Modell ermöglicht es, hohe Datensicherheitsstandards bei der Übertragung der Daten mit vertretbarem Kostenaufwand zu realisieren. Auch ist es aus Perspektive der Telekommunikationsanbieter zu begrüßen, da sie nicht mit einer Vielzahl von Polizeibehörden zur Abwicklung der Anfragen konfrontiert sind, sondern mit einer eindeutig benannten Stelle kommunizieren.[2011]

Zudem könnte auf diese Weise gewährleistet werden, dass die Auskunftsbegehren zentral registriert und (automatisch) statistisch erfasst werden. So könnte erhoben werden, wie häufig auf die Daten zugegriffen wird. Dies ist zur Wahrung der freiheitlich demokratischen Grundordnung und Verhinderung eines Verstoßes gegen das Verbot umfassender gesamtgesellschaftlicher Überwachung erforderlich.[2012]

Bei der Ausgestaltung der organisatorischen Regelungen des Abrufs muss berücksichtigt werden, dass zum Abruf grundsätzlich die jeweiligen Polizeistellen zuständig sind. Für die Strafverfolgung kann hier eine bundeseinheitliche Regelung zum Verfahren für den Zugriff auf die Daten getroffen werden. Für die Gefahrenabwehr ist zwar grundsätzlich das gleiche Vorgehen zu empfehlen, dazu bedarf es aber einer Vereinbarung zwischen den Ländern. Eine Zentralisierung der Abfrage widerspricht insofern der Aufgliederung Deutschlands als föderalistisches System.[2013] Für eine Zentralisierung der Abfrage im Bereich der Gefahrenabwehr wäre insofern eine zwischenstaatliche Vereinbarung erforderlich. Die Zentralisierung des Abrufs wäre aber sowohl für die Gefahrenabwehr als auch für die Strafverfolgung zu empfehlen. Denkbar wäre es, als zentrale Stelle die Bundesnetzagentur zu beauftragen.

[2011] Auch mehre Telekommunikationsdiensteanbieter haben laut Bericht des MPI die Einrichtung für eine zentralen Stelle, wie sie etwa in Bayern bestehen, zur Koordinierung der Abfragen auf Seite der Berechtigten plädiert. Zudem wurde sich hier für einen einheitlichen Richtervorbehalt in allen Fällen ausgesprochen; *Albrecht/Kilchling* 2011, 179.

[2012] Vgl. oben S. 242 ff.

[2013] Vgl. oben S. 329f.

Empfohlen wird die Einführung eines zentralisierten Abrufsystems. Die Datenübermittlung sollte nur elektronisch, unter besonders hohen Sicherheitsvorkehrungen, auf Anfrage einer eindeutig authentifizierten Behörde erfolgen.

10.2 Verwendung

Der Beschränkung der Verwendung der Daten kommt bei der Vorratsdatenspeicherung besondere Bedeutung zu, da die Erhebung grundsätzlich anlasslos erfolgt. Das *Bundesverfassungsgericht* führt dazu aus: „Für die Verwendung der umfangreichen und vielfältig aussagekräftigen Datenbestände einer vorsorglich anlasslosen Telekommunikationsverkehrsdatenspeicherung sind insoweit hohe Anforderungen zu stellen. Sie haben zum einen die Aufgabe, eine sich aus dem Nichtwissen um die tatsächliche Relevanz der Daten ergebende Bedrohlichkeit zu mindern, verunsichernden Spekulationen entgegen zu wirken und den Betroffenen die Möglichkeit zu schaffen, solche Maßnahmen in die öffentliche Diskussion zu stellen."[2014]

Die Ebene der Datenverwendung ist nach der Datenerhebung und Datenspeicherung die zweite Ebene auf der das Kollisionsverhältnis von Freiheits- und Sicherheitsebene im Sinne eines praktisch-konkordanten Ausgleichs aufgelöst werden kann.

In der Vorratsdatenspeicherungsrichtlinie wird in Art. 1 Abs. 1 die Verwendung beschränkt auf „Zwecke der Ermittlung, Feststellung und Verfolgung von schweren Straftaten". Welchen staatlichen Stellen unter welchen formellen und materiellen Voraussetzungen jedoch genau Zugriff auf die Daten gewährt werden soll, wird von der Richtlinie nicht vorgegeben.[2015]

Das *Bundesverfassungsgericht* hat in ständiger Rechtsprechung betont, dass die „Voraussetzungen für die Datenverwendung und deren Umfang in den betreffenden Rechtsgrundlagen umso enger begrenzt werden, je schwerer der in der Speicherung liegende Eingriff wiegt. Anlass, Zweck und Umfang des jeweiligen Eingriffs sowie die entsprechenden Eingriffsschwellen sind dabei durch den Gesetzgeber bereichsspezifisch, präzise und normenklar zu regeln".[2016] Da die Speicherung der Telekommunikationsverkehrsdaten sämtlicher Bürger ohne konkreten Anlass einen besonders schweren Grundrechtseingriff bedeutet,[2017] unterliegt die Verwendung im Rahmen der Vorratsdatenspeicherung anlasslos gespeicherter Telekommunikationsverkehrsdaten auch „besonders hohen Anforderungen".[2018]

[2014] BVerfGE 125, 260 (335).

[2015] *Szuba* 2011, 55; Aus den Erwägungsgründen der RL lässt sich lediglich ablesen, dass die Daten zu Zwecken der Strafverfolgung, insbesondere im Hinblick auf schwere Straften, Organisierte Kriminalität und den Terrorismus, gespeichert werden sollen. Art. 4 der RL räumt den Mitgliedstaaten insgesamt jedoch einen sehr weiten Umsetzungsspielraum ein und verlangt lediglich eine Regelung, dass die Daten nur in Übereinstimmung mit dem innerstaatlichen Recht weitergegeben werden dürfen.

[2016] BVerfGE 125, 260 (328), unter Hinweis auf BVerfGE 100, 313 (359f..); 110, 33 (53); 113, 29 (51); 113, 348 (375); 115, 166 (191); 115, 320 (365); 118, 168 (186f.).

[2017] Vgl. dazu oben S. 274 ff.

[2018] BVerfGE 125, 260 (329).

Es sind jedenfalls höhere Anforderungen als für die Verwendung von Telekommunikationsverkehrsdaten zu stellen, die die Dienstanbieter nach § 96 TKG speichern.[2019] Denn, so argumentiert das *Bundesverfassungsgericht*, „angesichts der Unausweichlichkeit, Vollständigkeit und damit gesteigerten Aussagekraft der über sechs Monate systematisch vorsorglich erhobenen Verkehrsdaten hat ihr Abruf ein ungleich größeres Gewicht. Da eine Auswertung dieser Daten tief in das Privatleben eindringende Rückschlüsse und unter Umständen detaillierte Persönlichkeits- und Bewegungsprofile ermöglicht, kann insoweit nicht ohne weiteres davon ausgegangen werden, dass der Rückgriff auf diese Daten grundsätzlich geringer wiegt als eine inhaltsbezogene Telekommunikationsüberwachung.“[2020] Vielmehr, so das Gericht, könne die Verwendung solcher Daten nur dann als verhältnismäßig angesehen werden, wenn sie besonders hochrangigen Gemeinwohlbelangen dient. Eine Verwendung der Daten kommt demnach insgesamt „nur für überragend wichtige Aufgaben des Rechtsgüterschutzes in Betracht, das heißt zur Ahndung von Straftaten, die überragend wichtige Rechtsgüter bedrohen oder zur Abwehr von Gefahren für solche Rechtsgüter“.[2021]

Zudem ist zu berücksichtigen, dass auch die Anforderungen an die Bestimmtheit sehr hoch sind, da es sich um einen besonders schweren Grundrechtseingriff handelt. Es ist daher erforderlich, die Verwendungszwecke eindeutig zu konkretisieren.[2022]

10.2.1 Abrufregelungen

Ein Interesse im Rahmen der Gewährleistung auf die Daten zuzugreifen besteht sowohl im Rahmen der Strafverfolgung, der Gefahrenabwehr als auch durch die Nachrichtendienste. Schließlich haben auch private Rechteinhaber, im Bereich von Urheberrechtsverletzungen, ein Interesse daran insbesondere auf die auf Vorrat gespeicherten IP-Zugangsdaten zuzugreifen. Ein direkter Zugriff dieser Interessenten auf die auf Vorrat gespeicherten Verkehrsdaten scheidet schon wegen des besonders hohen Eingriffsgewichts aus. Insofern ist allein im Folgenden zu diskutieren unter welchen Voraussetzungen ein Abruf der Daten durch staatliche Behörden erfolgen kann und im Sinne eines optimierten Interessenausgleichs auch erfolgen sollte.

10.2.1.1 Abruf durch Strafverfolgungsbehörden

Das *Bundesverfassungsgericht* legt dar, dass für den Zugriff im Rahmen der Strafverfolgung der Abruf „den durch bestimmte Tatsachen begründeten Verdacht einer schweren Straftat voraussetzt“. Die Straftatbestände, die davon erfasst werden, müsste der Gesetzgeber „abschließend mit der Verpflichtung zur Datenspeicherung“ festlegen. Er müsse zudem sicherstellen, dass ein Rückgriff auf die Vorratsdaten nur dann zulässig ist, wenn die verfolgte Straftat auch im konkreten Einzelfall schwer wiegt und die Verwendung der Daten verhältnismäßig ist.[2023] Entweder könnten einzelne Straftaten enumerativ aufgezählt werden, für deren Verfolgung Verkehrsdaten von besonderer Relevanz sind oder es könnte auf bestehende Straftatenkataloge (etwa wie in § 100c

[2019] Zur Abfrage nach altem Recht s. BVerfGE 107, 299 (322).
[2020] BVerfGE 125, 260 (328).
[2021] BVerfGE 125, 260 (328).
[2022] Vgl. etwa oben S. 286.
[2023] BVerfGE 125, 260 (328 f.).

Abs. 2 oder auch § 100a StPO) zurückgegriffen werden. Erforderlich sei wegen des hohen Eingriffsgewichts der Vorratsdatenspeicherung, dass der Zugriff grundsätzlich nur für entsprechend schwere Straftaten gestattet wird.

Laut der Untersuchung des Max-Planck-Instituts sprechen sich Polizei und Staatsanwaltschaft sowie Richter ausdrücklich gegen eine Kataloglösung aus. „Der abstrakte Straftatbestand indiziere nicht automatisch die tatsächliche Schwere einer Straftat". Verwiesen wird hier von Staatsanwälten auf die Nichtkatalogtat der Nachstellung. Diese nach dem Alltagsverständnis eher minderschweren Sachverhalte könnten allein anhand formaler Kriterien zum Teil schwer zu klassifizieren sein. Als Beispiel wird noch das „Abziehen auf dem Schulhof"[2024] genannt, das als Raub Katalogdelikt gem. §§ 100a und 100g StPO ist.[2025]

Von Vertretern der Polizei wurden zur Lösung des Problems verschiedene Möglichkeiten aufgezeigt. Erwogen wird, dass zwei Kriterien nebeneinander für die Abfrage aufgestellt werden. Und zwar solle „einerseits nach der Qualität einer Straftat gefragt werden, andererseits nach den Ermittlungsmöglichkeiten in dem jeweiligen Phänomenbereich unabhängig von der Schwere der einzelnen Tat".[2026] Eine solche Lösung ist aber mit den verfassungsrechtlichen Anforderungen nicht vereinbar. Der Zugriff auf die Daten ist – unabhängig von den Ermittlungsmöglichkeiten im jeweiligen Phänomenbereich – auf Grund der Eingriffsschwere allein zur Verfolgung schwerer Straftaten möglich. Vorgeschlagen wurde sodann, dass der Zugriff auf die gespeicherten Daten in all denjenigen Fällen eröffnet werden sollte, „in denen die Schädigung des Opfers eine bestimmte Schwelle überschreitet. Dabei könnten einerseits Schädigungen körperlicher oder psychischer Art, andererseits aber auch Schäden materieller Art berücksichtigt werden. Dieser Ansatz würde es ermöglichen, den volkswirtschaftlichen Schaden eines Kriminalitätsbereiches zu berücksichtigen."[2027] Ganz überwiegend wird gefordert, dass die Formulierung des § 100g Abs. 1 Nr. 2 StPO neben einem Katalog bestehen bleiben müsse, da ansonsten die Ermittlungen im gesamten Bereich der Computerkriminalität vielfach leer laufen oder unmöglich würden. Von Seiten der Richter wird übereinstimmend ein offener Katalog befürwortet. Mittels einer solchen Anlehnung etwa an die Regelbeispieltechnik, die aus dem Strafgesetzbuch bekannt ist, würde es ermöglicht, neben exemplarisch aufgelisteten Straftaten bei Bedarf auch andere Fälle vergleichbarer Schwere zu erfassen.[2028] Anders als Polizei, Staatsanwälte und Richter plädieren die Telekommunikationsanbieter überwiegend für eine Kataloglösung.[2029]

Um die Akzeptanz der Vorratsdatenspeicherung zu erhöhen, sollte ein Zugriff auf die Daten nur zu den Zwecken erlaubt werden mit denen die Einführung der Vorratsdatenspeicherung gerechtfertigt wird. Mithin sind das Terrorismus, organisierte Kriminalität

[2024] Wenn unter Androhung oder Anwendung von Gewalt Kleidung, Handys oder sonstiges von einem anderen Schüler herausverlangt oder diesem abgenommen wird, erfüllt dies dem Tatbestand der räuberischen Erpressung bzw. des Raubs (§§ 253, 255 StGB).
[2025] *Albrecht/Kilchling* 2011, 170; 160; 174.
[2026] *Albrecht/Kilchling* 2011, 161.
[2027] *Albrecht/Kilchling* 2011, 161.
[2028] *Albrecht/Kilchling* 2011, 174.
[2029] Vgl. Nachw. in Fn. 2011.

und Kinderpornographie. Allerdings darf auch für diese Straftaten nur dann der Zugriff zugelassen werden, wenn und soweit es sich um besonders schwere Straftaten handelt.[2030] Insbesondere der Besitz und der Handel mit Kinderpornographie sind nach geltendem Strafrecht nicht zwingend als besonders schwere Straftaten zu klassifizieren.

In den Erwägungen von Polizei, Staatsanwälten und Richtern tritt deutlich zu Tage, dass die alleinige Anknüpfung an einen Straftatenkatalog von diesen nicht für sachgerecht erachtet wird. Die dort verfolgte Argumentation, dass unbedingt ein Zugriff auch im Rahmen der mittels Telekommunikation begangener Taten möglich sein solle, entspricht dem Bild, das Ermittlungsbehörden ein großes Interesse an den Daten eben in genau diesem Deliktsbereich haben, auch wenn tatsächlich ohne diese Daten die Ermittlungen keineswegs unmöglich werden.[2031] Eine Vorratsdatenspeicherung kann aber aufgrund des hohen Eingriffsgewichts nicht nur eingeführt werden, nur um Aufklärungsdefizite für einen Deliktsbereich in dem es, auf Grund technischer und gesellschaftlicher Veränderungen an Ermittlungsansätzen mangelt, abzuhelfen.

Die Vorratsdatenspeicherung als infrastrukturelles Überwachungsinstrument wiegt grundsätzlich besonders schwer und darf entsprechend auch nur für besonders gewichtige Interessen der Allgemeinheit eingesetzt werden. Die Forderung, einen Zugriff im Rahmen der Verfolgung im Bereich der Informations- und Kommunikationskriminalität einzuräumen, ist aus verfassungsrechtlichen Gründen abzulehnen. Die Vorratsspeicherung sämtlicher Telekommunikationsverkehrsdaten aller Bürger ist nur zum Zweck der Verfolgung besonders schwerer Straftaten, die auch im konkreten Fall besonders schwer wiegen, zulässig.

Um sicherzustellen, dass es sich im konkreten Fall um eine besonders schwere Straftat handelt, könnte der Straftatenkatalog mit einer Anforderung an den Strafrahmen verknüpft werden.

Empfohlen wird, den Zugriff auf die Vorratsdaten für die Strafverfolgung wesentlich auf organisierte Kriminalität und Terrorismus zu begrenzen. Auch ein Abruf zur Verfolgung von Kinderpornografie ist denkbar. Darüber hinaus sollte ein Abruf nur zur Verfolgung besonders schwerer Straftaten zugelassen werden. Die Straftaten sind in einem Straftatenkatalog zu spezifizieren und mit einer Mindestanforderung an den Strafrahmen zu verknüpfen.

10.2.1.2 Abruf zu Zwecken der Gefahrenabwehr

Aus der Vorratsdatenspeicherungsrichtlinie lässt sich die Pflicht nicht ableiten, auf die Daten auch zum Zwecke der Gefahrenabwehr zuzugreifen. Art. 4 VDS-RL räumt den Mitgliedstaaten aber einen sehr weiten Umsetzungsspielraum ein. Es wird nur verlangt, dass die Daten nur in Übereinstimmung mit dem innerstaatlichen Recht weitergegeben werden. In Erwägungsgrund 25 wird erläutert, dass die Mitgliedstaaten die

[2030] BVerfGE 125, 260 (328).
[2031] Dies zeigen letztlich die durchaus hohen Aufklärungsquoten auch in diesem Deliktsfeld, vgl. dazu oben Kap. 4.4.2.2, S. 191 ff.

nationalen Behörden nennen müssen, die Zugang zu den Daten haben sollen. Der Zugriff auf die Daten zu Zwecken der Gefahrenabwehr ist insoweit europarechtlich nicht ausgeschlossen.

Es besteht ein hohes Interesse insbesondere im Rahmen der Bekämpfung von Terrorismus auf die Daten auch zur Gefahrenabwehr zuzugreifen. Soweit ein Zugriff auch zur Gefahrenabwehr zugelassen wird, muss es sich um Taten handeln, die ähnlich schwer wiegen, wie jene für die der Abruf im Rahmen der Strafverfolgung zugelassen wird.

So fordert das *Bundesverfassungsgericht*, dass die Verwendung der Vorratsdaten für die Gefahrenabwehr „gleichermaßen wirksam" begrenzt werden muss.[2032] Nicht geeignet sei eine Bezugnahme auf Kataloge von bestimmten Straftaten, die verhindert werden sollen – Gefahrenabwehr dient, wie der Name sagt, der Abwehr von Gefahren und zwar für Rechtsgüter. Die zu schützenden Rechtgüter sollten gesetzlich unmittelbar in Bezug genommen werden, ebenso wie die Intensität der Gefährdung dieser Rechtsgüter, die als Eingriffsschwelle erreicht sein muss.[2033] Für das *Bundesverfassungsgericht* ist, aufgrund der Schwere des Eingriffs der Datenspeicherung und der Datenverwendung, ein Abruf „nur zur Abwehr von Gefahren für Leib, Leben oder Freiheit einer Person, für den Bestand oder die Sicherheit des Bundes oder eines Landes oder zur Abwehr einer gemeinen Gefahr" zulässig.[2034]

Nach der Rechtsprechung des *Bundesverfassungsgerichts* wird die konkrete Gefahr durch drei Kriterien bestimmt: „den Einzelfall, die zeitliche Nähe des Umschlagens einer Gefahr in einen Schaden und den Bezug auf individuelle Personen als Verursacher."[2035]

Die Abfrage der vorsorglich gespeicherten Daten kann aber, so das Gericht ausdrücklich, „schon gerechtfertigt sein, wenn sich noch nicht mit hinreichender Wahrscheinlichkeit feststellen lässt, dass die Gefahr schon in näherer Zukunft eintritt, sofern bestimmte Tatsachen auf eine im Einzelfall drohende Gefahr für ein überragend wichtiges Rechtsgut hinweisen. Die Tatsachen müssen zum einen den Schluss auf ein wenigstens seiner Art nach konkretisiertes und zeitlich absehbares Geschehen zulassen, zum anderen darauf, dass bestimmte Personen beteiligt sein werden, über deren Identität zumindest so viel bekannt ist, dass die Maßnahme gezielt gegen sie eingesetzt und auf sie konzentriert werden kann."[2036] Eine weitreichende Verlagerung ins Vorfeld einer noch nicht absehbaren konkreten Gefahr ist dahingehend nicht verhältnismäßig zum Gewicht des Grundrechtseingriffs.[2037] Wichtig ist insofern, dass der Abruf von Verkehrsdaten im Vorfeld einer konkreten Gefahr tatsächlich nur unter sehr engen Voraussetzungen möglich ist.[2038]

[2032] BVerfGE 125, 260 (329).
[2033] BVerfGE 125, 260 (329).
[2034] BVerfGE 125, 260 (330).
[2035] BVerfGE 125, 260 (330).
[2036] BVerfGE 125, 260 (330).
[2037] BVerfGE 125, 260 (330 f.)
[2038] Ausführlich mit dem Gefahrenbegriff setzt sich auseinander: *Darnstädt*, DVBl. 2011, 263; Zur Definition des Gefahrenbegriffs und Nachweisen zur kritischen Auseinandersetzung mit diesem, auch oben Fn. 358.

Empfohlen wird den Abruf zu Zwecken der Gefahrenabwehr auf die Abwehr von Gefahren für Leib, Leben oder Freiheit einer Person, für den Bestand oder die Sicherheit des Bundes oder eines Landes oder zur Abwehr einer gemeinen Gefahr zuzulassen. Grundsätzlich ist der Abruf nur bei Vorliegen einer konkreten Gefahr zulässig. In Ausnahmefällen kann schon im Vorfeld einer konkreten Gefahr auf die Daten zugegriffen werden, wenn Tatsachen den Schluss auf ein wenigstens seiner Art nach konkretisiertes und zeitlich absehbares Geschehen zulassen und eine Konzentration der Maßnahme auf bestimmte Personen möglich ist.

10.2.1.3 Abruf für nachrichtendienstliche Zwecke

Die für den Abruf im Rahmen der Gefahrenabwehr geltenden Anforderungen, gelten auch für den Zugriff auf die auf Vorrat gespeicherten Daten durch Nachrichtendienste.[2039] Denn es kommt nicht auf die Aufgabe an, der die Dienste nachkommen, sondern auf die Beeinträchtigung durch den Eingriff beim Betroffenen. Daher besteht auch kein Unterschied, ob die Daten durch Polizeibehörden oder Nachrichtendienste abgerufen werden. So sieht es auch das *Bundesverfassungsgericht*. Es besteht kein „Anlass zu behördenbezogenen Differenzierungen, etwa zwischen Polizeibehörden und anderen mit präventiven Aufgaben betrauten Behörden wie Verfassungsschutzbehörden".[2040] Mehr noch bestehe eine „besondere Belastungswirkung" derartiger Eingriffe, da „nicht nur der jeweilige Eingriff in das Telekommunikationsgeheimnis als solcher (…) verdeckt geschieht, sondern praktisch die gesamten Aktivitäten der Nachrichtendienste geheim erfolgen." Das Gericht argumentiert daher, dass „Befugnisse dieser Dienste zur Verwendung der vorsorglich flächendeckend gespeicherten Telekommunikationsverkehrsdaten (…) das Gefühl des unkontrollierbaren Beobachtetwerdens in besonderer Weise" befördern und so „nachhaltige Einschüchterungseffekte auf die Freiheitswahrnehmung" entfalten.[2041]

Daher geht das *Bundesverfassungsgericht* davon aus, „dass damit eine Verwendung der vorsorglich gespeicherten Telekommunikationsverkehrsdaten von Seiten der Nachrichtendienste in vielen Fällen ausscheiden dürfte".[2042] Dem ist zuzustimmen.

Empfohlen wird Nachrichtendiensten keine Ermächtigung zum Abruf der Daten einzuräumen.

10.2.1.4 Keine mittelbare Verwendung zu anderen Zwecken

Wichtig für den Interessenausgleich ist schließlich, ob die auf Vorrat gesammelten Verkehrsdaten mittelbar genutzt werden dürfen zur Identifikation der Anschlussinhaber dynamischer IP-Adressen. Verkehrsdaten kommt eine herausragende Bedeutung für die Verfolgung von Urheberrechtsverletzungen, sowie zur Verfolgung von (teilweise niederschwelligen) Delikten im Bereich der Informations- und Kommunikationskriminalität zu.[2043]

[2039] BVerfGE 125, 260 (331).
[2040] BVerfGE 125, 260 (331).
[2041] BVerfGE 125, 260 (332).
[2042] BVerfGE 125, 260 (332).
[2043] Vgl. oben S. 196.

Allerdings würde eine solche mittelbare Nutzung der Verkehrsdaten für zivilrechtliche Ansprüche und für niederschwellige Delikte den Zweckbindungsgrundsatz konterkarieren, dem aber gerade bei der Vorratsdatenspeicherung eine herausragende Bedeutung zukommt, um das Vertrauen in das Telekommunikationsgeheimnis zu gewährleisten und die informationelle Selbstbestimmung zu schützen.

Für einen optimierten Interessenausgleich ist daher eine mittelbare Nutzung der Verkehrsdaten für andere Zwecke zu untersagen.[2044]

10.2.2 Umfang des Datenabrufs

Nicht nur die Voraussetzungen der Ausgestaltung der Ermächtigungsnormen zum Datenabruf sind durch die verfassungsrechtlichen Anforderungen geprägt. Auch hinsichtlich des jeweiligen Umfangs der abzurufenden Daten setzt die Verfassung Grenzen.

Es wurde bereits aufgezeigt, dass sich das Eingriffsgewicht unterscheidet je nachdem, welche und wie viele Daten abgerufen werden.[2045] So erkennt auch das *Bundesverfassungsgericht* „vielfältige Abstufungen zwischen den verschiedenen Auskunftsbegehren" an. Das Gericht differenziert „etwa danach, ob sie nur eine einzelne Telekommunikationsverbindung betreffen, sie auf die Übermittlung der Daten aus allein einer Funkzelle zu einem bestimmten Zeitpunkt zielen, sie bezogen sind nur auf die Kommunikation zwischen einzelnen Personen – begrenzt möglicherweise auf einen bestimmten Zeitraum oder eine bestimmte Form der Kommunikation – und hierbei auch die Standortdaten ein- oder ausschließen oder ob sie auf eine vollständige Übermittlung der Daten einer Person zur Erstellung eines möglichst detaillierten Bewegungs- oder Persönlichkeitsprofils zielen."[2046]

Der Grundsatz der Verhältnismäßigkeit verlangt, dass dem unterschiedlichen Gewicht des Abrufs der Daten Rechnung getragen wird. Der Gesetzgeber muss insofern allgemein regeln, welcher Datenumfang zur Verfolgung welcher Straftaten oder zur Abwehr welcher Gefahren angemessen ist. Auch muss er sicherstellen, dass sich der „Abruf sowie die tatsächliche Verwendung der Daten auf den unbedingt erforderlichen Teil der Datensammlung" beschränkt.[2047] Diese Forderung richtet sich an die jeweils abrufende staatliche Stelle. Sichergestellt werden kann dies zudem durch eine richterliche Prüfung des Ersuchens, das spezifisch auch den Umfang des Datenabrufs prüfen sollte.

Es ist durch rechtliche und organisatorische Maßnahmen sicherzustellen, dass sich der Datenabruf auf den jeweils unbedingt erforderlichen Teil beschränkt.

10.2.3 Proliferation von Daten und Informationen

Auch bei der Weitergabe von bereits an Behörden übermittelten Vorratsdaten und aus diesen gewonnen Erkenntnissen sind verfassungsrechtliche Anforderungen, die insbesondere aus dem datenschutzrechtlichen Kern des Telekommunikationsgeheimnisses erwachsen, zu beachten. In diesem Sinne hat auch das *Bundesverfassungsgericht* im Urteil zur Vorratsdatenspeicherung betont, dass „die Telekommunikationsverkehrsdaten

[2044] Vgl. oben S. 281.
[2045] Vgl. dazu oben S. 365 ff.
[2046] BVerfGE 125, 260 (333f.).
[2047] BVerfGE 125, 260 (330).

ihren durch Art. 10 GG vermittelten Schutz nicht dadurch“ verlieren, „dass bereits eine staatliche Stelle von ihnen Kenntnis erlangt hat“.[2048] Dies gilt auch aus Gründen der informationellen Gewaltenteilung.[2049] Es gelten daher die hohen Anforderungen an den Abruf der Daten, auch wenn die Daten nur an eine andere Behörde weitergegeben werden sollen.

In diesem Sinne verlangt § 474 Abs. 2 StPO, dass Daten nur weitergeben werden dürfen für die Zwecke, für die sie auch hätten erhoben werden dürfen.[2050] Zudem bedarf es für die Weitergabe einer eigenen gesetzlichen Grundlage, die ihrerseits verfassungsrechtlichen Ansprüchen genügt.[2051] Dies ist von der weiterleitenden Stelle zu protokollieren.[2052] Dabei lässt sich die Zweckbindung nur gewährleisten, wenn auch nach der Erfassung erkennbar bleibt, dass es sich um Daten handelt, die vorsorglich anlasslos gespeichert wurden. Der Gesetzgeber hat dementsprechend für diese Daten eine Kennzeichnungspflicht anzuordnen.[2053] Diese ist idealerweise durch technische Vorkehrungen zu realisieren.[2054]

Die Weitergabe von Daten und aus Ihnen gewonnen Informationen ist nur unter strenger Bindung an den Zweckbindungsgrundsatz zulässig.

10.2.4 Abrufverfahren: Richtervorbehalt

Grundsätzlich ist der Abruf unter Richtervorbehalt zu stellen, also ist eine vorbeugende richterliche Kontrolle einzuführen.[2055] Dies ist zunächst erforderlich, um effektiven Rechtsschutz zu gewährleisten.[2056] Sodann auf Grund der Tatsache, dass eine offene Erhebung in der Regel ausscheidet. Das *Bundesverfassungsgericht* führt bezüglich der Abfrage und Übermittlung von Telekommunikationsverkehrsdaten aus, dass aufgrund des Eingriffsgewichts der Spielraum des Gesetzgebers dahingehend reduziert sei solche Maßnahmen grundsätzlich unter den Vorbehalt richterlicher Anordnung zu stellen seien.[2057] An die richterliche Anordnung an sich seien sodann besonders strenge An-

[2048] BVerfGE 125, 260 (333) unter Hinweis auf BVerfGE 100, 313 (360f.).
[2049] Vgl. oben Kap. 9.3.2.1, S. 328.
[2050] Auch das *BVerfG* betont wiederholt in seiner Rspr., dass eine Weitergabe personenbezogener Daten nur erfolgen darf, soweit diese zur Wahrnehmung von Aufgaben erfolgt, die auch den unmittelbaren Zugriff auf die Daten rechtfertigen könnten, BVerfGE 100, 313 (389f.); 109, 279 (375f.); 110, 33 (73).
[2051] BVerfGE 100, 313 (360); 109, 279 (375f.).
[2052] BVerfGE 100, 313 (395f.).
[2053] BVerfGE 125, 260 (333) unter Hinweis auf BVerfGE 100, 313 (360f.).
[2054] Vgl. dazu S. 350 f.
[2055] BVerfGE 125, 260 (337); Das Grundgesetz stellt Eingriffe in Art. 10 GG zwar nicht grundsätzlich unter Richtervorbehalt. Das Gericht hat jedoch in ständiger Rspr. entwickelt, dass schwerwiegende Grundrechtseingriffe in das Telekommunikationsgeheimnis und die informationelle Selbstbestimmung unter Richtervorbehalt zu stellen sind; vgl. zur Anerkennung des Richtervorbehalts bei schweren Eingriffen in das Fernmeldegeheimnis, auch schon oben S. 99 f.
[2056] Vgl. dazu oben S. 99 f.; 278 ff.
[2057] Nur für die Kontrolle durch Nachrichtendienste könnte an die Stelle einer vorbeugenden Kontrolle auch eine Kontrolle durch ein von der Volksvertretung bestelltes Organ oder Hilfsorgan treten. Da nach der hier vertretenen Ansicht Nachrichtendiensten aber erst gar keine Ermächtigung zum Ab-

forderungen zu stellen, welches aus dem Erfordernis einer hinreichend substantiierten Begründung und Begrenzung der Abfrage der begehrten Daten erfolge. So müsse der Anordnungsbeschluss des Gerichts „gehaltvoll" begründet werden.[2058]

In den § 100d Abs. 2 und 3 StPO sind bereits spezifische Voraussetzungen an die Anordnung von Telekommunikationsüberwachungsmaßnahmen formuliert. Da das Eingriffsgewicht einer Vorratsdatenspeicherung nicht grundsätzlich weniger schwer wiegt als eine inhaltliche Überwachung,[2059] sind zumindest äquivalente Anforderungen auch bei einer Vorratsdatenspeicherung zu stellen. Denkbar wäre auch in Anlehnung an die Einrichtung von Schwerpunktstaatsanwaltschaften, die Anordnungsbefugnis jeweils nur bestimmten besonders geschulten Richtern zuzuweisen.[2060] Dies gilt insbesondere in Anbetracht der in der Realität vielfach festzustellenden mangelnden Effektivität des Richtervorbehalts.[2061]

Dem Richtervorbehalt kommt bei der Vorratsdatenspeicherung eine besonders hohe Bedeutung zu. Er dient dazu den grundsätzlich heimlichen Abruf der Verkehrsdaten insbesondere im Hinblick auf die Verhältnismäßigkeit im konkreten Einzelfall zu überprüfen. Daher sind umfassende organisatorische Maßnahmen vorzusehen, damit der Richtervorbehalt tatsächlich effektiv wirkt.

Die Abfrage ist grundsätzlich unter Richtervorbehalt zu stellen, allein bei Gefahr im Verzug darf ausnahmsweise auch die Staatsanwaltschaft den Abruf anordnen. Die richterliche Prüfung muss dann umgehend nachgeholt werden. Um die Effektivität des Schutzinstruments sicherzustellen, sollten verbindliche Regelungen für den Umfang und das Verfahren vorgegeben werden.

10.2.5 Bedingungen der Datenspeicherung bei staatlichen Behörden

Insgesamt gilt, dass auch bei der weiteren Verwendung von einmal rechtmäßig beauskunfteten Verkehrsdaten staatliche Stellen die informationelle Selbstbestimmung des Betroffenen achten müssen.

So ist beim Umgang mit den Daten ein hoher Sicherheitsstandard zu wahren. Zu berücksichtigen ist dabei, dass das Angriffspotential und das Missbrauchsrisiko, sobald die Daten von einer staatlichen Behörde verarbeitet werden, geringer werden. Schließlich entsteht hier keine große Datenbank, die Informationen beinhaltet, die von großem wirtschaftlichem Interesse sind, sondern es sind nur einzelne Datensätze, die konkret für bestimmte Verfahren benötigt werden. Auch sind sie nicht mehr in einer privaten Datenbank, sondern in einer staatlichen Datenbank, bei der die zum Zugriff berechtig-

---

ruf der Vorratsdaten erteilt werden soll (vgl. dazu oben S. 363f.), wird die Möglichkeit der Kontrolle durch eine andere Stelle auch nicht weiter diskutiert.

[2058] BVerfGE 125, 260 (338); dazu bereits ausführlich oben, S. 278 f.

[2059] BVerfGE 125, 260 (328).

[2060] *Roßnagel/Bedner/Knopp*, DUD 2009, 536, 540; *Szuba* 2011, 261; insbesondere im Hinblick auf das erforderliche technische Verständnis, um zu beurteilen, wie schwer ein solcher Eingriff wiegt, sind Schulungen der zuständigen Richter zu empfehlen.

[2061] Vgl. dazu oben Kap. 9.1.2.1.3.3, S. 278 ff.

ten Personen an Amtspflichten gebunden sind, und insofern schon ein höherer Schutz garantiert ist.

Dennoch besteht auch hier in technischer und organisatorischer Hinsicht ein hoher Schutzbedarf. Die Daten sind (jedenfalls zum Teil) hoch sensitiv und dürfen daher nur unter Beachtung hoher technischer und organisatorischer Sicherheitsvorkehrungen verarbeitet und gespeichert werden. Erforderlich sind daher konkrete Vorgaben zur Gewährleistung der Datensicherheit auch bei der Speicherung durch staatliche Stellen.[2062]

Daten dürfen sodann nur für die Zwecke verwendet werden für die sie gespeichert wurden. Die zweckfreie Bildung von Persönlichkeitsprofilen ist insofern auszuschließen.

Es ist sicherzustellen, dass „die Daten nach Übermittlung unverzüglich ausgewertet werden und, sofern sie für die Erhebungszwecke unerheblich sind, gelöscht werden".[2063] Im Übrigen ist vorzusehen, dass „die Daten vernichtet werden, sobald sie für die festgelegten Zwecke nicht mehr erforderlich sind, und dass hierüber ein Protokoll gefertigt wird".[2064] Denkbar wäre, um versehentliche „Aktenleichen" zu vermeiden, Fristen festzulegen in denen zu prüfen wäre, ob die gespeicherten Daten noch erforderlich sind.[2065]

Empfohlen wird die Formulierung spezifischer Anforderungen an die Aufbewahrung und Verarbeitung der Daten durch die abrufenden Behörden.

10.2.6 Datenübermittlung in andere Staaten

Die Vorratsdatenspeicherungsrichtlinie selbst enthält keine Vorgaben zum Austausch der Vorratsdaten mit anderen Staaten. Es besteht jedoch ein hohes Interesse, im Rahmen der europaweiten, aber auch der internationalen Zusammenarbeit, auf diese Daten zuzugreifen.

Bei der Übermittlung der Telekommunikationsverkehrsdaten in andere Staaten sind die verfassungsrechtlichen Vorgaben zu beachten.[2066] Nur soweit die Zweckbindung der Daten gewährleistet ist und allein Polizei und Gefahrenabwehrbehörden auf die Daten zugreifen dürfen, kann eine Übermittlung ins Ausland gerechtfertigt werden. Es muss sichergestellt sein, dass die Daten nicht zweckentfremdet werden. Das Vorliegen der Übermittlungsvoraussetzungen ist durch einen Richter zu prüfen.

Es wird empfohlen die Übermittlung von Vorratsdaten und aus diesen gewonnenen Informationen ins Ausland grundsätzlich unter Richtervorbehalt zu stellen. Eine Übermittlung darf nur erfolgen, soweit die Zweckbindung gewährleistet ist.

[2062] *Szuba* 2011, 251.
[2063] BVerfGE 100, 313 (387f.).
[2064] BVerfGE 125, 260 (332f.) mit Verweis auf BVerfGE 100, 313 (362); 113, 29 (58).
[2065] So generell für § 101 Abs. 7 StPO, *Szuba* 2011, 153 ff.
[2066] Vgl. dazu oben Kap. 9.3.1.2, S. 323 ff.

10.3 Transparenz

Die informationelle Selbstbestimmung verlangt, dass die Erhebung grundsätzlich offen erfolgt.[2067] Dies ist zwar dem Grunde nach bei der Vorratsdatenspeicherung für die Speicherungsverpflichtung der Fall, da sie nur auf einem Gesetz gründen kann, dass verkündet wird und somit jedem bekannt ist, dass die Daten gespeichert werden.

Transparenz ist aber auch für den Abruf zu fordern, da auch dieser eigenständig in das informationelle Selbstbestimmungsrecht der Bürger eingreift. Dies gilt insbesondere in Anbetracht des durch eine Vorratsdatenspeicherung ausgelöstem „Gefühl des ständigen Überwachtwerdens". Denn „der Einzelne weiß nicht, was welche staatliche Behörde über ihn weiß, weiß aber, dass die Behörden vieles, auch Höchstpersönliches über ihn wissen können."[2068]

Der Abruf von auf Vorrat gespeicherten Verkehrsdaten gegenüber dem Betroffenen muss daher möglichst transparent erfolgen. Auch das *Bundesverfassungsgericht* hat festgestellt, dass „zu den Voraussetzungen der verfassungsrechtlich unbedenklichen Verwendung" der Vorratsdaten auch „Anforderungen an die Transparenz" gehören. Soweit möglich muss daher die Verwendung der Daten dem Betroffenen gegenüber offen erfolgen. „Ansonsten bedarf es grundsätzlich zumindest nachträglich einer Benachrichtigung der Betroffenen", so das *Bundesverfassungsgericht*.[2069] Es sind daher entsprechende Informationspflichten einzuführen.

Für verdeckte Ermittlungsmaßnahmen sind Benachrichtigungspflichten in § 101 Abs. 4 bis 6 StPO geregelt. Bei einer Verkehrsdatenauskunft sind gemäß § 101 Abs. 4 S. 1 Nr. 6 StPO „die Beteiligten der betroffenen Telekommunikation" zu benachrichtigen. Fraglich ist, ob in dem Fall, dass Standortdaten im Stand-by-Betrieb abgefragt werden Benachrichtigungspflichten bestehen.[2070] Gemäß § 101 Abs. 4 S. 3 StPO kann eine Benachrichtigung unterbleiben, „wenn ihr überwiegende schutzwürdige Belange einer betroffenen Person entgegenstehen". Darüber hinaus wird in S. 4 die Möglichkeit eingeräumt, auf eine Benachrichtigung einer Person, „gegen die sich die Maßnahme nicht gerichtet hat" zu verzichten, „wenn diese von der Maßnahme nur unerheblich betroffen wurde und anzunehmen ist, dass sie kein Interesse an einer Benachrichtigung hat".

Schwierigkeiten bestehen hier insbesondere im Hinblick auf die Frage, wie ermittelt werden soll, ob ein Interesse an der Benachrichtigung besteht oder nicht.[2071] Wegen der hohen Bedeutung der Benachrichtigung für die informationelle Selbstbestimmung der Bürger und der Möglichkeit, durch die Gewährleistung umfassender Benachrichtigungspflichten das Gefühl des Überwachtwerdens zu reduzieren, ist eine enge Auslegung dieses Ausnahmetatbestands zu fordern.[2072]

[2067] Vgl. dazu oben S. 88.
[2068] BVerfGE 125, 260 (335).
[2069] BVerfGE 125, 260 (334f.).
[2070] *Szuba* 2011, 154.
[2071] *Szuba* 2011, 154 ff.; *Ziebarth*, DUD 2009, 25, 31.
[2072] So auch im Ergebnis *Puschke/Singelnstein*, NJW 2008, 113, 116; *Szuba* 2011, 155.

Unberührt davon bleibt die Regelung in § 101 Abs. 4 S. 5 StPO. Danach besteht keine Informationspflicht, wenn zunächst Nachforschungen zur Feststellung der Identität vorzunehmen wären, und dies „unter Berücksichtigung der Eingriffsintensität der Maßnahme gegenüber dieser Person, des Aufwands für die Feststellung ihrer Identität sowie der daraus für diese oder andere Personen folgenden Beeinträchtigungen geboten ist". Daran wird kritisiert, dass diese Einschränkung nicht mit dem verfassungsrechtlich vorgegebenen Anspruch auf Benachrichtigung in Einklang gebracht werden könne, da sich der Benachrichtigungsaufwand nur schwer von dem insgesamt durch die Überwachungsmaßnahme verursachten Arbeitsaufwand trennen lasse und insofern ohne Einfluss auf den Benachrichtigungsanspruch bleiben müsse.[2073] Dem ist zwar grundsätzlich zuzustimmen, jedoch ist zu beachten, dass wenn etwa für eine Benachrichtigung erst noch die Identität ermittelt werden muss und dadurch der Eingriff vertieft wird, durchaus auch im Sinne der informationellen Selbstbestimmung des Bürgers ein Interesse daran besteht, dass die Benachrichtigung unterbleibt.

Die Gewährleistung von Transparenz ist auch deshalb von so großer Bedeutung, weil erst die Kenntnis des Grundrechtseingriffs die Möglichkeit eröffnet, Rechtsschutz zu suchen.

Letztlich darf auf Grund dessen die nachträgliche Benachrichtigung nur ausnahmsweise unterbleiben. Erforderlich sind dafür zwingende Gründe. Es ist zudem eine richterliche Entscheidung einzuholen.[2074]

Auch für die Verwendung der Daten für Zwecke der Gefahrenabwehr sind die Benachrichtigungspflichten entsprechend auszugestalten.[2075] Grundsätzlich erfolgt eine Benachrichtigung gemäß § 100 Abs. 5 StPO erst, wenn dadurch der Untersuchungszweck nicht gefährdet wird. Ein so gerechtfertigter Aufschub der Benachrichtigung bedarf der gerichtlichen Zustimmung, wenn diese nicht innerhalb von zwölf Monaten nachgeholt wurde. Diese Frist ist jedoch sehr lang bemessen. Im Sinne eines optimierten Interessenausgleichs sollte die Benachrichtigung grundsätzlich umgehend erfolgen und bereits, wenn nach sechs Monaten die Benachrichtigung nicht nachgeholt wurde, dies richterlich überprüft werden.

Grundsätzlich sollte der Abruf der Daten offen erfolgen, es sei denn der Zweck der Maßnahme wird dadurch gefährdet. Der heimliche Zugriff sollte gesondert beim Richter beantragt werden. Eine nachträgliche Benachrichtigung sollte möglichst umgehend erfolgen. Wenn sie nicht innerhalb von sechs Monaten nachgeholt wurde, ist dies richterlich zu prüfen.

[2073] *Szuba* 2011, 155; So auch schon in der Stellungnahme zum Regierungsentwurf: *AK-Vorrat et al.,* 2007, 25.
[2074] BVerfGE 125, 260 (334f.).
[2075] BVerfGE 125, 260 (337).

10.4 Rechtsschutz und Sanktionen

Die Richtlinie verlangt, dass Rechtsschutzmöglichkeiten sowie Sanktionen vorgesehen werden – wie genau diese auszugestalten sind, gibt die Richtlinie jedoch nicht vor.[2076]

Auch das *Bundesverfassungsgericht* hat die Bedeutung von Rechtsschutzmöglichkeiten betont: „Von Verfassungs wegen geboten ist auch die Eröffnung eines Rechtsschutzverfahrens zur nachträglichen Kontrolle der Verwendung der Daten. Sofern ein Betroffener vor Durchführung der Maßnahme keine Gelegenheit hatte, sich vor den Gerichten gegen die Verwendung seiner Telekommunikationsverkehrsdaten zur Wehr zu setzen, ist ihm eine gerichtliche Kontrolle nachträglich zu eröffnen.“[2077]

§ 101 Abs. 7 StPO ermächtigt den Betroffenen dazu, innerhalb von zwei Wochen nach Benachrichtigung eine sofortige Beschwerde zu erheben und damit die Überprüfung der Rechtmäßigkeit der Maßnahme sowie der Art und Weise des Vollzugs bei Gericht zu beantragen.

Die Beschränkung auf zwei Wochen ist sehr kurz bemessen. Dies gilt insbesondere soweit keine konkreten Vorgaben zur Ausgestaltung der Benachrichtigungspflicht bestehen, da in diesem Fall die Benachrichtigung für den einzelnen juristisch nicht geschulten Bürger so komplex sein kann, das er kaum in der Lage ist sich innerhalb von zwei Wochen sachkundig zu machen und eine Entscheidung zu fällen, ob Rechtsmittel eingelegt werden sollen. Sinnvoll kann ein Betroffener nur dann Rechtsschutz suchen, wenn er auch die Möglichkeit hat sich über Art und Umfang der Maßnahme durch Akteneinsicht zu informieren und den Sachverhalt umfassend zu prüfen. Dies ist selbst dann wenn die Benachrichtigung gut verständlich formuliert ist, innerhalb von zwei Wochen kaum zu leisten. Die Frist führt letztlich auch zu einer Mehrbelastung der Gerichte. Denn Betroffene werden schon aus Zeitmangel für eine genaue Prüfung schon vorsorglich einen Antrag auf Überprüfung stellen. Entsprechend ist eine Frist zur Einlegung von Rechtsmitteln von mindestens vier Wochen zu fordern.[2078]

Neben Rechtsschutzmöglichkeiten ist es auch verfassungsrechtlich zwingend erforderlich, wirksame Sanktionen vorzusehen. Denn die Verpflichtung der staatlichen Gewalt, dem Einzelnen die Entfaltung seiner Persönlichkeit zu ermöglichen[2079] und ihn vor Persönlichkeitsrechtsgefährdungen durch Dritte zu schützen[2080] beinhaltet auch die Forderung, wirksame Sanktionen bei Verletzungen des Telekommunikationsgeheimnisses durch Missachtung der verfassungsrechtlichen Schutzanforderungen vorzusehen.[2081]

Das *Bundesverfassungsgericht* räumt dem Gesetzgeber diesbezüglich einen „weiten Gestaltungsspielraum“ ein. „Dabei kann er insbesondere in den Blick nehmen, inwieweit sich entsprechende Regelungen in die allgemeine Systematik des Strafprozess-

---

[2076] Ausführlich zu den Anforderungen der RL, vgl. oben Kap. S. 143 ff.
[2077] BVerfGE 125, 260 (339).
[2078] *Szuba* 2011, 156.
[2079] S. BVerfGE 35, 202 (220f.); 63, 131 (142f.); 96, 56 (64).
[2080] BVerfGE 73, 118 (210); 97, 125 (146); 99, 185 (194f.).
[2081] BVerfGE 125, 260 (339).

rechts oder des geltenden Haftungsrechts einfügen.“[2082] Auch kann er zunächst beobachten, ob die Rechtsprechung der besonderen Schwere der Persönlichkeitsverletzung durch die unberechtigte Erlangung oder Verwendung von Vorratsdaten auf der Grundlage des geltenden Rechts in der verfassungsrechtlich gebotenen Weise Rechnung trägt.[2083]

Es wird empfohlen, eine Frist zur Einlegung von Rechtsmitteln von vier Wochen ab bekannt werden einzuführen

10.5 Gewährleistung gesellschaftlicher Freiheit – Wahrung des Verbots umfassender gesamtgesellschaftlicher Überwachung

Erstmalig werden mit der Vorratsdatenspeicherung flächendeckend sensitive Daten aller Bürger erhoben, um eventuell in einem späteren Strafverfahren oder zur Gefahrenabwehr auf diese Daten zuzugreifen[2084]. Jedoch ist, so das *Bundesverfassungsgericht,* eine umfassende Erfassung und Registrierung der Freiheitswahrnehmung aller Bürger nicht mit der Identität der Verfassung zu vereinbaren.[2085] Es muss insoweit gewährleistet werden, dass die Vorratsdatenspeicherung weder für sich genommen noch im Zusammenspiel mit anderen Maßnahmen zu einer umfassenden staatlichen Überwachung führt. Erforderlich ist daher die Durchführung einer Überwachungs-Gesamtrechnung. Verlangt wird dafür eine doppelte Verhältnismäßigkeitsprüfung.[2086]

Es ist Pflicht des Gesetzgebers in künftigen Verfahren zu prüfen, ob sich durch die Einführung eines neuen Instruments eine umfassende gesamtgesellschaftliche Überwachung realisiert. Auch die Bundesregierung trifft eine solche Prüfungspflicht soweit sie sich in europäischen und internationalen Zusammenhängen neue Abkommen über Datenerhebungen und -speicherungen abschließt, da auch über den Umweg Europa keine Totalüberwachung eingeführt werden darf.[2087] Dies gilt auch beim Datenaustausch mit Drittstaaten.

Zur Durchführung einer Überwachungs-Gesamtrechnung, ist es erforderlich, das dafür benötigte Datenmaterial verfügbar zu halten.[2088] Insofern bestehen Beobachtungspflichten. Der Gesetzgeber muss dafür Sorge tragen, dass er darüber informiert ist, wie viel der Staat über den einzelnen Bürger ohne spezifische Überwachungsinstrumente weiß. Wichtig ist dafür unter anderem, welche verdachtsgebundenen Maßnahmen zulässig sind und wie häufig diese eingesetzt werden. Dabei muss auch berücksichtigt werden, welche Informationen durch private Unternehmen gespeichert werden, da diese Informationen soweit die entsprechenden Voraussetzungen vorliegen, auch dem Staat übermittelt werden.[2089] Nachkommen kann der Gesetzgeber der Beobachtungs-

[2082] BVerfGE 125, 260 (340).
[2083] BVerfGE 125, 260 (340).
[2084] Zur Definition des Begriffs Vorratsdatenspeicherung, oben S. 139 f.
[2085] BVerfGE 125, 260 (324); vgl. oben S. 156 f.; Kap.7.
[2086] *Roßnagel*, NJW 2010, 1238, 1240; *Roßnagel*, DUD 2010, 544; *Knierim*, ZD 2011, 17, 21 vgl. ausführlich oben Kap. 7.3.
[2087] BVerfGE 125, 260 (324).
[2088] Vgl. dazu oben S. 242 ff.
[2089] Vgl. dazu oben Kap. 7.3.1.

pflicht indem er den Bundesbeauftragten für Datenschutz und Informationsfreiheit mit der Berichterstattung beauftragt. Erforderlich ist dafür auch, dass umfassende Statistiken über Datenabruf und -verwendung durch Polizei und Nachrichtendienste geführt werden. Miteinbeziehen müsste er darüber hinaus Erkenntnisse über private Datenerhebungen und die technischen und sozialen Rahmenbedingungen. Diese Analyse könnte als Teil des vom Bundesbeauftragten für Datenschutz und Informationsfreiheit alle zwei Jahre erstellten Tätigkeitsberichts, der parlamentarischen Kontrolle zugeführt werden (§ 26 Abs. 1 BDSG).[2090]

Neben dieser periodischen Kontrolle, ist ein Zugriff auf die Informationen über den Grad gesamtgesellschaftlicher Überwachung im Gesetzgebungsverfahren erforderlich, soweit neue Überwachungsinstrumente oder staatliche Datenerhebungen eingeführt werden sollen. Wenn hier der maximale Grad gesamtgesellschaftlicher Überwachung durch das neue Instrument überschritten würde, ist der Gesetzgeber gezwungen zwischen den schon vorhandenen Instrumenten und dem neu-einzuführenden abzuwägen und sich für eines von beiden zu entscheiden.[2091] Die Durchführung der Überwachungs-Gesamtrechnung sollte durch die Einführung von Verfahrensvorschriften sichergestellt werden.

Konkret für die Vorratsdatenspeicherung verlangt die Überwachungs-Gesamtrechnung, dass statistische Erhebungen über das Abfrageverhalten und den Erfolg der Datenverwendung durchgeführt werden. Dabei sollte sich eine solche Statistik nicht nur auf die tatsächlichen Abrufe beschränken, sondern auch eine Statistik über den Erfolg der Datenabrufe beinhalten. Dies ermöglicht es nämlich, die Effektivität des Instruments zu bewerten. Dies ist sowohl erforderlich, um die Ausgestaltung der Regelungen optimal an die tatsächlichen sicherheitspolitischen Bedürfnisse anzupassen, als auch um beurteilen zu können, sollte sich eine umfassende gesamtgesellschaftliche Überwachung realisieren, welches Instrument in Bezug auf seinen Beitrag zur Sicherheitsgewährleistung vorzugswürdig ist.[2092] Es ist daher eine statistische Erhebung über den Erfolgswert der verwendeten Daten zu fordern. Dafür müsste von den Ermittlungsbehörden jeweils eine Rückmeldung an die Bundesnetzagentur erfolgen, welche Daten in welchem Verfahren angefordert wurden, ob sie entscheidungserheblich waren und ob sie wesentlich zur Aufklärung beigetragen haben. Dabei sollte in der statistischen Erhebung danach unterschieden werden, ob die Vorratsdaten tatsächlich einen Beitrag zur Aufklärung geleistet haben oder gar kausal für die Aufklärung waren und ob die Straftat ohne die Vorratsdaten nach aktuellem Verfahrensstand unter Berücksichtigung des übrigen verfügbaren Beweismaterials und der sonst noch denkbaren Ermittlungsmaßnahmen definitiv nicht aufzuklären gewesen wäre.

Auch bei der Zusammenarbeit auf europäischer Ebene ist die Bundesregierung verpflichtet, sich dafür einzusetzen, dass eine umfassende gesamtgesellschaftliche Überwachung nicht über den Umweg Europa eingeführt wird. Soweit derartige neue Instrumente eingeführt werden, ist die Bundesregierung bei Abstimmungen im Rat der

[2090] Vgl. dazu oben Kap. 7.3.2.1.
[2091] *Roßnagel*, DuD 2010, 544, 547; *Knierim*, ZD 2011, 17, 21.
[2092] Vgl. dazu oben S. 246.

Europäischen Union, als oberstes, gemäß Art. 1 Abs. 3 GG an die Verfassung gebundenes, Staatsorgan verpflichtet, im Fall einer drohenden Verletzung der Identität der Verfassung durch ausufernde Datensammlungen gegen diese zu stimmen.[2093]

Sodann erwachsen aus der Pflicht sicherzustellen, dass sich keine umfassende gesamtgesellschaftliche Überwachung realisiert, auch Schutzpflichten.[2094] Damit die Vorratsdatenspeicherung „nicht im Zusammenspiel mit anderen vorhandenen Dateien zur Rekonstruierbarkeit praktisch aller Aktivitäten der Bürger" führt muss der Staat unter anderem dafür Sorge tragen, „dass auch die Speicherung der von ihren Kunden aufgerufenen Internetseiten durch kommerzielle Dienstanbieter grundsätzlich untersagt ist".[2095] Er muss insofern zum Schutz des informationellen Selbstbestimmungsrechts der Bürger dafür Sorge tragen, dass eine Vorratsdatenspeicherung nur in einem datenschutzfreundlichen Umfeld erstellt wird, indem Privaten grundsätzlich eine zweckfreie Datensammlung auf Vorrat untersagt ist.

Empfohlen wird, dass der Gesetzgeber durch entsprechende Maßnahmen sicherstellt, dass das für die durchzuführende Überwachungs-Gesamtrechnung erforderliche Informationsmaterial verfügbar ist. Dazu gehören auch Statistiken über das Abrufverhalten und den Erfolg von Abruf und Datenverwendung. Um sicherzustellen, dass vor Einführung neuer Überwachungsinstrumente eine Überwachungs-Gesamtrechnung durchgeführt wird, sind entsprechende Verfahrensvorschriften einzuführen. Eine regelmäßige jährliche Kontrolle des gesamtgesellschaftlichen Überwachungsgrades sollte durch entsprechende Berichtspflichten des Bundesdatenschutzbeauftragten sichergestellt werden.

10.6 Überblick: Vorschläge zur Optimierung des Interessensausgleichs im Rahmen der Vorratsdatenspeicherung

Zur Optimierung des Interessenausgleichs im Rahmen der Vorratsdatenspeicherung konnten verschiedene Gestaltungsvorschläge entwickelt werden. Eine Vielzahl der Vorschläge beschreibt dabei das verfassungsrechtlich erforderliche Minimum und zeugt insofern nicht von einem insgesamt optimalen Interessenausgleich. Es verdeutlicht vielmehr, dass eine Entscheidung für eine Vorratsdatenspeicherung schon dem Grunde nach eine Entscheidung zugunsten der Sicherheit innewohnt. Gerade deshalb sollte sich um einen ansonsten möglichst weitgehenden Interessenausgleich bemüht werden. Der Ausgleichsbedarf ist, da sich bei einer Ausgestaltung der Vorratsdatenspeicherung der Interessenausgleich vielfach an der Grenze zum verfassungsrechtlich zulässigen bewegt, besonders hoch.

Wie eine möglichst verfassungsverträgliche Ausgestaltung einer Vorratsspeicherung gelingen kann, zeigen die hier entwickelten Gestaltungsvorschläge:

- Zur Reduzierung der Eingriffsintensität wird eine Beschränkung der Datenkategorien auf ein Minimum empfohlen.

[2093] *Knierim*, ZD 2011, 17, 22; vgl. dazu ausführlich oben Kap. 7.3.3.
[2094] Dazu oben Kap. 7.2.
[2095] BVerfGE 125, 260 (324); vgl. dazu ausführlich oben Kap. 7.3.2.1.

Dadurch kann der Interessenausgleich zwar optimiert werden, es bleibt aber selbst dann, wenn nur wenige Daten für einen kurzen Zeitraum auf Vorrat gespeichert werden bei einem Ungleichgewicht. Im Sinne eines optimalen Interessenausgleichs, sollte, da die Vorratsspeicherung der Telekommunikationsverkehrsdaten verzichtbar und auch nicht alternativlos ist, eine Vorratsspeicherung sämtlicher Telekommunikationsverkehrsdaten aller Bürger unterbleiben.

Soweit auf europäischer Ebene an einer Verpflichtung zur Vorratsdatenspeicherung festgehalten wird, ist es unter Verhältnismäßigkeitsgesichtspunkten zu empfehlen, zwischen verschiedenen Datenkategorien zu differenzieren. Erforderlich ist zudem eine eindeutige und bestimmte Regelung. Im Hinblick auf die zu speichernden Datenkategorien sollte eine Orientierung am Grundsatz der Erforderlichkeit erfolgen.

- Dies gilt auch für die Speicherfrist – diese ist vom europäischen Gesetzgeber sowie bei der Umsetzung in deutsches Recht so kurz wie möglich zu bemessen. Verfassungsrechtlich zulässig ist es maximal die Verkehrsdaten für sechs Monate zu speichern. Dabei liegt es nahe entsprechend der Bedeutung der Daten für die Arbeit der Ermittlungsbehörden und im Hinblick auf das Eingriffsgewicht der Erhebung der jeweiligen Verkehrsdaten zwischen verschiedenen Datenkategorien zu unterscheiden. Die Daten sind möglichst unmittelbar (innerhalb von einer Woche) und vollständig nach Ablauf der Speicherfrist zu löschen.
- Die Auswahl der Adressaten sollte auf die Bundesnetzagentur übertragen werden, die diese nach dem Grundsatz des „Cheapest Cost Avoider“ auswählt und die Speicherungspflicht dann durch Verwaltungsakt begründet. Dabei sollte sichergestellt werden, dass die Unternehmen die Speicherungsverpflichtung im eigenen Konzern durchführen.
- Zwingend erforderlich ist die Gewährleistung eines besonders hohen Sicherheitsstandards. Die Anforderungen sollten in technischen Richtlinien von der Bundesnetzagentur konkretisiert und regelmäßig den technischen Entwicklungen angepasst werden. Wichtig ist auch eine regelmäßige Kontrolle der Sicherheitsvorkehrungen durchzuführen und Sanktionen für den Fall der Missachtung einzuführen.
- Die Investitions- Betriebs- und Abrufkosten sollten den verpflichteten Anbietern zu 80 Prozent erstattet werden.
- Zur Gewährleistung des verfassungsrechtlich gebotenen Schutzes von Vertrauensbeziehungen wird ein dreistufiges Schutzsystem empfohlen. Soweit möglich sollten die Verkehrsdaten von Berufsgeheimnisträger auf einer ersten Stufe grundsätzlich von der Speicherung ausgenommen werden. In einer zweiten Stufe sollten, die Daten vor der Übermittlung an staatliche Stellen gefiltert werden.

Schließlich greift als dritte Stufe ein Beweisverwertungsverbot, sollten auf Vorrat gespeicherte Verkehrsdaten dem Geheimnisschutz unterfallen.

- In Bezug auf die Datenübermittlung wird für die Optimierung des Interessensausgleichs empfohlen, dass diese zentralisiert erfolgt und zwar über die Bundesnetzagentur. Der Abruf sollte allein auf elektronischem Wege über ein besonders gesichertes System und mit einer anspruchsvollen Verschlüsselung erfolgen.
- Abrufberechtigt sollten nur Strafverfolgungs- und Gefahrenabwehrbehörden sein. Im Rahmen der Strafverfolgung sollte der Zugriff auf die Vorratsdaten nur zur Verfolgung besonders schwerer Straftaten zugelassen werden. Empfohlen wird die Straftaten in einem Straftatenkatalog zu spezifizieren und mit einer Mindestanforderung an den Strafrahmen zu verknüpfen. Für Zwecke der Gefahrenabwehr ist der Zugriff auf die Daten zur Abwehr von Gefahren für Leib, Leben oder Freiheit einer Person, für den Bestand oder die Sicherheit des Bundes oder eines Landes oder zur Abwehr einer gemeinen Gefahr zu beschränken. Dabei ist der Abruf nur bei Vorliegen einer konkreten Gefahr zulässig. In Ausnahmefällen kann schon im Vorfeld einer konkreten Gefahr auf die Daten zugegriffen werden, wenn Tatsachen Rückschlüsse auf ein wenigstens seiner Art nach konkretisiertes und zeitlich absehbares Geschehen zulassen und eine Konzentration der Maßnahme auf bestimmte Personen möglich ist. Neben Strafverfolgungs- und Gefahrenabwehrbehörden sollte Nachrichtendiensten keine Ermächtigung zum Abruf der Daten eingeräumt werden.
- Mittels rechtlicher und organisatorischer Maßnahmen ist sicherzustellen, dass sich der Datenabruf auf den jeweils unbedingt erforderlichen Teil beschränkt.
- Die Weitergabe von Daten und aus ihnen gewonnen Informationen ist nur zulässig, soweit der Zweckbindungsgrundsatz gewahrt wird. Eine mittelbare Verwendung von Vorratsdaten für niederschwellige Delikte ist zu untersagen.
- Der Datenabruf ist grundsätzlich präventiv richterlich zu prüfen. Nur bei Gefahr im Verzug kann ausnahmsweise die Staatsanwaltschaft den Abruf anordnen. Die richterliche Prüfung muss dann umgehend nachgeholt werden. Um die Effektivität des Schutzinstruments sicherzustellen, sollten verbindliche Regelungen für den Umfang und das Verfahren vorgegeben werden.
- Auch für die Aufbewahrung und Verarbeitung der Daten bei staatlichen Behörden sind umfassende Regelungen zu treffen, die die Zweckbindung, Datensicherheit und unverzügliche Auswertung der Daten sicherstellen.
- Die Übermittlung der Vorratsdaten ins Ausland sollte grundsätzlich unter Richtervorbehalt gestellt werden. Eine Übermittlung darf nur erfolgen, soweit die Zweckbindung gewährleistet ist. Auch die Datensicherheit muss beachtet werden.

- Grundsätzlich sollte der Abruf der Daten offen erfolgen, es sei denn der Zweck der Maßnahme wird dadurch gefährdet. Der heimliche Zugriff sollte gesondert beim Richter beantragt werden. Eine nachträgliche Benachrichtigung sollte möglichst umgehend erfolgen. Wenn sie nicht innerhalb von sechs Monaten nachgeholt wurde, ist dies richterlich zu prüfen. Im Anschluss daran sollte eine Frist zur Einlegung von Rechtsmitteln von vier Wochen ab Bekanntwerden eingeführt werden.
- Der Gesetzgeber hat sicherzustellen, dass das für die Überwachungs-Gesamtrechnung erforderliche Datenmaterial verfügbar ist. Dafür sind auch Statistiken über den Datenabruf einzuführen. Es ist eine regelmäßige jährliche Kontrolle des gesamt-gesellschaftlichen Überwachungsgrades vorzusehen, die durch entsprechende Berichtspflichten des Bundesdatenschutzbeauftragten sichergestellt werden könnte.

11 Optimierung des Interessenausgleichs im Rahmen der Vorratsdatenspeicherung

Es wurde aufgezeigt, dass mittels einer umfassenden verfassungsrechtlichen Analyse der bei der Vorratsdatenspeicherung zu Tage tretende Interessenkonflikt durch rechtliche, technische und organisatorische Gestaltungsmaßnahmen abgemildert werden kann. Es kann durch entsprechende Vorkehrungen dafür gesorgt werden, dass die Interessenkollision auch im Rahmen einer Vorratsspeicherung sämtlicher Telekommunikationsverkehrsdaten aller Bürger im Sinne praktischer Konkordanz aufgelöst werden kann. Allerdings wurde auch deutlich, dass bereits die Entscheidung für eine Vorratsdatenspeicherung an sich eine Entscheidung für Sicherheit ist, die als solche schon ein Ungleichgewicht, welches es durch besondere rechtliche, technische und organisatorische Gestaltungsinstrumente auszugleichen gilt, provoziert. Denn sie ist durchaus verzichtbar und auch nicht alternativlos im Sinne der Verhältnismäßigkeitsprüfung Plus.[2096]

Eine Vorratsdatenspeicherung bewegt sich nicht nur deswegen, sondern vor allem auch, weil es sich um ein Sicherheitsinstrument neuer Qualität mit hohem Eingriffsgewicht handelt, immer an der Grenze zur Verfassungswidrigkeit. Dies zeigt sich daran, dass sie nur maximal für sechs Monate zulässig ist. Gerade deshalb ist die konkrete Ausgestaltung von so großer Bedeutung.

Beachtlich für die Ausgestaltung ist, die Erkenntnis, dass nur mit Hilfe von Technikgestaltung eine verhältnismäßige Ausgestaltung der Vorratsdatenspeicherung gelingen kann.[2097] Auch für die Optimierung des Interessenausgleichs ist diese von besonderer Bedeutung. IT-Sicherheit ist eine der Stellschrauben mit der das Gewicht von Eingriffen in die informationelle Selbstbestimmung (bzw. im Fall der Vorratsdatenspeicherung in das Telekommunikationsgeheimnis und in dessen datenschutzrechtlichen Kern) verringert werden können.[2098] Je stärker in die Telekommunikationsfreiheit oder das Grundrecht auf informationelle Selbstbestimmung eingegriffen wird, desto höher muss der Schutz der erhobenen Daten ausfallen.[2099] Entsprechend ist in Fällen besonders schwerwiegender Grundrechtseingriffe, wie im Fall der Vorratsdatenspeicherung, für die Verhältnismäßigkeit des Eingriffs die Gewährleistung eines besonders hohen Standards der Datensicherheit geboten.[2100]

[2096] Andere bewerten sie als „objektiv unzumutbar", so etwa *Hornung,* PVS 2012, 377, 394 f. m.w.Nachw.

[2097] So auch im Urteil des *BVerfG* zur Vorratsdatenspeicherung, BVerfGE 125, 260 (LS 2).

[2098] *Kloepfer* bezeichnet dies als „verfassungsoptimierende Technikgestaltung" und erkennt an, dass „staatliche(n) Schutzpflichten gegenüber Eingriffen Dritter in besonders geeigneter Weise durch rechtliche Anforderungen an technische Voraussetzungen" umgesetzt werden könnten, so *Kloepfer,* Verfassungsrecht II 2010, § 65 Rn. 56.

[2099] Die Eingriffsintensität bestimmt das *BVerfG* anhand der Streubreite der Datenerhebung, dem Missbrauchsrisiko und der Aussagekraft bzw. den Analyse- und Verwendungsmöglichkeiten der Daten, vgl. dazu oben S. 274 ff.

[2100] *Britz,* JA 2011, 81.

A. Moser-Knierim, *Vorratsdatenspeicherung,* DuD-Fachbeiträge,
DOI 10.1007/978-3-658-04156-4_11, © Springer Fachmedien Wiesbaden 2014

Es ist allerdings darauf hinzuweisen, dass selbst ein besonders hoher Sicherheitsstandard zwar normiert werden kann, aber es zu dessen Durchsetzung und ständiger Aktualisierung weiterer umfassender rechtlicher und organisatorischer Maßnahmen bedarf. Und auch diese können letztlich nie eine vollständige Sicherheit garantieren. So sind Verschlüsselungsalgorithmen etwa nur bis zu dem Zeitpunkt sicher, bis sie geknackt wurden. Auch ein Vier-Augen-Prinzip birgt keinen Schutz, wenn zwei zusammenwirken, etc. Daher ist gerade im Hinblick auf die Notwendigkeit technischer Sicherheitsvorkehrungen bei großen Datensammlungen der Grundsatz der Erforderlichkeit zu betonen.[2101]

Es sollte daher stets genau geprüft werden, ob eine Datenerhebung tatsächlich erforderlich ist. Denn am sichersten sind nur die Daten, die gar nicht erst erhoben werden und auf keinem Datenträger gespeichert werden.[2102] Entsprechend ist so unter Gesichtspunkten informationeller Selbstbestimmung jede Maßnahme vorzugswürdig, die eine Datenerhebung und -sammlung vermeidet. Wenn allerdings eine Entscheidung für eine Datenerhebung und Speicherung gefällt wird, ist es entscheidend, dass entsprechende technische und organisatorische Sicherheitsvorkehrungen getroffen werden.

Diese Erwägungen sollten auch im Diskurs um die Vorratsdatenspeicherung berücksichtigt werden. Und zwar sowohl bei den rechtspolitischen Entscheidungen auf europäischer wie auf nationaler Ebene. Für den Bundesgesetzgeber besteht aktuell eine Umsetzungspflicht der Vorratsdatenspeicherungsrichtlinie. Insofern ist er gehalten, wenn er die Richtlinie umsetzt, sie möglichst grundrechtsschonend und also entsprechend der in Kap. 10 entwickelten Gestaltungsvorschläge einzuführen.

Für die Diskussion auf europäischer Ebene, gilt hingegen, dass hier der Bundesgesetzgeber, genauer dessen Vertretung im Europäischen Rat, dazu verpflichtet darauf hin zu wirken, dass die Richtlinie im Sinne eines optimierten Interessenausgleichs überarbeitet wird. Dabei sollte berücksichtigt werden, dass die Kosten einer Vorratsdatenspeicherung sehr hoch sind, diese nicht auf die Telekommunikationsanbieter abgewälzt werden sollten und sowohl der Umfang der Speicherungsverpflichtung als auch die Verwendungszwecke auf ein Minimum zu begrenzen wären.

Zu erwägen ist daher, ob nicht in Anbetracht dieser Punkte und der bevorstehenden technologischen Entwicklungen – der vollständigen Umstellung auf IPv6, die in vielen Teilen eine Vorratsdatenspeicherung überflüssig machen wird – ein Verzicht auf eine Verpflichtung zur Speicherung sämtlicher Telekommunikationsverkehrsdaten auf Vorrat geboten ist. Dies gilt auch im Hinblick auf die durchzuführende Überwachungs-Gesamtrechnung. Denn mit der Einführung einer Vorratsspeicherung der Telekommunikationsverkehrsdaten wird der gesetzgeberische Spielraum für weitere Sicherheitsinstrumente stark reduziert.

[2101] Im Volkszählungsurteil hat das *Bundesverfassungsgericht* festgestellt: „alle Stellen, die zur Erfüllung ihrer Aufgaben personenbezogene Daten sammeln, auf das zum Erreichen des angegebenen Zieles erforderliche Minimum beschränken müssen." BVerfGE 65, 1 (46), vgl. zum Grundsatz der Erforderlichkeit, oben S. 88.

[2102] *Roßnagel/Scholz,* MMR 2000, 721 f.

Schlussbemerkung

Die Speicherung von Telekommunikationsverkehrsdaten auf Vorrat ist weder ein unentbehrliches Instrument zur Terrorprävention, noch ist sie Schritt in den Überwachungsstaat. Der Diskurs um die Vorratsdatenspeicherung ist in dieser Hinsicht, das hat diese Untersuchung gezeigt, stark emotionalisiert. Auf der anderen Seite lassen sich in diesen Emotionen die durchaus berechtigten Sorgen von Gegnern und Befürwortern der Vorratsdatenspeicherung ausmachen.

So ist die Vorratsdatenspeicherung zwar nicht unentbehrlich für die Sicherheitsgewährleistung, ihr kommt aber unter den Bedingungen digitaler Datenverarbeitung eine besondere Bedeutung zu. Denn solange und soweit Datenschutz und Technik dazu führen, dass Verbindungsdaten nur eingeschränkt gespeichert werden, sich aber auf der anderen Seite Straftaten immer mehr ins Netz verlagern, bedarf es einer Vorratsdatenspeicherung der Verbindungsdaten, um Anknüpfungspunkte für die Aufklärung gewisser Straftaten zu gewinnen. Die Vorratsdatenspeicherung ist darüber hinaus ein viel-versprechendes Instrument für Ermittlungsbehörden, um Informationen über Verdächtige, ihr Umfeld und ihr Verhalten zu gewinnen.

Auf der anderen Seite ist die Besorgnis der Gegner einer Vorratsdatenspeicherung berechtigt, die in ihr den Damm auf dem Weg in den Überwachungsstaat gebrochen sehen. Denn ihr wohnt als anlasslose Infrastruktur ein erhebliches Einschüchterungspotential inne. Auf Grund der Möglichkeit, das Leben eines jeden Bürgers mit der Auswertung von auf Vorrat gespeicherten Telekommunikationsdaten umfassend zu rekonstruieren, kann ein Gefühl der Überwachung entstehen. Dies gilt insbesondere, wenn die Erhebung nicht begrenzt und eine missbräuchliche Verwendung der Daten zu befürchten ist. Die Vorratsdatenspeicherung führt jedoch nicht unmittelbar zur Überwachung eines jeden Bürgers. Es wird „lediglich“ die Infrastruktur dafür geschaffen. Wenn eine Vorratsdatenspeicherung eingeführt wird, entsteht die Möglichkeit, jeden Bürger zu überwachen. Eine solche Überwachungsstruktur, bei der tatsächlich das Verhalten eines jeden Bürgers überwacht und kontrolliert wird, wäre mit der freiheitlich-demokratischen Grundordnung und dem Rechtsstaatsprinzip nicht vereinbar. Entsprechend muss der Zugriff auf die Daten begrenzt werden. Zudem darf die Schaffung solcher Infrastrukturen nicht zum politischen Konzept werden: anlasslose Datensammlungen auf Vorrat sind vielmehr nur als Ausnahme zulässig.

Es ist somit erforderlich, die Vorratsdatenspeicherung durch rechtliche, technische und organisatorische Maßnahmen so zu beschränken, dass ihre konkrete Ausgestaltung verhältnismäßig ist. Denn eine umfassende gesamtgesellschaftliche Überwachung ist mit der Identität der Verfassung nicht vereinbar, dies hofft diese Arbeit belegt zu haben.

Da es sich bei der Vorratsdatenspeicherung um einen von vielen Schritten handelt, mit welchen die Sicherheitsvorsorge weiter ausgedehnt wird und Freiheitsräume zunehmend eingeschränkt werden, kommt Maßnahmen zur Wahrung des Verbots umfassender gesamtgesellschaftlicher Überwachung besondere Bedeutung zu. Denn es hat sich

A. Moser-Knierim, *Vorratsdatenspeicherung,* DuD-Fachbeiträge,
DOI 10.1007/978-3-658-04156-4, © Springer Fachmedien Wiesbaden 2014

gezeigt, dass klassische Schranken-Schranken im Angesicht der erheblichen (als solches kommunizierten) Bedrohungen durch den internationalen Terrorismus und der Überlagerung nationalen Rechts durch europäisches Recht, nicht geeignet sind, die fortschreitende Einschränkung von verfassungsrechtlich garantierten Freiheiten zu verhindern. Legislative, Exekutive und Judikative sind daher aufgerufen, das Verbot umfassender gesamtgesellschaftlicher Überwachung zu beachten, zu dessen Konkretisierung hier Vorschläge entwickelt wurden.

Für die konkrete Umsetzung der Vorratsdatenspeicherungsrichtlinie muss, neben der Einführung von Evaluations- und Informationspflichten bezüglich des Grads gesamtgesellschaftlicher Überwachung, der Umfang der Datenerhebung (maximal sechs Monate, möglichst wenig Daten) und ihre Verwendung (nur zur Verfolgung und Verhinderung besonders schwerer Straftaten/Gefahren) begrenzt werden. Schließlich müssen, um die Einschüchterungswirkung zu verringern, Transparenz- und Rechtsschutzmaßnahmen vorgesehen werden.

In dieser Arbeit sind Gestaltungsmöglichkeiten für eine möglichst grundrechtsschonende Umsetzung der Vorratsdatenspeicherungsrichtlinie entwickelt worden. Deutlich wird dabei allerdings auch, dass der Gestaltungsspielraum des Gesetzgebers bei der Umsetzung der Vorratsdatenspeicherungsrichtlinie stark reduziert ist. Die Vorratsdatenspeicherungsrichtlinie kann deutlich grundrechtsschonender umgesetzt werden. Ein optimierter Interessenausgleich ist möglich, sie bewegt sich jedoch in weiten Teilen an der Grenze zur Verfassungswidrigkeit und ist verfassungsrechtlich zwingend determiniert. Hier kann daher nicht von einem optimalen Ausgleich gesprochen werden. Die Vorratsdatenspeicherung ist nicht alternativlos und auch nicht zwingend erforderlich zur Gewährleistung der Sicherheit.

Insofern sind die entwickelten Gestaltungsvorschläge auch nicht als Plädoyer für eine Vorratsdatenspeicherung zu verstehen. Es wird damit allein die Frage beantwortet, wie eine Umsetzung der Vorratsdatenspeicherungsrichtlinie gelingen kann unter Berücksichtigung des unter den Bedingungen digitaler Datenverarbeitung verschärften Spannungsverhältnisses zwischen Freiheits- und Sicherheitsinteressen.

Was die Frage betrifft, ob es überhaupt einer Vorratsdatenspeicherung bedarf, ist zu betonen, dass auch ohne Vorratsdatenspeicherung kein rechtsfreier Raum entsteht. Auch wenn in manchen Bereichen die Strafverfolgung und Gefahrenabwehr, ohne auf diese Daten zugreifen zu können, erschwert wird. Es sind aber vielfach entsprechende Daten auch ohne Vorratsdatenspeicherung vorhanden. Und auch wenn eine generelle Vorratsdatenspeicherung eingeführt wird, kann nicht davon ausgegangen werden, dass künftig die Informationen in Bezug auf alle Beschuldigten, Straftaten und Straftäter, Verdächtige und Gefahrenlagen gespeichert wären. Vielmehr werden dann, jedenfalls intelligente, Straftäter auf andere Kommunikationswege ausweichen. Dem Mehr an Daten, das durch eine Vorratsdatenspeicherung Strafverfolgung und Gefahrenabwehr zur Verfügung steht, stehen eine intensive Freiheitsbeeinträchtigung der Bürger, eine beschränkte Verwendbarkeit der Daten, hohe Kosten und ein schwerwiegender Eingriff in die Wirtschaft gegenüber. Insofern gibt es triftige Gründe gegen eine Vorratsspeicherung der Telekommunikationsverkehrsdaten.

Ein weiterer Grund, der die Erforderlichkeit einer Neueinführung der Vorratsdatenspeicherung in Frage stellt, ist, dass mit der Umstellung auf IPv6 zukünftig im Bereich der Internetkommunikation deutlich leichter Kennungen einem Anschlussinhaber zugeordnet werden können. Hier bestehen aktuell noch größere Schutzlücken.

Schließlich gilt es zu bedenken, dass der gesetzgeberische Spielraum in Bezug auf die Einführung neuer anlassloser Datensammlungen auf Vorrat, wenn eine Entscheidung für die Vorratsspeicherung der Telekommunikationsverkehrsdaten gefällt werden sollte, quasi auf null reduziert wäre. Denn eine anlasslose Datensammlung auf Vorrat ist nur als Ausnahme zulässig. Telekommunikationsverkehrsdaten und PNR-Daten dürften etwa nicht parallel anlasslos auf Vorrat gespeichert werden. Neben dieser Einschränkung der Gesetzgebungsprärogative wäre sie auch ansonsten durch den stark verdichteten Grad gesamtgesellschaftlicher Überwachung verringert.

Die Entscheidung für eine Vorratsdatenspeicherung oder gegen sie ist aber im Kern eine politische Entscheidung. Die Beantwortung dieser Frage stand nicht im Zentrum dieser Arbeit. Die Erkenntnisse konnten jedoch im Zuge der Suche nach einem bestmöglichen Ausgleich gewonnen werden. Und sie sind derzeit insbesondere für die ausstehende Überarbeitung der Richtlinie auf europäischer Ebene relevant.

Die europäische Kommission überarbeitet aktuell die Richtlinie. In diesem Zuge ist sie dazu aufgerufen, sich die Frage zu stellen, ob in Anbetracht der aufgeführten Argumente eine Harmonisierung der Speicherung der Telekommunikationsverkehrsdaten geboten ist. Wenn dieses Ziel weiterhin verfolgt werden sollte, müsste jedenfalls, um tatsächlich eine Harmonisierung zu erreichen, der Regelungsinhalt der Richtlinie stark ausgeweitet werden.

In dieser Hinsicht gilt es zu beachten, dass nicht allein die Europäische Kommission Adressat der Vorschläge ist. Auch die Bundesregierung ist verpflichtet sich auf europäischer Ebene für die Wahrung der Identität der Verfassung und insofern für die Beachtung des Verbots einer umfassenden gesamtgesellschaftlichen Erfassung und Registrierung einzusetzen.

Die Untersuchung hat gezeigt, dass sich das Spannungsverhältnis von Freiheit und Sicherheit im Angesicht von Digitalisierung, Globalisierung und einer Ausweitung des Sicherheitsdogmas verschärft hat. Das Grundgesetz kann hier zwar einen Ausgleich schaffen. Der Überwachungsstaat wird nicht mit der Vorratsdatenspeicherung über den Umweg Europa eingeführt. Doch die Tendenz zu einer immer weiteren Einschränkung von Freiheitsräumen ist deutlich.

Wie scharf Freiheits- und Sicherheitsinteressen heute kollidieren, hat sich ganz aktuell im NSA-Skandal gezeigt. In der Bundesrepublik ist seitdem die Forderung nach der Neueinführung der Vorratsdatenspeicherung (vorerst) verstummt. Jedoch zeigt sich in der Praxis der Geheimdienste ihr Interesse möglichst alles über jeden Bürger zu speichern. Dass dies mit der Identität der Verfassung nicht vereinbar ist, zeigt nicht erst die hier vorgenommene Konkretisierung des Verbots totaler Erfassung und Registrierung.

Ich hoffe jedoch, dass die vorgelegte Arbeit einen Beitrag zu der Diskussion leisten kann, wie in Deutschland, Europa und weltweit in Zukunft Freiheit und Sicherheit gewährleisten können. Dass es dafür von grundlegender Bedeutung ist, sicherzustellen, dass sich eben keine umfassende gesamtgesellschaftliche Überwachung realisiert, hoffe ich, überzeugend dargelegt zu haben. Dazu, wie dies gelingen könnte, habe ich erste Vorschläge gemacht.

Wesentlich dafür ist neben der Prüfung durch Gesetzgeber, Judikative und Exekutive auch das gesamtgesellschaftliche Bewusstsein für die Möglichkeit der Überwachung durch die Digitalisierung des Alltags. Die Wahrung der freiheitlichen Grundordnung als Bestandteil der Identität der Verfassung verbietet es Sicherheit absolut zu setzen und insofern Freiheit im Namen der Sicherheit grundsätzlich aufzugeben. Sicherheit ist ein Staatziel von herausragender Bedeutung. Aber letztlich muss Sicherheit dazu dienen, die Freiheit der Bürger zu ermöglichen. Das Grundgesetz beschreibt eine freiheitliche Grundordnung. Diese ist auch unter den Bedingungen digitaler Datenverarbeitung und im Angesicht neuer Bedrohungslagen zu schützen. Eine umfassende gesamtgesellschaftliche Überwachung verbietet die Identität der Verfassung. Die Arbeit hofft mit Vorschlägen, wie dieses Verbot gewahrt und der Ausgleich zwischen Freiheits- und Sicherheitsinteressen optimiert werden kann, einen Beitrag dazu geleistet zu haben, wie Freiheit und Sicherheit im digitalen Zeitalter in einen verfassungsverträglichen Ausgleich gebracht werden können.

Thesen

1. Freiheit und Sicherheit stehen in einem natürlichen Spannungsverhältnis zueinander.

2. Technisierung, Globalisierung und veränderte Bedrohungslagen haben in der Gesellschaft einen Eindruck der Verwundbarkeit herbeigeführt, welcher Sicherheitsbestrebungen den Weg ebnet.

3. Die Verabschiedung der Vorratsdatenspeicherungsrichtlinie ist Ergebnis einer erfolgreichen Ver(un-)sicherheitlichung.

4. Kommunikation ist zentraler Bestandteil aller grundgesetzlich garantierten Freiheiten. Durch die Digitalisierung der Kommunikation rückt die Telekommunikationsfreiheit ins Zentrum der Diskussion um die Gewährleistung von Freiheit und Sicherheit.

5. Die Verfassung bestimmt das Verhältnis von Freiheit und Sicherheit nicht abschließend. Es ist aber geprägt durch die Grundrechte in ihrer Funktion als Abwehrrechte. Das Verhältnis von Freiheit und Sicherheit kann als Sicherheit *für* Freiheit formuliert werden.

6. Ein im Sinne der Verfassung bestmöglicher und damit auch verfassungsverträglicher Ausgleich von Freiheits- und Sicherheitsinteressen verlangt, dass diese in einen praktisch konkordanten Ausgleich zueinander gebracht werden. Wobei Sicherheitsmaßnahmen immer Freiheitssichernde Funktion haben müssen.

7. Die Ausweitung der Sicherheitsvorsorge im Kampf gegen den internationalen Terrorismus zu Beginn des 21. Jahrhunderts stellt die verfassungsrechtliche Garantie einer freiheitlichen Grundordnung in Frage.

8. Die Einführung der Vorratsdatenspeicherung(-srichtlinie) steht paradigmatisch für das Kollisionsverhältnis von Freiheits- und Sicherheitsinteressen im digitalen Zeitalter.

9. Die Diskussion um die Vorratsdatenspeicherung ist stark emotionalisiert und vielfach polemisch: weder kann sie zwingend als „Dammbruch auf dem Weg in den Überwachungsstaat“ gesehen werden noch wird das Internet ohne sie zum rechtsfreien Raum.

10. Die Vorratsdatenspeicherung ist als infrastrukturelle Überwachungsmaßnahme ein Sicherheitsinstrument neuer Qualität.

A. Moser-Knierim, *Vorratsdatenspeicherung,* DuD-Fachbeiträge,
DOI 10.1007/978-3-658-04156-4, © Springer Fachmedien Wiesbaden 2014

11. Neue Herausforderungen für einen schonenden Ausgleich zwischen Freiheits- und Sicherheitsinteressen stellen sich zum einen, da klassische Grundrechtsschranken wegen des Umfangs der Datenerfassung leer laufen. Zum anderen ergeben sich auf Grund der Überlagerung durch europäisches (supranationales) Recht neue Herausforderungen für die Verfassungsordnung.

12. Absolute Grenzen stellen neben Verhältnismäßigkeit und Bestimmtheitsgebot, die Schranken staatlichen Sicherheitsstrebens dar. Sie werden in der Praxis jedoch relativ bestimmt. Absolute Verbote können zu Hohlformeln werden, wenn sie nicht konkretisiert werden.

13. Das vom Bundesverfassungsgericht aus der Identität der Verfassung abgeleitete Verbot totaler Erfassung und Registrierung der Freiheitswahrnehmung aller Bürger ist als Verbot einer umfassenden gesamtgesellschaftlichen Überwachung auszulegen.

14. Erforderlich ist in Zukunft eine doppelte Verhältnismäßigkeitsprüfung,. Den Gesetzgeber treffen Evaluations- und Beobachtungspflichten.

15. Anlasslose, flächendeckende Datenerhebungsinstrumente sind nur als Ausnahme zulässig.

16. Eine Vorratsspeicherung sowohl von Telekommunikations- als auch von Fluggastdaten auf Vorrat, würde das Verbot umfassender Erfassung und Registrierung verletzen.

17. Sollte sich eine politische Mehrheit für eine Vorratsdatenspeicherung finden, bzw. die Richtlinie weiter fortbestehen, kann eine Vorratsdatenspeicherung verfassungskonform ausgestaltet werden. Allerdings bewegt sie sich an der Grenze zur Verfassungswidrigkeit.

18. Wegen des hohen Eingriffsgewichts einer Vorratsdatenspeicherung sollte der Gesetzgeber eine Optimierung des Interessenausgleichs bei der Ausgestaltung der Maßnahme anstreben.

19. Ein optimierter Ausgleich zwischen Freiheits- und Sicherheitsinteressen kann ermittelt werden, indem die klassische Verhältnismäßigkeitsprüfung ergänzt wird: zunächst ist zu fragen, ob auf die Maßnahme verzichtet werden kann, ohne dass die Zweckerreichung grundsätzlich in Frage gestellt wird. Die Prüfung der Erforderlichkeit ist zu relativieren, indem danach gefragt wird, ob es ein entsprechend geeignetes Instrument gibt, das grundrechtsschonender das gleiche Ziel verfolgt. Im Rahmen der Angemessenheit ist schließlich umfassend zu

analysieren, welche Rechtspositionen betroffen sind. Es ist dann zu fragen, wie hoch der Beitrag der Maßnahme für Freiheit und Sicherheit jeweils ist.

20. Die Vorratsdatenspeicherung ist verzichtbar und auch nicht alternativlos. Quick-Freeze ist im Hinblick auf die Freiheitsrechte der Bürger eine grundrechtsschonendere Alternative, die die Gewährleistung von Sicherheit nicht grundsätzlich in Frage stellt.

21. Wenn die politische Entscheidung für eine Vorratsdatenspeicherung getroffen wird, kann diese verfassungsverträglich ausgestaltet werden. Erforderlich dafür sind jedoch umfassende, zahlreiche rechtliche, technische und organisatorische Maßnahmen, welche insgesamt sehr hohe Kosten verursachen.

22. Der Zweckbindungsgrundsatz ist für die Rechtfertigungsfähigkeit der Vorratsdatenspeicherung von besonderer Bedeutung. Eine mittelbare Nutzung der auf Vorrat gespeicherten Verkehrsdaten für niederschwellige Delikte scheidet daher aus.

Literaturverzeichnis

AK-Vorratsdatenspeicherung, *Netzwerk Neue Medien e.V., Neue Richtervereinigung e. V*, Stellungnahme zum Regierungsentwurf für ein Gesetz zur Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen sowie zur Umsetzung der Richtlinie 2006/24/EG v. 6.9.2007; abrufbar unter: http://webarchiv.bundestag.de/archive/2007/1105/ausschuesse/a06/anhoerungen/24_TKUE_Vorratsdatenspeicherung/04_Stellungnahmen/Stellungnahme_Breyer.pdf;
zitiert als *AK-Vorrat et al.,* 2007, S.

Albers, M., Informationelle Selbstbestimmung, 1. Auflage, Baden-Baden 2005;
zitiert als *Albers* 2005, S.

Albrecht, F., Mangelnde Unabhängigkeit der deutschen behördlichen Datenschutzbeauftragten, jurisPR-ITR 15/2010, Anm. 4.

Albert, H.-J., Das "Trennungsgebot" - ein für Polizei und Verfassungsschutz überholtes Entwicklungskonzept?, ZRP 1995, 105.

Albrecht, H.-J./ Grafe, A./ Kilchling, M., Rechtswirklichkeit der Auskunftserteilung über Telekommunikationsverbindungsdaten nach §§ 100g, 100h StPO, Forschungsbericht im Auftrag des Bundesministerium der Justiz. Berlin 2008;
zitiert als *Albrecht/Grafe/Kilchling* 2008, S.

Albrecht, H.-J., *Kilchling, M., u.a.* Schutzlücken durch Wegfall der Vorratsdatenspeicherung, Eine Untersuchung zu Problemen der Gefahrenabwehr und Strafverfolgung bei Fehlen gespeicherter Telekommunikationsverkehrsdaten, Gutachten des Max-Planck-Instituts für ausländisches und internationales Strafrecht, im Auftrag des Bundesministerium der Justiz, abrufbar unter: http://www.bmj.de/SharedDocs/Downloads/DE/pdfs/20120127_MPI_Gutachten_VDS_Langfassung.pdf?__blob=publicationFile,
zitiert als *Albrecht/Kilchling* 2011, S.

Albrecht, P.-A., Der Weg in die Sicherheitsgesellschaft, Auf der Suche nach staatskritischen Absolutheitsregeln. Berlin 2010;
zitiert als *Albrecht* 2010a.

Albrecht, P.-A., Die Entwicklung der Erosionen zentraler Rechtsprinzipien, in: Von der Rationalität des Rechts in die Irrationalität der Sicherheit, Reflexionen über Widerstandsformen in Sicherheitsgesellschaften, KritV 2010, 137.

Albrecht, P.-A., Die Polizei auf dem Weg zur Geheimpolizei, Staatliche Interessen verdrängen den Rechtsschutz des Bürgers, Deutschlandradio Kultur v. 16.2.2012; abrufbar unter: http://www.dradio.de/dkultur/sendungen/politischesfeuilleton/1678188/;
zitiert als *Albrecht* 16.2.2012.

A. Moser-Knierim, *Vorratsdatenspeicherung,* DuD-Fachbeiträge,
DOI 10.1007/978-3-658-04156-4, © Springer Fachmedien Wiesbaden 2014

Albrecht, P.-A., Vom Präventionsstaat zur Sicherheitsgesellschaft, Wege kontinuierlicher Erosion des Rechts, in: *Herzog, F./ Hassemer, W.* (Hrsg.), Festschrift für Winfried Hassemer, Heidelberg 2010, 3;
zitiert als *Albrecht* 2010b.

Alexy, R., Theorie der Grundrechte. Frankfurt am Main 1986.

Alpar, P./ Blaschke, S., Web 2.0 - Eine empirische Bestandsaufnahme, 1. Auflage, Wiesbaden 2008.

Alvaro, A., Die Richtlinie zur Vorratsdatenspeicherung, DANA 2006, 52.

Alvaro, A., Positionspapier zur Einführung der Vorratsdatenspeicherung von Daten, RDV 2005, 47.

Ambos, K., Entscheidungsanmerkung zum Urt. des EuGH v. 10.2.2009, JZ 2009, 468.

Ambs, R., Kommentierung § 12 BDSG in: *Erbs, G./ Kohlhaas, M.* (begr. v.) Strafrechtliche Nebengesetze, München 2012;
zitiert als *Ambs,* in: *Erbs/Kohlhaas,* 2012, § Rn.

Amelung, K., Die zweite Tagebuchentscheidung des BVerfG, NJW 1990, 1753.

Antoni, M., Kommentierung Vorbemerkung vor Art. 1 in: *Hömig, D.* (Hrsg.), Grundgesetz für die Bundesrepublik Deutschland, Kommentar. München, 2007;
zitiert als *Antoni,* in: *Hömig,* GG Komm 2007, Rn.

Arndt, H.-W., Gleichheit im Steuerrecht, NVwZ 1988, 787.

Arndt, H.-W./ Schumacher, A., Die verfassungsrechtlich zulässige Höhe der Steuerlast – Fingerzeig des BVerfG an den Gesetzgeber?, NJW 1995, S. 2603.

Arning, M./ Moos, F., Quick-Freeze als Alternative zur Vorratsdatenspeicherung, Auseinandersetzung mit dem Diskussionsentwurf des BMJ und der Stellungnahme des DAV, ZD 2012, 153.

Article 29 Data Protection Working Party, Report 01/2010 on the second joint enforcement action:, Compliance at national level of Telecom Providers and ISPs with the obligations required from national traffic data retention legislation on the legal basis of Articles 6 and 9 of the e-Privacy Directive 2002/58/EC and the Data Retention Directive 2006/24/EC amending the e-Privacy Directive 13 July 2010; WP 172;
zitiert als *Art. 29 DP WP,* v. 13 July 2010, WP 172.

Arzt, C./ Eier, J., Zur Rechtmäßigkeit der Speicherung personenbezogener Daten in "Gewalttäter"-Verbunddateien des Bundeskriminalamts, DVBl. 2010, 816.

Aulehner, J., Polizeiliche Gefahren- und Informationsvorsorge. Berlin, 1998.

Bäcker, M., Solange IIa oder Basta I?, Das Vorratsdaten-Urteil des Bundesverfassungsgerichts aus europarechtlicher Sicht, EuR 2011, 103.

Backes, O./ Gusy, C., Wer kontrolliert die Telefonüberwachung?, Eine empirische Untersuchung zum Richtervorbehalt bei der Telefonüberwachung. Frankfurt am Main 2003.

Badach, A., Voice over IP. Die Technik, 4. Auflage, München/Wien, 2010.

Baldus, M., Der Kernbereich privater Lebensgestaltung - absolut geschützt, aber abwägungsoffen, JZ 2008, 218.

Bär, W., Telekommunikationsüberwachung und andere verdeckte Ermittlungsmaßnahmen, Gesetzliche Neuregelungen zum 1.1.2008, MMR 2008, 215.

Bär, W., Anmerkungen zu AG Bayreuth, 17.9.2009 – Gs 911/09, MMR 2010, 267.

Baum, G. R./ Schantz, P., Die Novelle des BKA-Gesetzes - Eine rechtspolitische und verfassungsrechtliche Kritik, ZRP 2008, 137.

Baumann, R., Die Entwicklung des öffentlichen Rechts, Stellungnahme zu den Auswirkungen des Urteils des Bundesverfassungsgerichts vom 15.12.1983 zum Volkszählungsgesetz 1983, DVBl. 1984, 612.

Beck, U., Risikogesellschaft, Auf dem Weg in eine andere Moderne, 1. Auflage, Frankfurt am Main 1986.

Benda, E., Privatsphäre und "Persönlichkeitsprofil", Ein Beitrag zur Datenschutzdiskussion, in: *Leibholz, G.* (Hrsg.) 1974 – Menschenwürde und freiheitliche Rechtsordnung, S. 23-44;
zitiert als *Benda* 1974, S.

Benda, E., Das Recht auf informationelle Selbstbestimmung und die Rechtsprechung des Bundesverfassungsgerichts zum Datenschutz, DUD 1984, 86.

Berger, E. G., Wer anschaffen will, muss auch zahlen, Die Verfassungswidrigkeit des § 110 TKG am Beispiel der Auslandskopfüberwachung und Vorratsdatenspeicherung, CR 2008, 557.

Berndiek, A., Europäische Sicherheitspolitik, Stiftung Wissenschaft und Politik (Hrsg.). Berlin 2012, abrufbar unter:
http://www.swp-berlin.org/fileadmin/contents/products/studien/2012_S15_bdk.pdf;
zitiert als *Berndiek* 2012, S.

Bernsdorff, N., in: *Meyer, J.* (Hrsg.), Kommentar zur Charta der Grundrechte der Europäischen Union, Baden-Baden 2003, Art. 6-19;
zitiert als *Bernsdorff*, in: *Meyer*, EU-GRCh., Art.

Bethge, H., § 72 Grundrechtskollisionen, in: *Merten, D./ Papier, H.-J.* (Hrsg.), Handbuch der Grundrechte, Grundrechte in Deutschland: Allgemeine Lehren, Bnd. II. Heidelberg 2009;
zitiert als *Bethge,* in: *Merten/Papier,* GR II, 2009, § 72 Rn.

Bettermann, K. A., Der totale Rechtsstaat, Zwei kritische Vorträge. Göttingen 1986;
zitiert als *Bettermann* 1986.

Beukelmann, S., Vorratsdatenspeicherung so nicht verfassungsgemäß, NJW Spezial 2010, 184.

Beukelmann, S., Surfen ohne strafrechtliche Grenzen, NJW 2012, 2617.

Blankenburg, D., Quo vadis §§ 106, 108a UrhG?, Strafrechtlicher Urheberrechtsschutz nach dem BVerfG-Urteil zur Vorratsdatenspeicherung, MMR 2010, 587.

Blumenwitz, D., Souveränität - Gewaltverbot - Menschenrechte, Eine völkerrechtliche Bestandsaufnahme nach Abschluß des nicht mandatierten NATO-Einsatzes in Ex-Jugoslawien, Politische Studien 1999, 19.

Böckenförde, E.-W., Grundrechte als Grundsatznormen – zur gegenwärtigen Lage der Grundrechtsdogmatik, Der Staat 29 (1990), 1.

Böckenförde, T., Die Ermittlung im Netz. Tübingen, 2003; zitiert als *Böckenförde* 2003, S.

Boehm, F., Anlasslose Datensammlungen und die Mitarbeit Privater bei der Strafverfolgung - der neue Trend in der europäischen Verbrechensbekämpfung? Vorratsdaten und Fluggastdatenspeicherung, KritV 2012, 82.

Boehm, F., Information sharing and data protection in the area of freedom, security and justice, Towards harmonised data protection principles for EU-internal information exchange, 1. Auflage, Berlin 2011.

Boehm, F./ Hornung, G., Comparative Study on the 2011 draft Agreement between the Unites States of America and the European Union on the use and transfer of Passenger Name Records (PNR) to the United States Department of Homeland Security, Luxembourg/Passau 14.3.2012; abrufbar unter: http://gruen-digital.de/wp-content/uploads/2012/03/PNR-EU-USA-Study-120313.pdf;
zitiert als *Boehm/Hornung* 2012.

Bohne, in: *Wandtke, A.-A./Bullinger, Winfried* (Hrsg.), Praxiskommentar zum Urheberrecht, München 2009;
zitiert als *Bohne,* in: UrhR 2009, § 101 UrhG Rn.

Böse, M., Der Grundsatz der Verfügbarkeit von Informationen in der strafrechtlichen Zusammenarbeit der Europäischen Union. Göttingen 2007.

Brakelmann, G., Die soziale Frage des 19. Jahrhunderts, 2. Auflage, Witten/Ruhr 1964.

Braun, F., Die entschädigungslose Indienstnahme Privater am Beispiel der sog. Vorratsdatenspeicherung, K&R 2009, 386.

Braun, F., Ozapftis - (Un)Zulässigkeit von "Staatstrojanern", K&R 2011, 681.

Brenneisen, H./ Bock, D., Die präventiv-polizeiliche Rasterfahndung im Lichte der aktuellen Rechtsprechung des BVerfG, DUD, 685.

Breuer, R., Der Stand der Technik im geltenden Recht, in: *Leibholz, G.* (Hrsg.) Aktuelle Probleme des umwelt- und Technikrechts, Symposium aus Anlass des 70. Geburtstages von Professor Dr. Peter Marburger, S. 9 ff. Bamberg 2011;
zitiert als *Breuer* 2011, S.

Breyer, P., Die systematische Aufzeichnung und Vorhaltung von Telekommunikations-Verkehrsdaten für staatliche Zwecke in Deutschland. Berlin 2005.

Breyer, P., Rechtsprobleme der Richtlinie 2006/ 24/ EG zur Vorratsdatenspeicherung und ihrer Umsetzung in Deutschland, StV 2007, 214 ff.

Breyer, P., Nach dem Vorratsdatenspeicherungs-Urteil - Was nun mit den anderen Massendatensammlungen passieren muss, NJW aktuell 2010, 12.

Brinkel, G./ Lammers, J., Innere Sicherheit auf Vorrat?, ZUM 2008, 11 ff.

Britz, G., Schutz informationeller Selbstbestimmung gegen schwerwiegende Grundrechtseingriffe, Entwicklungen im Lichte des Vorratsdatenspeicherungsurteils, JA 2011, 81.

Brodowski, D., Strafrechtsrelevante Entwicklungen in der Europäischen Union – ein Überblick, ZIS 2011, 940.

Brugger, W., Einschränkung des absoluten Folterverbots bei Rettungsfolter?, APuZ 2006, 9.

Brugger, W./ Gusy, C., Gewährleistung von Freiheit und Sicherheit im Lichte unterschiedlicher Staats- und Verfassungsverständnisse, VVDStRL 2004.

Brunst, P. Anonymität im Internet - rechtliche und tatsächliche Rahmenbedingungen, Zum Spannungsfeld zwischen einem Recht auf Anonymität bei der elektronischen Kommunikation und den Möglichkeiten zur Identifizierung und Strafverfolgung. Erlangen-Nürnberg 2009.

Brunst, P., Staatlicher Zugang zur digitalen Identität, Erosion der Anonymität im Internet, DuD 2011, 618.

Buchner, *B.,* Kommentierung § 3, in: *Taeger, J./ Gabel, D./ Braun, M.* (Hrsg.), Kommentar zum BDSG und zu den Datenschutzvorschriften des TKG und TMG, 1. Auflage, Frankfurt am Main 2010;
zitiert als *Buchner,* in: *Taeger/Gabel* (Hrsg.), BDSG, §, Rn.

Bull, H. P., Die Staatsaufgaben nach dem Grundgesetz, 2., erw. Auflage, Kronberg/Ts. 1977;
zitiert als *Bull* 1977, S.

Bull, H.-P., Informationelle Selbstbestimmung- Vision oder Illusion? Datenschutz im Spannungsverhältnis von Freiheit und Sicherheit. 2. Auflage, Tübingen 2011.

Bundeskriminalamt, Presseinformation v. 8.10.2010, Die Bedeutung von Mindestspeicherfristen für Gefahrenabwehr und Strafverfolgung, abrufbar unter:
http://www.*BKA*.de/nn_233982/SharedDocs/Downloads/DE/ThemenABisZ/Mindestspeicherfristen/101008PresseinformationMindestspeicherfristen.html;
zitiert als: *BKA,* Mindestspeicherfristen 2010, S.

Bundeskriminalamt, Statistische Datenerhebung im BKA zu den Auswirkungen des Bundesverfassungsgerichts-Urteil vom 02.03.2010 zu "Mindestspeicherungsfristen" von Telekommunikationsverkehrsdaten, 2011, abrufbar unter:
http://www.bka.de/nn_233982/DE/ThemenABisZ/Mindestspeicherfristen/DatenerhebungBKA/datenerhebungBKA.html;
zitiert als *BKA,* Statistische Datenerhebung 2011.

Bundesministerium des Innern, Verfassungsschutzbericht 2009, v. 21.6.2010,
abrufbar unter: http://www.verfassungsschutz.de/de/publikationen/verfassungsschutzbericht/vsbericht_2009/;
zitiert als *BMI,* Verfassungsschutzbericht 2009, S.

Buzan, B./ Waever, O./ Wilde, J. de, Security, A new framework for analysis. Boulder Colo. u.a 1998;
zitiert als *Buzan/Waever/de Wilde* 1998, S.

Calliess, C., Sicherheit im freiheitlichen Rechtsstaat, Eine verfassungsrechtliche Gratwanderung mit staatstheoretischem Kompass, ZRP 2002, 1.

Caspar, J., Geoinformationen und Datenschutz am Beispiel des Internetdienstes Google Street View, DÖV 2009, 965.

Collignon, S., Demokratische Anforderungen an eine europäische Wirtschaftsregierung, Friedrich Ebert Stiftung, 2010.

Comer, D. E., Computernetzwerke und Internets, Mit Internet-Anwendungen, 3., überarb. München 2002.

Cornils, M., Grundrechtsschutz gegenüber polizeilicher Kfz-Kennzeichenüberwachung, Jura 2010, 443.

Cremer, H.-J., Kap. 22, in: *Grote, R./ Marauhn, T.* (Hrsg.), EMRK/GG, Konkordanzkommentar zum europäischen und deutschen Grundrechtsschutz. Tübingen 2006;
zitiert als *Cremer*, EMRK/GG , Kap. 22, Rn.

Czychowski, C./ Nordemann, B., Vorratsdaten und Urheberrecht – Zulässige Nutzung gespeicherter Daten, NJW 2008, 3095.

Daase, C., Der erweiterte Sicherheitsbegriff, 22.11.2010, abrufbar unter:
http://www.sicherheitskultur.org/fileadmin/files/WorkingPapers/01-Daase.pdf;
zitiert als *Daase* 2010, S.

Dammann, I., Der Kernbereich der privaten Lebensgestaltung, Zum Menschenwürde- und Wesensgehaltsschutz im Bereich der Freiheitsgrundrechte. Berlin 2011.

Dammann, U., in: *Simitis, S* (Hrsg.), Bundesdatenschutzgesetz. 7. Auflage, Baden-Baden 2011;
zitiert als *Dammann*, in: *Simitis*, BDSG, 2011, § Rn.

Darnstädt, T., Karlsruher Gefahr - Eine kritische Rekonstruktion der polizeirechtlichen Ausführungen des Bundesverfassungsgerichts im Vorratsdaten-Urteil und im Online-Urteil, DVBl. 2011, 263.

Dauses, M. A. (Hrsg.), Handbuch des EU-Wirtschaftsrechts, München 2011.

Degener, *W.,* Grundsatz der Verhältnismäßigkeit und strafprozessuale Zwangsmaßnahmen, 1. Auflage, Berlin 1985.

Degenhardt, C., Art. 73, in: *Sachs, M.* (Hrsg.), Grundgesetz Kommentar, München 2011;
zitiert als *Degenhardt*, in: *Sachs,* GG 2011, Art. 73 Rn.

Degenhardt, C., Staatsorganisationsrecht, Mit Bezügen zum Europarecht, 27. Auflage, Heidelberg 2011.

Dellwo, K.-H., Widerstandsformen in der BRD, in: Von der Rationalität des Rechts in die Irrationalität der Sicherheit, Reflexionen über Widerstandsformen in Sicherheitsgesellschaften, KritV 2010, 137.

Denninger, E., Der gebändigte Leviathan, 1. Auflage, Baden-Baden 1990;

Denninger, E., Die Trennung von Verfassungsschutz und Polizei und Das Grundrecht auf informationelle Selbstbestimmung, ZRP 1981, 231.

Denninger, E., Verfassungsrechtliche Grenzen des Lauschens, Der "große Lauschangriff" auf dem Prüfstand der Verfassung, ZRP 2004, 101.

Depenheuer, O., Selbstbehauptung des Rechtsstaats, 2. Auflage, Paderborn 2007.

Derksen, R., Zur Vereinbarkeit der Richtlinie über die Vorratsspeicherung von Daten mit der Europäischen Grundrechtecharta, Ausarbeitung des Wissenschaftlichen Dienst des Bundestages, v. 25.2.2011, WD 11 – 3000 – 18/11, abrufbar unter:
http://www.vorratsdatenspeicherung.de/images/rechtsgutachten_grundrechtecharta.pdf;
zitiert als: *Derksen* 2011, S.

Desoi, M./ Knierim, A., Intimsphäre und Kernbereichsschutz, Ein unantastbarer Bereich privater Lebensgestaltung in der Rechtsprechung des Bundesverfassungsgerichts, DÖV 2011, 398.

DESTATIS (Statistische Bundesamt), Informationsgesellschaft in Deutschland, Ausgabe 2009, abrufbar unter:
https://www.destatis.de/DE/ZahlenFakten/GesellschaftStaat/EinkommenKonsumLebensbedingungen/ITNutzung/ITNutzung.html;
zitiert als *DESTATIS* Informationsgesellschaft 2009, S.

Di Fabio, U., Art. 2 in *Maunz, T./ Dürig, G.* (Hrsg.), Grundgesetzkommentar, Loseblatt. 63. Auflage, München 2011;
zitiert als *Di Fabio,* in: *Maunz/Dürig,* GG 2011, Art. 2, Rn.

Di Fabio, U., Gewaltenteilung, § 27 in: *Isensee, J./ Kirchhof, P.* (Hrsg.), Verfassungsstaat, Handbuch des Staatsrechts, Bnd. II, Heidelberg 2004;
zitiert als *Di Fabio,* in: *Isensee/Kirchof,* HStR II, 2004, § 27.

Di Fabio, U., Sicherheit in Freiheit, NJW 2008, 421.

Dieterich, T., Grundgesetz, Einleitung in: *Dieterich, T./ Hanau, P./ Schaub, G.,* Erfurter Kommentar zum Arbeitsrecht, 12. Auflage, 2012;
zitiert als: *Dieterich,* ErfKomm, 2012, Einl. GG Rn.

Dix, A., Freiheit braucht Sicherheit - Sicherheit braucht Freiheit, Benjamin Franklin und die Freiheit zur unbeobachteten Kommunikation, in: *Bundeskriminalamt* (Hrsg.), Informations- und Kommunikationskriminalität, Vorträge anlässlich der Herbsttagung des Bundeskriminalamtes vom 2. bis 4. Dezember 2003, München 2004;
zitiert als *Dix* 2004, S.

Dix, A., Vorratsdatenspeicherung verletzt Europäische Grundrechte, Impulsreferat, 6. Europäischer Datenschutztag. Berlin 27.1.2012, abrufbar unter: http://datenschutz-berlin.de/;
zitiert als *Dix* 2012.

Dix, A./ Petri, T., Das Fernmeldegeheimnis und die deutsche Verfassungsidentität - Zu Verfassungswidrigkeit der Vorratsdatenspeicherung, DUD 2009, 531.

Dolzer, R., Wirtschaft und Kultur, 6. Abschnitt in: *Vitzthum, W.* (Hrsg.), Völkerrecht. Berlin 2010; zitiert als *Dolzer,* in: *Vitzthum,* VR 2010.

Dörr, O., Kap. 13, in: *Grote, R./ Marauhn, T.* (Hrsg.), EMRK/GG, Konkordanzkommentar zum europäischen und deutschen Grundrechtsschutz, Tübingen 2006;
zitiert als *Dörr*, EMRK/GG.

*Dreier, H., (*Hrsg.), Grundgesetz-Kommentar in 3 Bänden, 2. Auflage, Tübingen 2004;
zitiert als *Autor,* in *Dreier* GG, Art. Rn.

Dürig, G., Der Grundrechtssatz von der Menschenwürde, AöR 1956, 117.

Durner, W., Art. 10, in: *Maunz, T./ Dürig, G.*, Grundgesetz, Kommentar, München 2011;
zitiert als *Durner,* in: *Maunz/Dürig*, GG 2011, Art., Rn.

Eagle, N./ Pentland, A./ Lazer, D., From the Cover: Inferring friendship network structure by using mobile phone data, Proceedings of the National Academy of Sciences 2009, 15274;
zitiert als *Eagle/Pentland/Lazer* 2009, 15274.

Eckhardt, J., § 96 TKG, in*: Spindler, G./ Schuster, F.* (Hrsg.), Recht der elektronischen Medien, München 2011;
zitiert als *Eckhardt,* in: *Spindler/Schuster* 2011, § 96 Rn.

Eckhardt, J., Einstweilige Anordnung des BVerfG zur Vorratsdatenspeicherung, Eine Praxisbetrachtung aus der Sicht der Telekommunikationsunternehmen, DUD 2008, 520.

Eckhardt, J., IP-Adresse als personenbezogenes Datum - neues Öl ins Feuer, Personenbezug im Datenschutzrecht - Grenzen der Bestimmbarkeit am Beispiel der IP-Adresse, CR 2011, 339.

Eckhardt, J./ Schütze, M., Vorratsdatenschutz - Verkennen die Gerichte die Besonderheiten, K&R 2010, I.

Eckhardt, J./ Schütze, M., Vorratsdatenspeicherung nach BVerfG: "Nach dem Gesetz ist vor dem Gesetz…", Und der Staat wird im Streit mit Bürgern und TK-Unternehmen zum "lachenden Dritten", CR 2010, 225.

Ehlers, D., Verhältnis des Unionsrechts zu dem Recht der Mitgliedstaaten, § 11, in*: Schulze, R./ Zuleeg, M./ Kadelbach, S.* (Hrsg.), Europarecht, Handbuch für die deutsche Rechtspraxis, Baden-Baden 2010;
zitiert als *Ehlers,* in: *Schulze/Zuleeg/Kadelbach*, EuR 2010, § 11 Rn.

Eichhorn, P., Das Prinzip Wirtschaftlichkeit, Basiswissen der Betriebswirtschaftslehre, 3. Auflage, Wiesbaden 2005.

Eifert, M., Informationelle Selbstbestimmung im Internet, Das BVerfG und die Online-Durchsuchungen, NVwZ 2008, 521.

Endres, J., IPv6, Antworten auf die häufigsten Fragen, c't 2011, 182.

Endres, J., Ist IPv6 privat genug?, Was die lange IP-Adresse über Sie verrät, c't 2011, 146.

Erbguth, W., Art. 35, in: *Sachs,* M. (Hrsg.), Grundgesetz, Kommentar, München 2011;
zitiert als: *Erbguth* in *Sachs,* GG 2011, Art. 35.

Eser, A., in: *Meyer, J.*, (Hrsg.),Kommentar zur Charta der Grundrechte der Europäischen Union. Baden-Baden 2003, Art. 47-50;
zitiert als *Eser,* in: *Meyer,* EU-GRCh. 2003, Art., Rn.

EU Kommission, Bewertungsbericht zur Richtlinie über die Vorratsdatenspeicherung (Richtlinie 2006/24/EG), Bericht der Kommission an den Rat und das Europäische Parlament, KOM (2011), 225, abrufbar unter: http://ec.europa.eu/commission_2010-2014/malmstrom/archive/20110418_data_retention_evaluation_de.pdf, 20. April 2011;
zitiert als KOM (20011), 225, S.

FDP, Eckpunktepapier zur Sicherung vorhandener Verkehrsdaten und Gewährleistung von Bestandsdatenauskünften im Internet 17. 1.2011; abrufbar unter: http://www.bmj.de/SharedDocs/Downloads/DE/pdfs/Eckpunktepapier_zur_Sicherung_vorhandener_Verkehrsdaten_und_Gewaehrleistung_von_Bestandsdatenauskuenften_im_Internet.pdf;
zitiert als: *FDP* Eckpunktepapier v. 17.1.2011.

Feldman, A., Formations of violence, The narrative of the body and political terror in Northern Ireland. Chicago u.a 1991.

Feldmann, T., Unterliegen Arbeitgeber der Pflicht zur Vorratsdatenspeicherung gem. § 113a TKG?, Erwiderung auf Koch, NZA 2008, 911; NZA 2008, 1398.

Fetscher, I., Terrorismus und Reaktion, 2. Auflage, Köln 1978.

Fischer, S., Verhandlungssache 'Sicherheit' - Akteure, Konstruktionen und Sicherheitsmaßnahmen. München 6.-7.10.2011;
zitiert als *Fischer* 2011.

Fischer-Lescano, A., Kritik der praktischen Konkordanz, KJ 2008, 166.

Flechsig, N. P., Zur Zukunft des Urheberrechts im Zeitalter vollständiger Digitalisierung künstlicher Leistungen, ZGE 2011, 19.

Forgó, N./ Krügel, T./ Rapp, S., Zwecksetzung und informationelle Gewaltenteilung, Ein Beitrag zu einem datenschutzgerechten E-Government, 1. Auflage, Baden-Baden 2006;
zitiert als *Forgó/Krügel/Rapp* 2006, S.

Forgó, N./ Jlussi, D./ Klügel, C./ Krügel, T., Die Umsetzung der Richtlinie zur Vorratsdatenspeicherung, *Forgó et al.* DUD 2008, 680.

Forgó, N./ Krügel, T., Der Personenbezug von Geo-Daten, Cui bono, wenn alles bestimmbar ist?, MMR 2010, 17.

Forgó, N./ Krügel, T., Vorschriften zur Vorratsdatenspeicherung verfassungswidrig: Nach der Entscheidung ist vor der Entscheidung, Zugleich Kommentar zu BVerfG, Urteil vom 2.3.2010, K&R 2010, 217.

Foucault, M., Überwachen und Strafen, Die Geburt des Gefängnisses, 1. Auflage, Frankfurt am Main 1993 (franz. Originaltitel „Surveiller et punir – la naissance de la prison", Erstausgabe Paris 1975), Dt. Übersetzung von *W. Seitter*;
zitiert als *Foucault* 1993, S.

Fox, D., Der IMSI-Catcher, DuD 2002, 212.

Fox, D., Sicheres Löschen von Daten auf Festplatten, Best Practice, DuD 2009, 110.

Freiling, F., Zur Nutzung von Verkehrsdaten im Rahmen der Vorratsdatenspeicherung, Technischer Bericht TR-2009-005, abrufbar unter: http://madoc.bib.uni-mannheim.de/madoc/volltexte/2009/2360/pdf/TR_2009_005.pdf;
zitiert als *Freiling* 2009.

Frenz, W., Europäische Grundrechte, 1. Auflage, Berlin Heidelberg 2009;
zitiert als *Frenz* 2009, Rn.

Frenz, W., Europäischer Datenschutz und Terrorabwehr, EuZW 2009, 6.

Freund, B./ Schnabel, C., Bedeutet Ipv6 das Ende der Anonymität im Internet?, Technische Grundlagen und rechtliche Beurteilung des neuen Internet-Protokolls, MMR 2011, 495.

Frowein, J. A./ Peukert, W., Europäische MenschenRechtsKonvention, EMRK-Kommentar, 3. Auflage, Kehl am Rhein 2009;
zitiert als *Frowein/Peukert,* EMRK 2009, Art., Rn.

Fuchs, W., Kontrollkulturen im Wandel: auf dem Weg in die Sicherheitsgesellschaft, Vortrag im Rahmen der IWK-Vortragsreihe: Culture of Control?, Wien 8.11.2010;
zitiert als *Fuchs* 2010.

Gärditz, K. F., Strafprozess und Prävention, Entwurf einer verfassungsrechtlichen Zuständigkeits- und Funktionenordnung, Tübingen 2003.

Gausling, T., Verdachtsunabhängige Speicherung von Verkehrsdaten auf Vorrat, Zur Umsetzung der Richtlinie 2006/24/EG durch die §§ 113a, 113b TKG. München 2010.

Gebauer, P., Zur Grundlage des absoluten Folterverbots, NVwZ 2004, 1405.

Gercke, B., Telekommunikationsüberwachung: Lückenlose Kontrolle von Datennetzen, in: *Roggan, F.* (Hrsg.), Handbuch zum Recht der inneren Sicherheit, 2. Auflage, Berlin 2006;
zitiert als *Gercke,* in: *Roggan* 2006, S.

Gercke, B., Anmerkung zu BVerfG vom 2.3.2010 - 1 BvR 25/08, 263/08; 58/08, StV 2010, 281.

Gerhartinger, H., Österreich: Umstrittene Richtlinie zur Vorratsdatenspeicherung umgesetzt, MMR-Aktuell 2011, 318504

Gietl, *A.,* Die Einführung der Vorratsdatenspeicherung, K&R 2007, 545

Gietl, A., Das Schicksal der Vorratsdatenspeicherung, DUD 2008, 317.

Gietl, A./ Tomasic, L., Kompetenz der Europäischen Gemeinschaft zur Einführung der Vorratsdatenspeicherung, Anmerkung zu den Schlussanträgen von Generalanwalt Yves Bot im Verfahren C-301/06 vom 14.10.2008, DUD 2008, 795.

Gitter, R./ Schnabel, C., Die Richtlinie zur Vorratsspeicherung und ihre Umsetzung in das nationale Recht, MMR 2007, 411.

Glasser, P., Seid Netz zueinander!, c't soziale netze 2/2012, 8.

Gola, P./ Klug, C. Grundzüge des Datenschutzrechts. München 2003;
zitiert als *Gola/Klug* 2003, S.

Gola, P./ Klug, C./ Reif, Y., Datenschutz- und presserechtliche Bewertung der "Vorratsdatenspeicherung", NJW 2007, 2599.

Gola, P./ Klug, C./ Schomerus, R., Bundesdatenschutzgesetz, 10. Auflage, München 2010;
zitiert als *Gola/Klug/Schomerus,* BDSG, 2010, §.

Götz, V., Innere Sicherheit, § 85, in: *Isensee, J./ Kirchhof, P.* (Hrsg.), Handbuch des Staatsrechts der Bundesrepublik Deutschland, Band. IV, Aufgaben des Staates, Heidelberg 2006; zitiert als *Götz,* in: *Isensee/Kirchof*, HStR IV 2006, § 85 Rn.

Grabenwarter, C./ Pabel, K., Europäische Menschenrechtskonvention, 5. Auflage, München 2011;
zitiert als *Grabenwarter/Pabel* 2011, § Rn.

Grabitz, E., Der Grundsatz der Verhältnismäßigkeit in der Rechtsprechung des Bundesverfassungsgerichts, AöR 1973 (Bd. 98), 568.

Grabitz, E., Freiheit der Person (§ 130) in *Isensee, J./ Kirchhof, P.* (Hrsg.), Handbuch des Staatsrechts der Bundesrepublik Deutschland, Band. VI, Freiheitsrechte, 2. Auflage, Heidelberg 2001;
zitiert als *Grabitz,* in: *Isensee/Kirchof*, HStR VI 2001, §130 Rn.

Graf, J.-P. (Hrsg.), Strafprozessordnung. München 2011;
zitiert als *Graf,* StPO 2011, § Rn.

Grafe, A., Die Auskunftserteilung über Verkehrsdaten nach §§ 100g, 100h StPO, Staatliche Kontrolle unter Mitwirkung Privater; Freiburg 2007; abrufbar unter:
http://www.freidok.uni-freiburg.de/volltexte/6085/pdf/Verkehrsdaten.pdf.

Grawert, R., Wechselwirkungen zwischen Landes- und Bundesgrundrechten (§ 81), in *Merten, D/ Papier, H.-J.,* Handbuch Grundrechte Bnd. 3, Heidelberg 2009;
zitiert als *Grawert* in HGR III § 81, Rn.

Greenawalt, T., Die Indienstnahme privater Netzbetreiber bei der Telekommunikationsüberwachung in Deutschland, Spannungsfeld zwischen staatlichen Kontrollbefugnissen und wirtschaftlicher Betätigungsfreiheit. Berlin 2009.

Grimm, D., Die Meinungsfreiheit in der Rechtsprechung des Bundesverfassungsgerichts, NJW 1995, 1703 ff.

Grimm, D./ Michaelis, I., Keine Vorratsdatenspeicherung für Arbeitgeber, Der Betrieb 2009, 174.

Gröschner, R./ Wiehart-Howaldt, A., Menschenwürde und Sepulkralkultur in der grundgesetzlichen Ordnung, Die kulturstaatlichen Grenzen der Privatisierung im Bestattungsrecht. Stuttgart 1995.

Grote, R./ Marauhn, T. (Hrsg.), EMRK/GG , Konkordanzkommentar zum europäischen und deutschen Grundrechtsschutz, Tübingen 2006.

*Grupp, K.***,** Steuerung des Verwaltungshandelns durch Wirtschaftlichkeitskontrolle?, Zum zweiten Beratungsgegenstand der Staatsrechtslehrertagung, in: DÖV 1983, 661.

Grzeszick, B., Art. 20, in: *Maunz, T./ Dürig, G.*, Grundgesetz, Kommentar, München 2011; zitiert als *Grzeszick* in *Maunz/Dürig,* GG 2011, Art. Rn.

Gudermann, A., Online-Durchsuchung im Lichte des Verfassungsrechts, Die Zulässigkeit eines informationstechnologischen Instruments moderner Sicherheitspolitik, Hamburg 2010.

Guinard, D./ Trifa, V./ Mattern, F./ Wilde, E., From the Internet of Things to the Web of Things: Resource Oriented Archtitecture and Best Practices, in: *Uckelmann, D./ Harrison, M./ Michahelles, F.* (Hrsg.), Architecting the Internet of Things, Berlin 2011, S. 97 – 129;
zitiert als *Guinard/Trifa/Mattern/Wilde* 2011, S.

Gundel, J., Vorratsdatenspeicherung und Binnenmarktkompetenz: Die ungebrochene Anziehungskraft des Art. 95 EGV, Anmerkung zu EuGH RS. C-301/06 - Irland/ Rat und Parlament, EuR 2009, 536.

Gurlit, E., Verfassungsrechtliche Rahmenbedingungen des Datenschutzes, NJW 2010, 1035.

Gusy, C., Die "freiheitliche demokratische Grundordnung" in der Rechtsprechung des Bundesverfassungsgerichts, AöR 1980 (105), 279.

Gusy, C., Gewährleistung von Freiheit und Sicherheit im Lichte unterschiedlicher Staats- und Verfassungsverständnisse, VVDStRL 63 (2004), 151.

Gusy, C., Parlamentarische Kontrolle der Nachrichtendienste im demokratischen Rechtsstaat, ZRP 2008, 36.

Gusy, C., Polizei- und Ordnungsrecht, 7. Auflage, Tübingen 2009; zitiert als *Gusy* 2009, Rn.

Gusy, C., Überwachung der Telekommunikation unter Richtervorbehalt - Effektiver Grundrechtsschutz oder Alibi?, ZRP 2003, 275.

Gusy, C., Vom neuen Sicherheitsbegriff zur neuen Sicherheitsarchitektur, VerwArch 2010, 309.

Gusy, C., Die "Schwere" des Informationseingriffs, in: *Baumeister, P./ Roth, W./ Ruthig, J.* (Hrsg.), Staat, Verwaltung und Rechtsschutz, Festschrift für Wolf-Rüdiger Schenke zum 70. Geburtstag, Berlin 2011, 395 – 413;
zitiert als *Gusy* 2011, S.

Habermas, J., Die Zukunft der menschlichen Natur, Auf dem Weg zu einer liberalen Eugenik?, 1. Auflage, Frankfurt am Main 2001;
zitiert als *Habermas* 2001.

Hamacher, K./ Katzenbeisser, S., Public Security: Simulations need to Replace Conventional Wisdom; abrufbar unter: http://www.nspw.org/papers/2011/nspw2011-hamacher.pdf;
zitiert als *Hamacher/Katzenbeisser,* NSPW 2011.

Hammer, V./ Pordesch, U./ Roßnagel, A., Betriebliche Telefon- und ISDN-Anlagen rechtsgemäß gestaltet. Berlin 1993;
zitiert als *Hammer/Pordesch/Roßnagel* 1993.

Hammerstein, C. v., Kostentragung für staatliche Überwachungsmaßnahmen nach der TKG-Novelle, MMR 2004, 222.

Hansen, M., Privacy Enhacing Technologies, in: *Roßnagel, A.* (Hrsg.), Handbuch Datenschutzrecht, Die neuen Grundlagen für Wirtschaft und Verwaltung, München 2003, Kap. 3.3;
zitiert als *Hansen* 2003.

Hansen, M./ Pfitzmann, A., Technische Grundlagen von Online-Durchsuchung und -Beschlagnahme, DRiZ 2007, 225.

Härtel, I., Handbuch europäische Rechtsetzung. Berlin 2006.

Härting, N., Datenschutz im Internet - Gesetzgeberischer Handlungsbedarf, BB 2010, 839 ff.

Hassemer, W., Zum Spannungsverhältnis von Freiheit und Sicherheit: Drei Thesen, vorgänge 2002 (Nr. 159), 10.

Hassemer, W., Sicherheit durch Strafrecht, HRRS 2006, 130.

Hassemer, W., Sicherheit durch Strafrecht, in: Wieviel Sicherheit braucht die Freiheit?, 30. Strafverteidigertag 2006, Berlin 2007, 9 – 40;
zitiert als *Hassemer* 2007, S.

Heckmann, D., Editorial, jurisPR-ITR 2010.

Heckmann, D., Vertrauen in virtuellen Räumen?, K&R 2010, 1.

Hefendehl, R., Daten-Dammbrüche - oder warum nicht jede Nase zu einem Kamel führt, Zugleich ein Beitrag zur aktuellen Diskussion um die Vorratsdatenspeicherung, JZ 2009, 165.

Heidrich, J./ Wegener, C., Datenschutzrechtliche Aspekte bei der Weitergabe von IP-Adressen, DUD 2010, 172.

Heinson, D./ Freiling, F., Probleme des Verkehrsdatenbegriffs im Rahmen der Vorratsdatenspeicherung, DUD 2009, 547 ff.

Hellebrand, J., Die Staatsanwaltschaft, Arbeitsgebiet und Arbeitspraxis : eine Einführung für angehende Staatsanwälte und für Referendare bei Eintritt in die staatsanwaltschaftliche Ausbildung. München 1999.

Henrichs, A./ Wilhelm, J., Funkzellenauswertung, Rechtliche und taktische Aspekte der telekommunikativen Spurensuche, Die Kriminalpolizei 3/2010; abrufbar unter: http://www.kriminalpolizei.de/articles,funkzellenauswertung,1,275.htm;
zitiert als *Henrichs/Wilhelm* 2010.

Hensel, D., Die Vorratsdatenspeicherung aus datenschutzrechtlicher Sicht, Die Bildung von Persönlichkeitsprofilen und andere Probleme der Vorratsdatenspeicherung, DUD 2009, 527.

Herdegen, M., Europarecht, 13. Auflage, München 2011.

Hermes, G., Art. 10 in *Dreier, H.* (Hrsg.), Grundgesetzkommentar, Bnd. 1, Tübingen 2004; zitiert als *Hermes,* in: *Dreier,* GG 2004, Art. 10 Rn.

Herrmann, K./ Soiné, M., Durchsuchung persönlicher Datenspeicher und Grundrechtsschutz, NJW 2011, 2922.

Herzog, R., in: *Maunz, T./Dürig, G*, Grundgesetz, Kommentar, München 2010/2012; zitiert als *Herzog,* in: *Maunz/Dürig*, GG 2011, Art. Rn.

Herzog, R., Zur Auslegung des Sozialstaatsprinzips, BayVBl 1976, 161.

Hesse , *K*., Die normative Kraft der Verfassung, Tübingen 1959.

Hesse, K., Grundzüge des Verfassungsrechts der Bundesrepublik Deutschland, 20., neubearb. Auflage, Heidelberg 1995, Erstveröffentlichung 1977; zitiert als *Hesse* 1995 (1977), S.

Hesse, H. A., Der Schutzstaat, Rechtssoziologische Skizzen in dunkler Zeit, 1. Auflage, Baden-Baden 1994.

Heun, S.-E., Anmerkung zum Urteil des BVerfG vom 2.3.2010, CR 2010, 247.

Heußner, H., Das informationelle Selbstbestimmungsrecht des Grundgesetzes als Schutz des Menschen vor totaler Erfassung, BB 1990, 1281.

Hillgruber, C., in *Epping, V./ Hillgruber, C.* (Hrsg.), Beck'scher Online-Kommentar zum Grundgesetz. München 2012; zitiert als *Hillgruber* in: BeckOK GG, Art. 1 Rn.

Hirsch, B., Gesellschaftliche Folgen staatlicher Überwachung, DUD 2008, 87.

Hirsch, B., Zu den Anforderungen eines modernen Datenschutzes, KritV 2011, 139.

Hirschmann, K., Terrorismus in neuen Dimensionen, Hintergründe und Schlussfolgerungen, APuZ 2001 (Bd. 51), 7.

Hobbes, T., Leviathan, Erster und zweiter Teil, Bibliogr. erg. Ausg., Nachdr., *Mayer, J. P.* (Hrsg.); Stuttgart 2000; zitiert als *Hobbes* (Hrsg. *Mayer* 2000).

Hobe, S., Einführung in das Völkerrecht, 8. Auflage, Tübingen 2008; zitiert als *Hobe* 2008, S.

Hochreiter, M., 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; zitiert als *Hochreiter* 2002, S.

Hoeren, T., Die Umsetzung der Richtlinie zur Vorratsdatenspeicherung - Konsequenzen für die Privatwirtschaft, JZ 2008, 668.

Hoeren, T., Vorratsdaten und Urheberrecht, Keine Nutzung gespeicherter Daten, NJW 2008, 3099.

Hoffmann, D., Die verfassungsrechtliche Problematik der Inpflichtnahme Privater am Beispiel der entschädigungslosen Inanspruchnahme der Kreditinstitute für das Kontenabrufverfahren (§ 24 KWG, §§ 93, 93b AO), WM 2010, 193.

Hoffmann-Riem, W., Der grundrechtliche Schutz der Vertraulichkeit und Integrität eigengenutzter informationstechnischer Systeme, JZ 2008, 1009.

Hoffmann-Riem, W., Gesetzliche Gewährleistung der Freiheit der Kommunikation im Internet?, in: *Ladeur, K.-H.* (Hrsg.), Innovationsoffene Regulierung des Internet, Neues Recht für Kommunikationsnetzwerke. Baden-Baden 2003, 53 – 82;
zitiert als *Hoffmann-Riem* 2003, S.

Hoffmann-Riem, W., Sicherheit braucht Freiheit, in: Kritische Justiz (Hrsg.), Verfassungsrecht und gesellschaftliche Realität, Dokumentation: Kongress "60 Jahre Grundgesetz: Fundamente der Freiheit stärken" der Bundestagsfraktion Bündnis 90/ Die Grünen am 13./ 14. März 2009 in Berlin. Baden-Baden 2009, 54 – 64;
zitiert als *Hoffmann*-Riem 2009, S.

Höfling, W., Art. 1, in: *Sachs, M.* (Hrsg.), Grundgesetz, Kommentar. München 2011;
zitiert als *Höfling,* in: *Sachs,* GG 2011, Art. 1 Rn.

Hofmann, H., Art. 20, in: *Schmidt-Bleibtreu, B./ Klein, F.* (Begr.); *Hofmann, H./ Hopfauf, A.* (Hrsg.), Kommentar zum Grundgesetz 2011;
zitiert als *Hofmann,* in: *Schmidt-Bleibtreu/Klein*, GG 2011, Art. Rn.

Hofmann, H., Die versprochene Menschenwürde, Antrittsvorlesung 21. Januar 1993, AöR 118 (1993), 353.

Hömig, D., Grundgesetz, Handkommentar, 8. Auflage, Baden-Baden, 2007;
zitiert als: *Bearbeiter,* in: *Hömig* Hnd. Komm GG 2007, Art. Rn.

Hopfauf, A., Kommentierung in: *Schmidt-Bleibtreu,* B./ *Klein*, F. (Begr.); *Hofmann, H./ Hopfauf, A.* (Hrsg.), GG, Kommentar zum Grundgesetz 2011;
zitiert als *Hopfauf,* in: *Schmidt-Bleibtreu/Klein*, GG 2011, Art. Rn.

Horn, H.-D., Sicherheit und Freiheit durch vorbeugende Verbrechensbekämpfung - Der Rechtsstaat auf der Suche nach dem rechten Maß, in: Horn, Hans-Detlef (Hrsg.), Festschrift für Walter Schmitt Glaeser zum 70. Geburtstag, Berlin 2003, 435 – 462;
zitiert als *Horn* 2003, S.

Hornig, J., Sicherheit statt Freiheit? Eichstätt 2009;
abrufbar unter: http://d-nb.info/1003616496/34.

Hornung, *G.,* Der Personenbezug biometrischer Daten, DuD 2004, 218.

Hornung, G., Zwei runde Geburtstage: Das Recht auf informationelle Selbstbestimmung und das WWW, MMR 2004, 3.

Hornung, G., Die digitale Identität, Rechtsprobleme von Chipkartenausweisen: digitaler Personalausweis, elektronische Gesundheitskarte, JobCard-Verfahren, 1. Auflage, Baden-Baden 2005.

Hornung, G., Wireless und speicherpflichtig? Die Vorratsdatenspeicherung und der Betrieb von W-LAN-Systemen, MMR 2007, XIII.

Hornung, G., Eine Datenschutz-Grundverordnung für Europa?, Licht und Schatten im Kommissionsentwurf vom 25.1.2012, ZD 2012, 99.

Hornung, G., Datenschutz – nur solange der Vorrat reicht? Die Speicherung von Telekommunikationsverkehrsdaten als Problem der Abwägungskompetenz im Mehrebenensystem, in: *Busch, A. / Hofmann, J.* (Hrsg.), Politik und die Regulierung von Information, PVS-Sonderheft 46/2012, 377-407;
zitiert als *Hornung* PVS 2012, 377, S.

Hornung, G., Keine Vorratsdatenspeicherung bei Fluggästen, ZRP 2013, 97.

Hornung, G./ Schnabel, C., Verfassungsrechtlich nicht schlechthin verboten - Das Urteil des Bundesverfassungsgerichts in Sachen Vorratsdatenspeicherung, DVBl. 2010, 824.

Huber, B., Die Reform der parlamentarischen Kontrolle der Nachrichtendienste und des Gesetzes nach Art. 10 GG, NVwZ 2009, 1321.

Hubmann, *H.,* Das Persönlichkeitsrecht, 1. Auflage, Böhlau 1953.

Hufen, F., Die Menschenwürde, Art. 1 Abs. 1 GG, JuS 2010, 1.

Humboldt, W. v., Schriften zur Anthropologie und Geschichte, *Filtner, A./ Giel, K*. (Hrsg.). Darmstadt 1960;
zitiert als *Humboldt* 1960.

Hund, H., Überwachungsstaat auf dem Vormarsch - Rechtsstaat auf dem Rückzug?, NJW 1992, 2118.

Hüsken, B./ Mann, S., Der Staat als "Homo Oeconomicus"?, Drei Säulen des Wirtschaftlichkeitsvergleichs bei Public Private Partnerships, DÖV 2005, 143.

Huster, S./ Rudolph, K. (Hrsg.), Vom Rechtsstaat zum Präventionsstaat, 1. Auflage, Frankfurt am Main 2008.

Huster, S./ Rux, J., Art. 20 in *Epping, V./ Hillgruber, C.* (Hrsg.), Beck'scher Online-Kommentar zum Grundgesetz. München 2011;
zitiert als *Huster/Rux,* in: BeckOK-GG, 2011, Art. Rn.

IfD Allensbach Der Wert der Freiheit, Ergebnisse zur Grundlagenstudie zum Freiheitsverständnis der Deutschen, Oktober/November 2003, abrufbar unter: http://www.ifd-allensbach.de/pdf/akt_0406.pdf;
zitiert als *IfD Allensbach* 2003, S.

Ignor, A., Der rechtliche Schutz des Vertrauensverhältnisses zwischen Rechtsanwalt und Mandant im Visier des Gesetzgebers, NJW 2007, 3403.

Ipsen, J., „Stufentheorie" und Übermaßverbot – Zur Dogmatik des Art. 12 GG, JuS 1990, 634.

Isensee, J., Das Grundrecht auf Sicherheit, Zu den Schutzpflichten des freiheitlichen Verfassungsstaates. Berlin 1983.

Isensee, J., Der Verfassungsstaat als Friedensgarant, in: *Kirchhof, P. / Mellinghoff, R.* (Hrsg.), Die Erneuerung des Verfassungsstaates, Symposion aus Anlass des 60. Geburtstages von Prof. Paul Kirchhof, Heidelberg 2003, 7 – 43;
zitiert als *Isensee* 2003.

Isensee, J., Staat und Verfassung, § 15, in: *Isensee, J. / Kirchhof, P.* (Hrsg.), Verfassungsstaat, Handbuch des Staatsrechts der Bundesrepublik Deutschland, Bnd. II, Heidelberg 2004;
zitiert als *Isensee,* in: *Isensee/Kirchof* HStR II, § 15 Rn.

Isensee, J., Gemeinwohl im Verfassungsstaat, § 71, in: *Isensee, J. / Kirchhof, P.* (Hrsg.), Handbuch des Staatsrechts der Bundesrepublik Deutschland, Aufgaben des Staates, Bnd. IV, Heidelberg 2006;
zitiert als *Isensee,* in: *Isensee/Kirchof* HStR IV, § 71 Rn.

Isensee, J., Staatsaufgaben, § 73, in: *Isensee, J./ Kirchhof, P.* (Hrsg.), Handbuch des Staatsrechts der Bundesrepublik Deutschland, Aufgaben des Staates, Bnd. IV, Heidelberg 2006;
zitiert als *Isensee,* in: *Isensee/Kirchof* HStR IV, § 73 Rn.

Jachmann, M., Art. 33, in: v. *Mangoldt, H/ Klein, F./ Starck, C.*, Das Bonner Grundgesetz Kommentar, München 2010;
zitiert als *Jachmann,* in: *Mangoldt/Klein,* GG 2010, Art. 33 Rn.

Jäger, W., Vorfeldermittlungen - Reizwort und Streitgegenstand, Ein Befund widerstreitender Interessen, Kriminalistik 1995, 189.

Jakab, É., Freiheit und Sicherheit in Platons Nomoi, in: *Krasai, K./ Nagy, F./ Szomora, Z.* (Hrsg.), Freiheit - Sicherheit - (Straf)Recht, Beiträge eines Humboldt-Kollegs, Osnarück 2011, 127 – 140;
zitiert als *Jakab* 2011.

Jakowatz, S., Herausforderung „Terrorismus" Politik der inneren Sicherheit und der internationalen Gefahrenabwehr, gesis (Leibniz-Institut für Sozialwissenschaften); Recherche Spezial, 7/2010, abrufbar unter:
http://www.gesis.org/sowiport/fileadmin/user_upload/pdf_recherche_spezial/rs_10_07_terror_online.pdf;
zitiert als *Jakowatz* 2010.

Jandt, S./ Roßnagel, A./ Volland, B., Datenschutz für Smart Meter - Spezifische Neuregelungen im EnWG, ZD 2011, 99.

Jarass, H. D./ Pieroth, B., Grundgesetz für die Bundesrepublik Deutschland: Kommentar, 11. Auflage, München 2011;
zitiert als *Bearbeiter,* in: *Jarass/Pieroth,* GG 2011, Art. Rn.

Jellinek, G., Allgemeine Staatslehre, 3. Auflage, Darmstadt 1959;
zitiert als *Jellinek,* Allgemeine Staatslehre 1959, S.

Jenny, V., Eile mit Weile - Vorratsdatenspeicherung auf dem Prüfstand, CR 2008, 282 ff.

Jestaedt, M., Bundesstaat als Verfassungsprinzip, § 29, in: *Isensee, J./ Kirchhof, P.* (Hrsg.), Verfassungsstaat, Handbuch des Staatsrechts der Bundesrepublik Deutschland, Bnd. II, Heidelberg 2004;
zitiert als *Jestadt,* in: HStR II, § 29 Rn.

Joecks, W./ Miebach, K. (Hrsg.)*,* Münchner Kommentar zum Strafgesetzbuch, in 3 Bänden, München 2011;
zitiert als *Bearbeiter,* in: MüKo 2011, § Rn.

JungdemokratInnen / Junge Linke. Landesverbände Berlin & Brandenburg (Hrsg.), Freiheit stirbt mit Sicherheit, Handbuch gegen Überwachung und Ausgrenzung. Berlin 2001;
zitiert als *JungdemokratInnen et al.* 2001.

Kahl, W., Vom weiten Schutzbereich zum engen Gewährleistungsgehalt, Kritik einer neuen Richtung der deutschen Grundrechtsdogmatik, Der Staat 2004, 167.

Kamlah, R., Datenüberwachung und Bundesverfassungsgericht, DÖV 1970, 361

Karg, M., IP-Adressen sind personenbezogene Verkehrsdaten, MMR-Aktuell, 315811.

Kaufmann-Bühler, W., EUV Art. 43 Missionen und Operationen,
in: *Grabitz, E./ Hilf, M./ Nettesheim, M.* (Hrsg.), Das Recht der Europäischen Union, 48. Auflage, München 2012;
zitiert als *Kaufmann-Bühler*, in: *Grabitz/Hilf/Nettesheim,* EUR 2012, Art. 43 EUV Rn.

Kersten, J., Das Klonen von Menschen, Eine verfassungs-, europa- und völkerrechtliche Kritik. Tübingen 2004.

Kersten, J., Die genetische Optimierung des Menschen, JZ 2011, 161.

Kettler, D., Die Drei-Elemente-Lehre, Ein Beitrag zu Jellineks Staatsbegriff, seiner Fortführung und Kritik 199.

Kinast, K./ Schmitz, A., Vorratsdatenspeicherung – was vom Verbot umfasst ist, NJW-aktuell 2011 Nr. 40, 14.

Kindler, W., Freiheit braucht Sicherheit - Sicherheit braucht Freiheit, in: *Bundeskriminalamt* (Hrsg.) Informations- und Kommunikationskriminalität; BKA Polizei und Forschung, Bd. 27 zur Herbsttagung 'Informations- und Kommunikationskriminalität' 2003; München 2004; S. 147 – 158;
zitiert als *Kindler* 2004, S.

Kindt, A., Die grundrechtliche Überprüfung der Vorratsdatenspeicherung: EuGH und BVerfG - wer traut sich?, MMR 2009, 661.

Kirchof, P. Die Identität der Verfassung, § 21, in: *Isensee, J./ Kirchhof, P.* (Hrsg.), Handbuch des Staatsrechts der Bundesrepublik Deutschland, Bnd. II, Verfassungsstaat, 3. Auflage, Heidelberg 2004;
zitiert als *Kirchof,* in: HStR II § 21.

Kläner, T., Kommentar zu BVerfG, Urteil vom 2.3.2010, NJ 2010, 204.

Klee, R., Neue Instrumente zur Zusammenarbeit von Polizei und Nachrichtendiensten, Geltung, Rang und Reichweite des Trennungsgebots, Baden-Baden 2010.

Klein, E./ Schmahl, S., Die Internationalen und die Supranationalen Organisationen, 5. Abschnitt in: *Vitzthum, W.* (Hrsg.), Völkerrecht, Berlin 2010, 5. Abschnitt;
zitiert als *Klein/Schmahl,* in: *Vitzthum,* VR 2010, Abschnitt 5, Rn.

Klesczewski, D., Anmerkung BVerfG v. 2.3.2010, JZ 2010, 629 ff.

Klesczewski, D., Straftataufklärung im Internet -Technische Möglichkeiten und rechtliche Grenzen von strafprozessualen Ermittlungseingriffen im Internet, ZStW 2011 (123), 737.

Kloepfer, M., Verfassungsrecht, Band I: Grundlagen, Staatsorganisationsrecht, Bezüge zum Völker- und Europarecht. München 2011;
zitiert als *Kloepfer,* Verfassungsrecht I 2011, § Rn.

Kloepfer, M., Verfassungsrecht, Band II: Grundrechte. München 2010;
zitiert als *Kloepfer,* Verfassungsrecht II, 2010 § Rn.

Klug, C./ Reif, Y., Vorratsdatenspeicherung in Unternehmen?, Gesetzeslage und Ausblick, RDV 2008, 89.

Knierim, A., Kumulation von Datensammlungen auf Vorrat, ZD 2011, 17.

Knierim, A., Technikgestaltung bei Vorratsdatenspeicherung & Quick-Freeze, in: *Schartner, P./ Taeger, J.* (Hrsg.), D-A-CH security 2011, Bestandsaufnahme, Konzepte, Anwendungen, Perspektiven, Klagenfurt 2011, 480 – 490;
zitiert als *Knierim* 2011a.

Knierim, A., Vorhang auf für ein Vorratsdatenurteil 2.0?, in: *Taeger, J.* (Hrsg.), Die Welt im Netz, Folgen für Wirtschaft und Gesellschaft; Tagungsband Herbstakademie 2011, Edewecht 2011, 431 – 447;
zitiert als *Knierim* 2011b.

Kniesel, M., Innere Sicherheit und Grundgesetz, ZRP 1996, 482.

Koch, F., Rechtsprobleme privater Nutzung betrieblicher elektronischer Kommunikationsmittel, NZA 2008, 911.

Koep-Kerstin, W./ Will, R., Merkmale der deutschen Sicherheitspolitik nach dem 11. September, in: *Rzepka, D.* (Hrsg.), Graubuch Innere Sicherheit, Die schleichende Demontage des Rechtsstaates nach dem 11. September 2001, Norderstedt 2009, 13 – 15;
zitiert als *Koep-Kerstin/Will* 2009, S.

König, D./ Peters, A., Kap. 21, in: *Grote, R./ Marauhn, T.* (Hrsg.), EMRK/GG , Konkordanzkommentar zum europäischen und deutschen Grundrechtsschutz, Tübingen 2006;
zitiert als *König/Peters,* in: EMRK/GG 2006, Kap. 21 Rn.

Kotzur, M., Der Schutz personenbezogener Daten in der europäischen Grundrechtsgemeinschaft, Die korrespondierende Verantwortung von EuGH, EGMR und mitgliedstaatlichen Verfassungsgerichten, EuGRZ 2011, 105.

Kramer, S., Gestaltung betrieblicher Regelungen zur IT-Nutzung, ArbR Aktuell 2010, 164 ff.

Krauss, R. v., Der Grundsatz der Verhältnismäßigkeit, In seiner Bedeutung für die Notwendigkeit des Mittels im Verwaltungsrecht, Hamburg 1955.

Krüger, S./ Maucher, S.-A., Ist die IP-Adresse wirklich ein personenbezogenes Datum?, Ein falscher Trend mit großen Auswirkungen auf die Praxis, MMR 2011, 433.

Kube, H., Art. 14 in *Maunz, T./ Dürig, G*., Grundgesetzkommentar, Loseblatt. München 2011/2012;
zitiert als *Kube,* in: *Maunz/Dürig,* GG 2011, Art. 14, Rn.

Kube, H., Der eingriffsrechtfertigende Konnex - Zu Inhalt und Grenzen freiheitsbegleitender Verantwortung, JZ 2010, 265.

Kube, H./ Palm, U./ Seiler, C., Zur Finanzierungsverantwortung für Gemeinwohlbelange, Zu den finanzverfassungsrechtlichen Maßstäben quersubventionierender Preisinterventionen, NJW 2003, 927.

Kühling, J., Freiheitsverluste im Austausch gegen Sicherheitshoffnungen im künftigen TKG?, K&R 2004, 105 ff.

Kunig, P., Art. 2 in: *Münch, I. v./Kunig, P.* (Hrsg.), Grundgesetzkommentar, 6. Auflage, München 2012;
zitiert als *Kunig,* in: *Münch/Kunig,* GG 2012, Art. 2 Rn.

Kurose, J. F./ Ross, K. W., Computernetzwerke, Der Top-Down-Ansatz, 4. Auflage, München 2008;
zitiert als *Kurose* 2008, S.

Kurz, C./ Rieger, F., Stellungnahme des Chaos Computer Clubs zur Vorratsdatenspeicherung, v. 9. Juni 2009; abrufbar unter http://213.73.89.124/vds/VDSfinal18.pdf;
zitiert als *Kurz/Rieger* 2009, S.

Kurz, C./ Rieger, F., Die Datenfresser, Wie Internetfirmen und Staat sich unsere persönlichen Daten einverleiben und wie wir die Kontrolle darüber zurückerlangen, 2. Auflage, Frankfurt am Main 2011.

Kutscha, M., Überwachungsmaßnahmen von Sicherheitsbehörden im Fokus der Grundrechte, LKV 2008, 481.

Lang, H., Art. 2, in: *Epping, V./ Hillgruber, C. (Hrsg.),* Beck'scher Online-Kommentar zum Grundgesetz, München 2010;
zitiert als *Lang,* in: BeckOK GG, Art. Rn.

Lange, N., Vorermittlungen, Die Behandlung des staatsanwaltschaftlichen Vorermittlungsverfahrens unter besonderer Berücksichtigung von Abgeordneten, Politikern und Prominenten, Frankfurt am Main; New York 1999.

Lenk, K., ELENA oder der Weg in die durchorganisierte Informationsgesellschaft, VM 2010, 137.

Lerche, P., Übermass und Verfassungsgrecht, Zur Bindung des Gesetzgebers an die Grundsätze der Verhältnismäßigkeit und der Erforderlichkeit 1961.

Lessig, L., Code, und andere Gesetze des Cyberspace. Berlin 2001 (im Original 1999 bei Basic Books, New York).

Leutheusser-Schnarrenberger, S., Vorratsdatenspeicherung - Ein vorprogrammierter Verfassungskonflikt, ZRP 2007, 9.

Link, H.-C., Staatszwecke im Verfassungsstaat - nach 40 Jahre Grundgesetz, VVDStRL 1990, 7.

Lisken, H., Zur polizeilichen Rasterfahndung, NVwZ 2002, 513.

LKA Baden-Württemberg, IuK-Kriminalität Jahresbericht 2010, Stuttgart 2011, abrufbar unter: http://www.lka-bw.de/LKA/statistiken/Documents/IuK_Kriminalitaet_2010.pdf;
zitiert als *LKA Baden-Württemberg,* S.

Lorenz, D., Die verdeckte Onlinedurchsuchung als Herausforderung an die Grundrechtsdogmatik, in: *Lerche, P. / Scholz, R.* (Hrsg.), Realitätsprägung durch Verfassungsrecht, Kolloquium aus Anlass des 80. Geburtstages von Peter Lerche, Berlin 2008, 31 ff;
zitiert als *Lorenz* 2008, 31.

Lorenz, D., Art. 2, in: *Dolzer, R. / Kahl, W./ Waldhoff, C./ Graßhof, K.* (Hrsg.), Bonner Kommentar zum Grundgesetz, Heidelberg 2011;
zitiert als *Lorenz,* in: BK-GG 2011, Art. 2 Rn.

Luhmann, N., Soziologie des Risikos, 1. Auflage, Berlin 1991.

Luhmann, N., Grundrechte als Institution, Ein Beitrag zur politischen Soziologie, 4. Auflage, Berlin 1999 (Erstausgabe 1986).

Maaßen, S., Urheberrechtlicher Auskunftsanspruch und Vorratsdatenspeicherung, MMR 2009, 511.

Mahnken, E., Mindestspeicherungsfristen für Telekommunikationsverbindungsdaten, *Bundeskriminalamt* (Hrsg.) v. 15.11.2005, abrufbar unter: https://www.vorratsdatenspeicherung.de/images/bka_vorratsdatenspeicherung.pdf; zitiert als *Mahnken* 2005.

Manssen, G., Art. 12, in: in: v. *Mangoldt, H/ Klein, F./ Starck, C*., Das Bonner Grundgesetz Kommentar, München 2010; zitiert als *Manssen,* in: *Mangoldt/Klein/Starck,* GG 2010, Art. 12 Rn.

Manssen, G., Das Telekommunikationsgesetz (TKG) als Herausforderung für die Verfassungs- und Verwaltungsrechtsdogmatik, Archiv PT 1998, 236.

Maras, M.-H., From targeted to mass surveillance: is the EU Data Retention Directive a necessary measure or an unjustified threat to privacy?, in: *Goold, B/ Neyland, D.* (Hrsg.), New Directions In Surveillance And Privacy, Cullompton, Devon; Portland, 2009, 74ff.; zitiert als *Maras* 2009, S.

Markowitz, M./ Bergemann, N,. Die Anti-Terrordatei, v. 24.7.2009, abrufbar unter: http://www.datenschutz.de/feature/detail/?featid=9; zitiert als *Markowitz/Bergemann* 2009.

Marlie, M./ Bock, D., Zur Verwertbarkeit der vor der Entscheidung des BVerfG zur Vorratsdatenspeicherung erlangten retrograden Verbindungsdaten, Zugleich Überlegungen zu OLG Hamm, Beschl. v. 13.4.2010 - 3 Ws 140/10 und LG Verden Beschl. v. 3.5.2010 - 7 KLs 2/10, ZIS 2010, 524.

Mattern, F. (Hrsg.), Total vernetzt, Szenarien einer informatisierten Welt; 7. Berliner Kolloquium der Gottlieb Daimler- und Karl Benz-Stiftung. Berlin 2003; zitiert als *Mattern* 2003, S.

Maunz, T./ Dürig, G (Begr.)*.,* Grundgesetz Kommentar, Loseblatt., (Hrsg. v. Herzog, R.; Scholz, R.; Herdegen, M; Klein, H.), München 2011/2012; zitiert als *Bearbeiter,* in: *Maunz/Dürig*, GG 2012, Art., Rn.

Maurer, J., Mindestspeicherfristen, Praktische Erfahrungen aus Sicht der Polizei, Beitrag zur SIRA-Konferenz 2011, abrufbar unter: http://www.sira-security.de/wp-content/uploads/JProzentC3ProzentBCrgen-Maurer-SIRA-Thesenpapier-110526.pdf; zitiert als *Maurer* 2011, S.

Mayer, C., Pflicht zur Vorratsdatenspeicherung bei unentgeltlichen E-Mail-Diensten?, K&R 2009, 313.

Meinicke, D., Aktuelle Strafprozessuale Folgefragen des „Vorratsdatenurteils“ des BVerfG, HRRS 2011, 398.

Meinicke, D., Anmerkung zu einer Entscheidung des AG Reutlingen, Beschl. v. 31.10.2011, Zur Beschlagnahme von (Facebook-)Nutzerkonten, StV 2012, 463.

Merten, D., Das Prinzip Freiheit im Gefüge der Staatsfundamentalbestimmungen, § 27, in: *Badura, P.* (Hrsg.), Handbuch der Grundrechte in Deutschland und Europa, Grundrechte in Deutschland - Allgemeine Lehren I, Heidelberg 2006;
zitiert als *Merten,* in: HGR I, 2006, § 27 Rn.

Meyer, Ch./ Behrens, S. Bis zum Ende von NAT, c't 5/2012, 180.

Meyer, F., Der Grundsatz der Verfügbarkeit, NStZ 2008, 188.

Meyer, F./ Macke, J., Rechtliche Auswirkungen der Terroristenlisten im deutschen Recht, HRRS 2007, 445.

Meyer, J./ Bernsdorff, N. (Hrsg.), Kommentar zur Charta der Grundrechte der Europäischen Union, 1. Auflage, Baden-Baden 2003;
zitiert als *Bearbeiter* in *Meyer,* EU-GRCh. 2003, Art.

Meyer, K., Grenzen der Unschuldsvermutung, in: *Tröndle, H./ Vogler, T.* (Hrsg.), Festschrift für Herbert Tröndle, zum 70. Geburtstag am 24. August 1989. Berlin, New York 1989, S. 61-76;
zitiert als *Meyer,* in: FS Tröndle 1989, S.

Meyerdierks, P., Sind IP-Adressen personenbezogene Daten, MMR 2009, 8.

Meyer-Ladewig, J., EMRK Handkommentar, 3. Auflage, Baden-Baden 2011;
zitiert als: *Meyer-Ladewig,* EMRK Hd. Komm 2011, Art. Rn.

Michael, L., Die drei Argumentationsstrukturen des Grundsatzes der Verhältnismäßigkeit -, Zur Dogmatik des Über- und Untermaßverbotes und der Gleichheitssätze, JuS 2001, 148.

Möllers, M. H. W., Innenpolitische Dimensionen der Sicherheitspolitik in Deutschland, in: *Böckenförde, S./ Gareis, S.* (Hrsg.), Deutsche Sicherheitspolitik, Herausforderungen, Akteure und Prozesse, Opladen & Farmington Hills 2009, 131 – 172;
zitiert als *Möllers* 2009, S.

Morasch, K./ Bartholomae, F., Internationale Wirtschaft, Handel und Wettbewerb auf globalen Märkten, Stuttgart 2011.

Möstl, M., Die staatliche Garantie für die öffentliche Sicherheit und Ordnung, Sicherheitsgewährleistung im Verfassungsstaat, im Bundesstaat und in der Europäischen Union, Tübingen 2002.

Möstl, M., Die neue dogmatische Gestalt des Polizeirechts - Thesen zur Integration eines modernen informationellen Vorfeldrechts in das klassische rechtsstaatliche Gefahrenabwehrrecht, DVBl. 2007, S. 581.

Möstl, M., Das Bundesverfassungsgericht und das Polizeirecht, Eine Zwischenbilanz aus Anlass des Urteils zur Vorratsdatenspeicherung, DVBl. 2010, 808.

Möstl, M., Vorratsdatenspeicherung – wie geht es weiter?, ZRP 2011, 225.

Mozek, M./ Zendt, M., Telefonieren über das Internet, Teil 23, in: *Hoeren, T./ Sieber, U.* (Hrsg.) Handbuch Multimediarecht, 31. Erg.Lief. 2012;
zitiert als *Mozek/Zendt,* in: *Hoeren/Sieber* 2012, Teil 23 Rn.

Mückenberger, U., Datenschutz als Verfassungsgebot, Das Volkszählungsurteil des Bundesverfassungsgerichts, KJ 1984, 1.

Müller-Dietz, H., Zur negativen Utopie von Recht und Staat - am Beispiel des Romans "Corpus Delicti" von Juli Zeh, JZ 2011, 85.

Müller-Franken, S., Vorbemerkung zu Art. 1, Kommentierung, in: *Schmidt-Bleibtreu, B./ Klein, F.* (Begr.); *Hofmann, H./ Hopfauf, A.* (Hrsg.), GG, Kommentar zum Grundgesetz 2011;
zitiert als *Müller-Franken,* in: *Schmidt-Bleibtreu/Klein*, GG 2011.

Müller-Kullmann, W., Kommentierung § 5 EnEG, in *Danner, W./Theobald, C.* (Hrsg.) Energierecht. München 2012;
zitiert als *Müller-Kullmann,* in: *Danner/Theobald,* Energierecht 2012, § 5 EnEG Rn.

Murswiek, D., Art. 2, in: *Sachs, M.* (Hrsg.), Grundgesetz, Kommentar, München 2011;
zitiert als *Murswiek,* in: *Sachs* GG 2011, Art. 2 Rn.

Nazari-Khanachayi, A., Sicherheit vs. Freiheit - der moderne Rechtsstaat vor neuen Herausforderungen, JA 2010, 761.

Nehm, K., Das nachrichtendienstrechtliche Trennungsgebot und die neue Sicherheitsarchitektur, NJW 2004, 3289.

Nettesheim, M., Wirtschaftsverfassung und Wirtschaftspolitik, § 19 in: *Oppermann, T./ Classen, C. D./ Nettesheim, M.* (Hrsg.), Europarecht, München 2009;
zitiert als *Nettesheim,* in: *Oppermann/Classen/Nettesheim* EuR 2009, § 19, Rn.

Neuhöfer, D., Anmerkung zum Beschluss des AG Reutlingen vom 31.10.2011 (5 Ds 43 Js 18155/10 jug; CR 2012, 93) - Zur Frage der Beschlagnahme von Facebook-Daten, ZD 2012, 178.

Neumann, D., Vorsorge und Verhältnismäßigkeit, Die kriminalpräventive Informationserhebung im Polizeirecht. Berlin 1993.

Nolte, M., Die Anti-Terror-Pakete im Lichte des Verfassungsrechts, DVBl. 2002, 573.

Nusser, J., Die Bindung der Mitgliedstaaten an die Unionsgrundrechte, Vorgaben für die Auslegung von Art. 51 Abs. 1 S. 1 EuGrCh., Tübingen 2011.

O'Ballance, E., Terror in Ireland, The heritage of hate. Novato, CA 1981.

Ohler, C., Anmerkung BVerfG Urt. v. 2.3.2010, JZ 2010, 626.

Oppermann, T., Wesen der Europäischen Union, § 5, in: *Oppermann, T./ Classen, C. D./ Nettesheim, M.* (Hrsg.), Europarecht, München 2009;
zitiert als *Oppermann,* in: *Oppermann/Classen/Nettesheim* EuR 2009 § 5 Rn.

Orantek, K., Die Vorratsdatenspeicherung in Deutschland, NJ 2010, 193.

Pagenkopf, M., Art. 10, in: *Sachs, M.* (Hrsg.), Grundgesetz, Kommentar. München 2011; zitiert als *Pagenkopf,* in: *Sachs,* GG 2011, Art. 10 Rn.

Pahlen-Brandt, *I.,* Datenschutz braucht scharfe Instrumente, Ein Beitrag zur Diskussion um „personenbezogene Daten", DuD 2008, 34.

Papier, H.-J., in *Maunz, T./ Dürig, G.*, Grundgesetzkommentar, Loseblatt, München 2011/2012;
zitiert als *Papier,* in: *Maunz/Dürig,* GG 2011, Art. 14, Rn.

Papier, H.-J., Rechtsstaat im Risiko, DVBl. 2010, 801.

Petersen, J., Wilhelm von Humboldt (1767-1835), Die rechts- und staatsphilosophischen Ideen Wilhelm von Humboldts als Grundlage einer Bildungsreform, in: *Grundmann, S.* (Hrsg.), Festschrift 200 Jahre Juristische Fakultät der Humboldt-Universität zu Berlin, Geschichte, Gegenwart und Zukunft; Berlin, New York 2010; S. 115 – 132;
zitiert als *Petersen* 2010, S.

Petri, *T.,* Im Schatten des Leviathan, Zum Verhältnis von Sicherheit und Freiheit anhand von Beispielen aus der TK-Überwachung, RDV 2003, 16.

Petri, T., Unzulässige Vorratssammlungen nach dem Volkszählungsurteil? Die Speicherung von TK-Verkehrsdaten und Flugpassagierdaten, DUD 2008, 729.

Petri, T., Die Richtlinie 2006/24/EG zur Vorratsspeicherung von Telekommunikationsverkehrsdaten, DUD 2011, 607.

Petri, T., Informationsverarbeitung im Polizei- und Strafverfahrensrecht, Abschnitt G, in: *Denninger, E./ Rachor, F.* (Hrsg.)*, Lisken, H. (*begr.), Handbuch des Polizeirechts, Gefahrenabwehr – Strafverfolgung – Rechtsschutz, 5. Auflage,München 2012;
zitiert als: *Petri,* in: *Lisken/Denninger* 2012, G, Rn.

Peukert, W., Art. 1 des 1. ZP (Schutz des Eigentums), in: *Frowein, J./ Peukert, W.* (Hrsg.), EMRK-Kommentar, Kehl am Rhein 2009;
zitiert als *Peukert,* in: *Frowein/Peukert,* EMRK 2009, Art. 1 ZP 1 Rn.

Pfeiffer G., Einleitung in: *Hannich, R.* (Hrsg.), Karlsruher Kommentar zur Strafprozessordnung, 6. Auflage, München 2008;
zitiert als *Pfeiffer,* in: KarlsruherKomm StPO, Einl. Rn.

Pfitzmann, A./ Köpsell, S., Risiken der Vorratsdatenspeicherung - Grenzen der Nutzungsüberwachung, DUD 2009, 542 ff.

Pieroth, B./ Schlink, B./ Kniesel, M., Polizei- und Ordnungsrecht, 7. Auflage,München 2012;
zitiert als *Pieroth/Schlink/Kniesel* 2012, § Rn.

Podlech, Prinzipien des Datenschutzes in der öffentlichen Verwaltung. Allgemeiner Teil einer Begründung zum Entwurf eines Bundes-Datenschutz-Rahmengesetzes in: *Kilian, W./ Lenk, K./ Steinmüller, W.* (Hrsg.), Datenschutz; Juristische Grundsatzfragen beim Einsatz elektronischer Datenverarbeitungsanlagen in Wirtschaft und Verwaltung, Frankfurt am Main 1973;
zitiert als *Podlech* 1973, S.

Podlech, A., Die Begrenzung staatlicher Informationsverarbeitung durch die Verfassung angesichts der Möglichkeit unbegrenzter Informationsverarbeitung mittels der Technik, zur Entscheidung des Bundesverfassungsgerichts über das Volkszählungsgesetz 1983, Leviathan 1984, 85.

Polenz, S., Speicherpflicht für Unternehmer nach § 113a TKG, CR 2009, 225

Polenz, S., Teil 13: Rechtsquellen und Grundbegriffe des Allgemeinen Datenschutzes; Verfassungsrechtliche Grundlagen des Datenschutzes, in: *Kilian, W./ Heussen, B.* (Hrsg.), Computerrechts-Handbuch, Informationstechnologie in der Rechts- und Wirtschaftspraxis, 29. Erg.-Lieferung., München 2011;
zitiert als *Polenz,* in: *Kilian/Heussen*, Teil 13 Rn.

Pordesch, U., Informatisierung und neue Polizeistrategien, in: *Roßnagel*, A. (Hrsg.), Freiheit im Griff, Informationsgesellschaft und Grundgesetz, Stuttgart 1989, 87 – 106;
zitiert als *Pordesch,* in: *Roßnagel* 1989, S.

Poscher, R., Menschenwürde und Kernbereichsschutz, Von den Gefahren einer Verräumlichung des Grundrechtsdenkens, JZ 2009, 269.

Prantl, H., Der Terrorist als Gesetzgeber, Wie man mit Angst Politik macht. München 2008;
zitiert als *Prantl* 2008.

Puschke, J./ Singelnstein, T., Telekommunikationsüberwachung, Vorratsdatenspeicherung und sonstige heimliche Ermittlungsmaßnahmen der StPO nach der Neuregelung zum 1.1.2008, NJW 2008, 113.

Pütter, N., Spielarten und Abgründe einer populären Überzeugung, Bürgerrechte & Polizei / CILIP 2007, Heft Nr. 1, S. 3 ff.

Putzke, H., Schriftliche Stellungnahme zum Gesetzentwurf der Bundesregierung „Entwurf eines Gesetzes über die Vereinfachung des Austauschs von Informationen und Erkenntnissen zwischen den Strafverfolgungsbehörden der Mitgliedstaaten der Europäischen Union", BT-Drucksache 17/5096, BT (Innenausschuss) Ausschussdrucksache 17(4)336 G, abrufbar unter:
http://www.bundestag.de/bundestag/ausschuesse17/a04/Anhoerungen/Anhoerung12/Stellungnahmen_SV/Stellungnahme_07.pdf;
zitiert als *Putzke* 2007, S.

Raabe, O./ Lorenz, M./ Pallas, F./ Weis, E./ Malina, A., 14 Thesen zum Datenschutz im Smart Grid, DuD 2011, 519.

Rath, C., Der Überwachungsstaat – eine bürgerrechtliche Projektion, vorgänge 1984 (2008), 79.

Redeker, H., IT-Recht, 5. Auflage, München 2012.

Richter, D., Kap. 9, in: *Grote, R./ Marauhn, T.* (Hrsg.), EMRK/GG , Konkordanzkommentar zum europäischen und deutschen Grundrechtsschutz, Tübingen 2006;
zitiert als *Richter,* EMRK/GG , Kap. 9, Rn.

Richter, P., Datenschutz bei Internetdiensten nach der DS-GVO – Vergleich der deutschen Rechtslage mit dem Kommissionsentwurf, ZD 2012, 407.

Richter, P., Datenschutz durch Technik und die Grundverordnung der EU-Kommission, DuD 2012, 576.

Robbers, G., Sicherheit als Menschenrecht, Aspekte der Geschichte, Begründung und Wirkung einer Grundrechtsfunktion, 1. Auflage, Baden-Baden 1987.

Robbers, *G.,* Art. 20, in: *Dolzer, R. / Kahl, W./ Waldhoff, C./ Graßhof, K.* (Hrsg.), Bonner Kommentar zum Grundgesetz, Heidelberg 2011;
zitiert als *Robbers* in BK-GG 2011, Art. 20 Rn.

Roggan, F./ Bergemann, N., Die "neue Sicherheitsarchitektur" der Bundesrepublik Deutschland, Anti-Terror-Datei, gemeinsame Projektdateien und Terrorismusbekämpfungsgesetz, NJW 2007, 876.

Roggenkamp, J., Schutz und Sicherheit in der virtuellen Welt, K&R 2012, Nr. 2, Editorial.

Rohlf, D., Der grundrechtliche Schutz der Privatsphäre. Berlin 1980.

Ronellenfitsch, M., Der Dreiklang: Freiheit - Sicherheit - Datenschutz - ein Bermuda-Dreieck für die Grundrechte?, in: *Ronellenfitsch, M./ Wehrmann, R.* (Hrsg.), Freiheit Sicherheit Datenschutz, Wiesbaden 2008, S. 9 – 39;
zitiert als *Ronellenfitsch* 2008, S.

Rössel, M., BVerfG Urteil zur Vorratsdatenspeicherung, ITRB 2010, 74.

Rössel, M., Europarechtliche Grenzen der Filterpflicht eines Access-Providers, jurisPR-ITR 25/2011 Anm. 2.

Roßnagel, A., Bedroht die Kernenergie unsere Freiheit, München 1983.

Roßnagel, A., Radioaktiver Zerfall der Grundrechte?, Zur Verfassungsverträglichkeit der Kernenergie. München 1984.

Roßnagel, A., Möglichkeiten verfassungsverträglicher Technikgestaltung in: *Roßnagel, A.* (Hrsg.), Freiheit im Griff, Informationsgesellschaft und Grundgesetz. Stuttgart 1989, S. 177 – 186,
zitiert als: *Roßnagel* 1989, S.

Roßnagel, *A.,* Die parlamentarische Verantwortung für den technischen Fortschritt, *ZRP 1992*, 55.

Roßnagel, A., Freiheit im Cyberspace, Informatik-Spektrum 2002, 33.

Roßnagel, A., Handbuch Datenschutzrecht, Die neuen Grundlagen für Wirtschaft und Verwaltung, München 2003;
zitiert als *Roßnagel,* Hb. DSR 2003.

Roßnagel, A., Sicherheit für Freiheit?, Grundlagen und Fragen, in: *Roßnagel, A.* (Hrsg.), Sicherheit für Freiheit?, Riskante Sicherheit oder riskante Freiheit in der Informationsgesellschaft, Baden-Baden 2003, 17–46;
zitiert als *Roßnagel* 2003, S.

Roßnagel, A., Die EG-Richtlinie zur Vorratsspeicherung von Kommunikationsdaten, EuZW 2006, 30.

Roßnagel, A., Datenschutz in einem informatisierten Alltag, Gutachten im Auftrag der Friedrich-Ebert-Stiftung. Berlin 2007;
zitiert als *Roßnagel* 2007, S.

Roßnagel, A. (Hrsg.), Digitale Visionen, Zur Gestaltung allgegenwärtiger Informationstechnologien. Berlin 2008.

Roßnagel, A., Die Zukunft informationeller Selbstbestimmung: Datenschutz ins Grundgesetz und Modernisierung des Datenschutzkonzepts, in: Kritische Justiz (Hrsg.), Verfassungsrecht und gesellschaftliche Realität, Dokumentation: Kongress "60 Jahre Grundgesetz: Fundamente der Freiheit stärken" der Bundestagsfraktion Bündnis 90/ Die Grünen am 13./ 14. März 2009 in Berlin, Baden-Baden 2009, 99 – 119;
zitiert als *Roßnagel* 2009, S.

Roßnagel, A., Anmerkung zu EuGH v. 9.3.2010, Verurteilung Deutschlands zur Neuorganisation seiner Datenschützer, EuZW 2010, 299.

Roßnagel, A., Das Bundesverfassungsgericht und die Vorratsdatenspeicherung in Europa, DUD 2010, 544.

Roßnagel, A., Die "Überwachungs-Gesamtrechnung" - Das BVerfG und die Vorratsdatenspeicherung, NJW 2010, 1238.

Roßnagel, A., Das De-Mail-Gesetz – Grundlage für mehr Rechtssicherheit im Internet, NJW 2011, 1473.

Roßnagel, A., Das Gebot der Datenvermeidung und -sparsamkeit als Ansatz wirksamen technikbasierten Persönlichkeitsschutzes?, in: *Eifert, M./ Hoffmann-Riem, W.*(Hrsg.), Innovation, Recht und öffentliche Kommunikation, Berlin 2011, 41;
zitiert als *Roßnagel* 2011a, S.

Roßnagel, A., Datenschutz und Innere Sicherheit, in: Humanistische Union (Hrsg.), Perspektiven des nationalen und europäischen Schutzes der Bürger- und Menschenrechte, Erstes Gustav-Heinemann-Forum, Berlin 2011b, 35 - 54.;
zitiert als *Roßnagel* 2011b, S.

Roßnagel, A./ Bedner, M./ Knopp, M., Rechtliche Anforderungen an die Aufbewahrung von Vorratsdaten, DUD 2009, 536.

Roßnagel, A./ Hornung, G./ Knopp, M., De-Mail und Bürgerportale - Eine Infrastruktur für Kommunikationssicherheit, DUD 2009, 728.

Roßnagel, A./ Jandt, S./ Schnabel, C./ Yilniva-Hoffmann, Die Zulässigkeit einer Kulturflatrate nach nationalem und europäischem Rech, Kurzgutachten im Auftrag von: Bundestagsfraktion BÜNDNIS 90/DIE GRÜNEN und Fraktion der Grünen/Freie Europäische Allianz im Europäischen Parlament, v. 13.3.2009, abrufbar unter: http://www.gruene-bundestag.de/cms/netzpolitik/dokbin/278/278059.kurzgutachten_zur_kulturflatrate.pdf;
zitiert als *Roßnagel* et al. 13.3.2009.

Roßnagel, A./ Müller, J., Ubiquitous Computing - neue Herausforderungen für den Datenschutz, Ein Paradigmenwechsel und die von ihm betroffenen normativen Ansätze, CR 2004, 625.

Roßnagel, A./ Pfitzmann, A., Der Beweiswert von E-Mail, NJW 2003, 1209.

Roßnagel, A./ *Pfitzmann, A./Garstka, H.,* Modernisierung des Datenschutzrechts, Gutachten im Auftrag des Bundesministerium des Inneren, 2011, abrufbar unter: http://www.verwaltung-innovativ.de/nn_684264/SharedDocs/Publikationen /Bestellsevice/modernisierung__des__datenschutzrechts,templateId=raw,property=publicationFile.pdf/modernisierung_des_datenschutzrechts.pdf;
zitiert als: *Roßnagel/Pfitzmann/Garstka* 2011, S.

Roßnagel, A./ Scholz, P., Datenschutz durch Anonymität und Pseudonymität – Rechtsfolgen der Verwendung anonymer und pseudonymer Daten, MMR 2000, 721-731.

Roßnagel, A./ Moser-Knierim, A./ Schweda, S., Interessenausgleich im Rahmen der Vorratsdatenspeicherung. Baden-Baden, 2013.

Roßnagel, A. / Skistims, H., Rechtlicher Schutz vor Staatstrojanern?, ZD 2012, 3.

Roßnagel, A./ Wedde, P. / Hammer, V. / Pordesch, U., Digitalisierung der Grundrechte. Zur Verfassungsverträglichkeit der Informations- und Kommunikationstechnik, 1990.

Ruffert, M., Art. 12 in *Epping, V./ Hillgruber, C.* (Hrsg.), Beck'scher Online-Kommentar zum Grundgesetz. München 2010;
zitiert als *Ruffert,* in: BeckOK, 2010, Art. 12 GG, Rn.

Ruffert, M., Art. 15 in *Calliess, C./ Ruffert, M.* (Hrsg.), EUV/AEUV, Das Verfassungsrecht der Europäischen Union mit Europäischer Grundrechtecharta : Kommentar, 4. Auflage, München 2011;
zitiert als *Ruffert,* in: *Calliess/Ruffert* EUV/AEUV, 2011, Art. 15 Rn.

Rusteberg, B., Die EG- Richtlinie zur Vorratsspeicherung von Verkehrsdaten im System des europäischen Grund- und Menschenrechtsschutzes, VBlBW 2007, 171 ff.

Rzepka, D., Graubuch Innere Sicherheit, Die schleichende Demontage des Rechtsstaates nach dem 11. September 2001; *Gustav-Heinemann-Initiative & Humanistische Union* (Hrsg.). Norderstedt 2009;
zitiert als *Rzepka* 2009.

Sachs, M., Art. 20, in: *Sachs, M.* (Hrsg.), Grundgesetz, Kommentar, München 2011;
zitiert als *Sachs,* in: *Sachs,* GG, 2011, Art. 20 Rn.

Sacksofsky, U., Umweltschutz durch nicht-steuerliche Abgaben, zugleich ein Beitrag zur Geltung des Steuerstaatsprinzips, Tübingen 2000.

Sacksofsky, U./ Wieland, J., Vom Steuerstaat zum Gebührenstaat, Baden-Baden 2000.

Saeltzer, G., Sind diese Daten personenbezogen oder nicht?, Wie der Personenbezug von Daten, auch biometrischer, sich fundiert prüfen lässt…, DUD 2004, 218.

Saurer, J., Die Ausweitung sicherheitsrechtlicher Regelungsansprüche im Kontext der Terrorismusbekämpfung, NVwZ 2005, 275.

Schädler, W., Art. 8 EMRK, in: *Hannich, R.* (Hrsg.), Karlsruher Kommentar zur Strafprozessordnung, 6. Auflage, München 2008;
zitiert als *Schädler,* in: KarlsruherKomm StPO, Art. 8 EMRK Rn.

Schäfer, A., Nach dem permissiven Konsens. Das Demokratiedefizit der Europäischen Union, Leviathan 2006, 350-376.

Schäfer, J., § 89b in *Joecks, W./ Miebach, K.* (Hrsg.)*,* Münchner Kommentar zum Strafgesetzbuch, in 3 Bänden, München 2011;
zitiert als *Schäfer,* in: MüKo 2011, § 89b, Rn.

Schirra, A., Die Indienstnahme Privater im Lichte des Steuerstaatsprinzips. Frankfurt 2002.

Schlepper, C./ Leese, M., Plädoyer für eine unabhängige und grundrechtsgerechte Evaluation der EU-Richtlinie zur Vorratsdatenspeicherung, NK 2011,70.

Schliesky, U., Souveränität und Legitimität von Herrschaftsgewalt, Die Weiterentwicklung von Begriffen der Staatslehre und des Staatsrechts im europäischen Mehrebenensystem. Tübingen 2004.

Schmid, V., Datenschutz als Tatenschutz, - eine weitere Perspektive zur Vorratsdatenspeicherung - 2/2010; abrufbar unter: http://tuprints.ulb.tu-darmstadt.de/2062/1/CyLaw_Report_XXX_100222.pdf;
zitiert als *Schmid* CyLaw Report 2/210, S.

Schmidt-Bleibtreu, B.; Klein, F (Begr.v.)*.,* Kommentar zum Grundgesetz; *Hofmann, H./Hopfauf, A.* (Hrsg.)*,* 12. Auflage, 2011;
zitiert als *Bearbeiter* in *Schmidt-Bleibtreu/Klein*, GG 2011, Art., Rn.

Schnabel, P., Kommunikationstechnik-Fibel, 2. Auflage,Ludwigsburg, 2008.

Schneckener, U., Warum lässt sich Terrorismus nicht »besiegen«?, Herausforderungen und Leitlinien für die Terrorismusbekämpfung, in: *Huster, S./ Rudolph, K.* (Hrsg.), Vom Rechtsstaat zum Präventionsstaat, Frankfurt am Main 2008, 25 – 44;
zitiert als *Schneckener* 2008, S.

Schneider, P., Die Abwehr äußerer Gefahren für den Luftverkehr als Aufgabe von Luftfahrtbehörden und Luftfahrtunternehmen - Eine Abgrenzung von hoheitlicher Gefahrenabwehr und Eigensicherung, NVwZ 1988, 605.

Schneider, P., Im Zweifel für die Freiheit, KritV 1988, 294.

Schneider, P., In dubio pro libertate, in: *Caemmerer, E. v./ Friesenhahn, E./ Lange, R.* (Hrsg.), Hundert Jahre Deutsches Rechtsleben, Festschrift zum hundertjährigen Bestehen des deutschen Juristentages 1860-1960, Karlsruhe 1960, 263 – 290;
zitiert als *Schneider* 1960, S.

Schneider, W., L., Die Komplementarität von Sprechakttheorie und systemtheoretischer Kommunikationstheorie. Ein hermeneutischer Beitrag zur Methodologie von Theorievergleichen, ZfS 1996, 263.

Schoch, F., Der verfassungsrechtliche Schutz des Fernmeldegeheimnisses (Art. 10 GG), Jura 2011, 194.

Scholz, R., Art. 23/ Art. 12 in *Maunz, T./ Dürig, G*., Grundgesetzkommentar, Loseblatt, München 2007/ 2013; zitiert als *Scholz,* in: *Maunz/Dürig,* GG Jahr, Art. Rn.

Scholz, R., Rechtsfrieden im Rechtsstaat, Verfassungsrechtliche Grundlagen, aktuelle Gefahren und rechtspolitische Folgerungen, NJW 1983, 705.

Scholz, R., Zur Kostenerstattungspflicht des Staates für gesetzliche Maßnahmen der Telefonüberwachung, Archiv PT 1995, 169.

Scholz, R./ Pitschas, R., Informationelle Selbstbestimmung und staatliche Informationsverantwortung. Berlin 1984.

Scholz, S., Internet-Politik in Deutschland: vom Mythos der Unregulierbarkeit, Münster 2004.

Schorkopf, F., § 15 Würde des Menschen, in: *Ehlers, D./ Becker, U.* (Hrsg.), Europäische Grundrechte und Grundfreiheiten. Berlin 2009;
zitiert als *Schorkopf,* in: *Ehlers/Becker* § 15 Rn.

Schorkopf, F., § 16.1 Höchstpersönliche Rechte, in: *Ehlers, D./ Becker, U.* (Hrsg.), Europäische Grundrechte und Grundfreiheiten, Berlin 2009;
zitiert als *Schorkopf,* in: *Ehlers/Becker* § 16.1

Schramm, M./ Wegener, C, Neue Anforderungen an eine anlasslose Speicherung von Vorratsdaten - Umsetzungsmöglichkeiten der Vorgaben des Bundesverfassungsgerichts, MMR 2011, 9.

Schuldt, M., Abschlusstagung des Forschungsprojekts INVODAS, abrufbar unter: http://rsw.beck.de/CMS/?toc=ZD.60&docid=323207, ZD 2011, 112.

Schulte, M., Kommentierung § 3 BImSchG, in: *Giesberts, L./Reinhardt, M.,* (Hrsg.), Beck'scher Online-Kommentar Umweltrecht, München 2012;
zitiert als *Schulte,* in: Beck-OK Umweltrecht 2012, § 3 BImSchG Rn.

Schulze-Fielitz, H., Art. 5 in: Grundgesetz, Kommentar, *Dreier, H.* (Hrsg.), Bnd. 1, Tübingen 2004;
zitiert als *Schulze-Fielitz*, in: *Dreier*, GG 2004, Art.

Schütze, M./ Eckhardt, J., die Vielseitigkeit der Rechtsprechung zur Vorratsdatenspeicherungspflicht, CR 2009, 775.

Schwabe, *J.* Die Stufentheorie des Bundesverfassungsgerichts zur Berufsfreiheit, DÖV 1969, 734.

Schweda, S., Schweden: Gesetz zur Vorratsdatenspeicherung verabschiedet, ZD Aktuell 2012, 02882.

Schweda, S., Umsetzungsunterschiede der Vorratsdatenspeicherungsrichtlinie in Europa – ein Bericht aus dem Forschungsprojekt INVODAS im Mai 2011, in: SIRA, Sicherheit im öffentlichen Raum, 1/2011, 56-86.

Schwegel, A., Auf dem Weg zu einem "deutschen FBI"? Bundeskriminalamt (BKA) und föderale Sicherheitsarchitektur im Zeichen der Terrorismusbekämpfung, in: *Glawe, R.* (Hrsg.), Eine neue deutsche Sicherheitsarchitektur, Impulse für die nationale Strategiedebatte, Berlin 2009, 307 – 320;
zitiert als *Schwegel* 2009.

Seong, H.-J., Europol im Recht der Europäischen Union. Tübingen 2005;
zitiert als *Seong* 2005, S.

Sieber,U., Grenzen des Strafrechts, ZStW (119) 2007, 1 ff.

Sierck, G. M./ Schöning, F./ Pöhl, M., Zulässigkeit der Vorratsdatenspeicherung nach europäischem und deutschem Recht. Berlin 2006; Ausarbeitung des Wissenschaftlichen Dienst des Bundestags, WD 3-282/06; abrufbar unter: http://hp.kairaven.de/files/btwd-ausarbeitung-vds.pdf;
zitiert als *Sierck/Schöning/Pöhl* 2006,S.

Sievers, M., Der Schutz der Kommunikation im Internet durch Artikel 10 des Grundgesetzes. Kiel 2002.

Simitis, S., § 1, in: *Simitis, S.* (Hrsg.), Bundesdatenschutzgesetz, 7. Auflage, Baden-Baden 2011;
zitiert als *Simitis,* in: *Simitis,* BDSG Komm 2011, § 1 Rn.

Simitis, S., Die informationelle Selbstbestimmung - Grundbedingung einer verfassungskonformen Informationsordnung, NJW 1984, 394.

Simitis, S., Hat der Datenschutz noch eine Zukunft?, RDV 2007, 143.

Simitis, S., Der EuGH und die Vorratsdatenspeicherung oder die verfehlte Kehrtwende bei der Kompetenzregelung, NJW 2009, 1782.

Sisk, T. D., Between terror and tolerance, Religious leaders, conflict, and peacemaking. Washington, D.C 2011.

Sodan, H., Vorb. v. Art. 1, Art. 1, Art. 10, in: *Sodan, H.* (Hrsg.), Grundgesetz, Beck'scher Kompakt-Kommentar, München 2011;
zitiert als *Sodan,* in: *Sodan,* GG, 2011, Art. Rn.

Sommermann, K.-P., Art. 20 in v. *Mangoldt, H/ Klein, F./ Starck, C.*, Das Bonner Grundgesetz Kommentar, München 2010;
zitiert als *Sommermann,* in: *Mangoldt/Klein/Starck,* GG 2010, Art. 20 Rn.

Song, C./ Zehui, Q./ Blumm, N./ Barabási, A.-L., Limitis of Preditability in Human Mobility, Science 2010, Vol. 327, 1018.

Spiecker gen. Döhmann, I./ Eisenbardt, M., Kommt das Volkszählungsurteil nun durch den EuGH? Der europäische Datenschutz nach dem Inkrafttreten des Vertrags von Lissabon, JZ 2011, 169.

Spindler, *G.*, Der Auskunftsanspruch gegen Verletzter und Dritte im Urheberrecht nach neuem Recht, ZUM 2008, 640.

Spindler, G., Persönlichkeitsrecht und Datenschutz im Internet – Anforderungen und Grenzen einer Regulierung, NJW-Beil. 2012, 98.

Spindler, G./ Nink, J., § 11 TMG, in: *Spindler, G./ Schuster, F.* (Hrsg.), Recht der elektronischen Medien, München 2011;
zitiert als *Spindler/Nink* in *Spindler/Schuster,* 2011, § 11 TMG, Rn

Spindler, G./ Schuster, F. (Hrsg.), Recht der elektronischen Medien, 2. Auflage, München 2011;
zitiert als *Bearbeiter* in *Spindler/Schuster* 2011, § Rn.

Starck, C., Art. 3, in: v. *Mangoldt, H/ Klein, F./ Starck, C.*, Das Bonner Grundgesetz Kommentar, München 2010;
zitiert als *Starck* in *Mangoldt/Klein/Starck,* GG 2010, Art. 3 Rn.

Stegner, R., Im Zweifel für die Freiheit, in *Huster, S./ Rudolph, K.* (Hrsg.), Vom Rechtsstaat zum Präventionsstaat, 1. Auflage, Frankfurt am Main 2008;
zitiert als *Stegner* 2008, S.

Stern, K., Allgemeine Lehren der Grundrechte, Das Staatsrecht der Bundesrepublik Deutschland, Bnd. III Teilband. 2 1994;
zitiert als *Stern* Staatsrecht III, Bnd. 2, 1994, §.

Stober, R., Privatisierung öffentlicher Aufgaben, Phantomdiskussion oder Gestaltungsoption in einer verantwortungsgeteilten, offenen Wirtschafts-, Sozial- und Sicherheitsverfassung?, NJW 2008, 2301.

Stober, R., Staatliches Gewaltmonopol und privates Sicherheitsgewerbe - Plädoyer für eine Police-Private-Partnership, NJW 1997, 889.

Störing, M., Paukenschlag als Pyrrhussieg, Deutsche Regelung zur Vorratsdatenspeicherung verfassungswidrig, c't 2010, 52.

Stowasser, J./ Petschenig, M.,/ Skutsch, F., Stowasser, Lateinisch- deutsches Schulwörterbuch. München 1994;
zitiert als *Stowasser* 1994.

Strasser, H./ van den Brink, H., Auf dem Weg in die Präventionsgesellschaft, APuZ 46/2005, 3; abrufbar unter: http://www.bpb.de/apuz/28688/auf-dem-weg-in-die-praeven-tionsgesellschaft;
zitiert als *Strasser/ van den Brink,* APuZ 2005, S.

Streinz, R., Art. 21, in v. *Mangoldt, H/ Klein, F./ Starck, C*., Das Bonner Grundgesetz Kommentar, München 2010;
zitiert als *Streinz,* in: *Mangoldt/Klein/Starck,* GG 2010, Art. 21 Rn.

Strutynski, P., „Die Sicherheit Deutschlands wird auch am Hindukusch verteidigt", in: Die Linke (Hrsg.) Schwarzbuch zur Sicherheits- und Militärpolitik Deutschlands, Berlin 2007, S. 22-33; abrufbar unter: http://www.ag-friedensforschung.de/themen/Bundeswehr/weissbuch/strutynski.html;
zitiert als *Strutynski* 2007.

Stubenrauch, J., Gemeinsame Verbunddateien von Polizei und Nachrichtendiensten, Eine verfassungsrechtliche Untersuchung am Beispiel der Antiterrordatei, 1. Auflage, Baden-Baden 2009.

Szuba, D., Vorratsdatenspeicherung, Der europäische und deutsche Gesetzgeber im Spannungsfeld zwischen Sicherheit und Freiheit, 1. Auflage, Baden-Baden 2011.

Tanenbaum, A., Computernetzwerke, 4. Auflage, München 2003.

Terhechte, J.-P., Rechtsangleichung zwischen Gemeinschafts- und Unionsrecht - die Richtlinie über die Vorratsdatenspeicherung vor dem EuGH, EuZW 2009, 199.

Thiel, M., Die "Entgrenzung" der Gefahrenabwehr, Grundfragen von Freiheit und Sicherheit im Zeitalter der Globalisierung, 1. Auflage, Tübingen 2011.

Tinnefeld, M.-T., Persönlichkeitsrecht und Modalitäten der Datenerhebung im Bundesdatenschutzgesetz, NJW 1993, 1118.

Tinnefeld, M.-T., Sapere aude! Über Informationsfreiheit, Privatheit und Raster, NJW 2007, 625.

Tinnefeld, M.-T., Totale Überwachung - die einzige Antwort auf die Terroranschläge?, MMR 2007, 493.

Tinnefeld, M.-T./ Ehmann, E./ Gerling, R., Einführung in das Datenschutzrecht, Datenschutz und Informationsfreiheit in europäischer Sicht. München 2005;
zitiert als *Tinnefeld/Ehmann/Gerling* 2005.

Trute, H.-H., Verfassungsrechtliche Gewährleistung des Rechts auf informationelle Selbstbestimmung, in: *Roßnagel*, *A.* (Hrsg.), Handbuch Datenschutzrecht, Die neuen Grundlagen für Wirtschaft und Verwaltung, München 2003;
zitiert als *Trute* 2003, S.

Uerpmann-Wittzack, R./ Jankowska-Gilberg, M., Die Europäische Menschenrechtskonvention als Ordnungsrahmen für das Internet, MMR 2008, 83.

Uhle, A., Die Gesetzgebungskompetenz des Bundes für die Abwehr von Gefahren des internationalen Terrorismus, - Anmerkungen zu Art. 73 Abs. 1 Nr. 9 a GG -, DÖV 2010, 989.

ULD, Stellungnahme des Unabhängigen Landeszentrums für Datenschutz Schleswig (ULD) vom 27.6.2007 zum, Gesetzesentwurf der Bundesregierung für ein Gesetz zur Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen sowie zur Umsetzung der Richtlinie 2006/24/EG, BR-DS275/07;
zitiert als *ULD* 27.6.2007.

van Ooyen, R. C., "Zwei Senate in meiner Brust"?, Die "Vorratsdatenspeicherung" im Spiegel bisheriger Europa-Rechtsprechung des Bundesverfassungsgerichts, Recht und Politik 2010, 98.

van Ooyen, R. C., Mit „Mangold“ zurück zu „Solange II“?, Das Bundesverfassungsgericht nach „Lissabon", Der Staat 2011, 45.

Verfassungsausschuss der Ministerpräsidenten-Konferenz der westlichen Besatzungszonen, Bericht über den Verfassungskonvent auf Herrenchiemsee, vom 10. bis 25. August 1948.

Vitzthum, W. G., Begriff, Geschichte und Rechtsquellen des Völkerrechts, 1. Abschnitt, in: *Vitzthum, W.* (Hrsg.), Völkerrecht, Berlin 2010;
zitiert als *Vitzthum,* in: *Vitzthum,* VR 2010, Abschnitt. 1, Rn.

Vogelsang, K., Grundrecht auf informationelle Selbstbestimmung?, Baden-Baden 1987.

Vogler, T., Die strafschärfende Verwertung strafbarer Vor- und Nachtaten bei der Strafzumessung und die Unschuldsvermutung (Art. 6 Abs. 2 EMRK), in: *Gössel, K. H./ Kauffmann, H.* (Hrsg.), Strafverfahren im Rechtsstaat, Festschrift für Theodor Kleinknecht zum 75. Geburtstag am 18. August 1985, München 1985, S. 429 – 444;
zitiert als *Vogler* 1985, S.

Volkmann, U., Anmerkung zum Urteil des BVerfG vom 27.2.2008, 1 BvR 370/07, DVBl. 2008, 590.

Volkmer, M., Verwertbarkeit von Vorratsdaten, Zu beweisrechtlichen Konsequenzen des Urteils des BVerfG vom 2.3.2010 - 1 BvR 256/08, 1 BvR 263/08, 1 BvR 586/08, NStZ 2010, 318.

von Bogdandy, A./ Schill, S., Die Achtung der nationalen Identität unter dem reformierten Unionsvertrag - Zur unionsrechtlichen Rolle nationalen Verfassungsrechts und zur Überwindung des absoluten Vorrangs, ZaöRV 2010, 701.

Von Lewinski, K., Europäisierung des Datenschutzrechts, DuD 2012, 564.

Voß, M., zur Erforderlichkeit und Angemessenheit legitimer Widerstandsformen gegen die Sicherheitsgesellschaft, in: , Von der Rationalität des Rechts in die Irrationalität der Sicherheit, Reflexionen über Widerstandsformen in Sicherheitsgesellschaften, KritV 2010, 137.

Voßkuhle, A., Grundwissen - Öffentliches Recht: Der Grundsatz der Verhältnismäßigkeit, JuS 2007, 429.

Waechter, K., Bereitstellungspflicht für Fernmeldeanlagenbetreiber, VerwArch 1996, 68.

Waever, O., Securitization and Desecuritization, in: *Lipschutz, R.* (Hrsg.), On security, New York 1995, S. 46 – 86;
zitiert als *Waever* 1995, S.

Wagner, S., Zwangsrabatte für Arzneimittel als verfassungswidrige Sonderabgabe mit Finanzierungsfunktion, PharmR 2003, 409.

Wahl, R., Der offene Staat und seine Rechtsgrundlagen, JuS 2003, 1145.

Wainwright, R., Die Zukunft des Europäischen Polizeiamtes Europol in der Sicherheitsarchitektur der Europäischen Union: zur strategischen Ausrichtung von Europol als eine eigenständige EU-Behörde, Die Polizei 2010, 206.

Walden, M., Zweckbindung und -änderung präventiv und repressiv erhobener Daten im Bereich der Polizei, Berlin, 1996.

Wandtke, A.-A. Ausgangspunkt und Reform des Urheberrechts, in *Wandtke, A.A./Bullinger, W.,* Praxiskommentar zum Urheberrecht, 3. Auflage, München 2009;
zitiert als *Wandtke* in *Wandtke/Bullinger,* 2009, Einl. Rn.

Weber-Grellet, H., Lenkungssteuern im Rechtssystem, NJW, 3657.

Wehr, C./ Ujica, M., "Alles muss raus!", Datenspeicherungs- und Auskunftspflichten der Access-Provider nach dem Urteil des BVerfG zur Vorratsdatenspeicherung, MMR 2010, 667.

Weichert, T., Wo liegt Prüm?, Der polizeiliche Datenaustausch in der EU bekommt eine neue Dimension, DatenschutzNachrichten, 2006, 12-15;
abrufbar unter: https://www.datenschutzzentrum.de/polizei/060329-pruem.htm;
zitiert als *Weichert* 2006.

Weichert, T., in*: Däubler, W./ Klebe, T./ Wedde, P./ Weichert, T.* (Hrsg.), Bundesdatenschutzgesetz, Kompaktkommentar zum BDSG ; Frankfurt 2010;
zitiert als *Weichert*, in: *Däubler/Klebe/Wedde/Weichert* BDSG 2010, § Rn.

Weichert, T., Die (un)heimlichen Datensammlungen - von der Deutungsmacht und Deutungshoheit der Polizei, Beitrag für den Strafverteidigertag in Berlin am 26.3.2011; abrufbar unter: https://www.datenschutzzentrum.de/vortraege/20110326-weichert-datenschutz-strafverfolgung.html;
zitiert als *Weichert* 2011a.

Weichert, T., Optimierte Verantwortung/slosigkeit, Wer verantwortet eigentlich was in unserer „smarten Welt?", Hintergrundtext für die Sommerakademie des Unabhängigen Landeszentrums, v. 18.7.2011,
abrufbar unter: https://www.datenschutzzentrum.de/sommerakademie/2011/sak2011-thilo-weichert-hin-tergrundtext.html;
zitiert als *Weichert* 2011b.

Weise, B./ Freiheit, H.-J., IT Labor, Bnd. 2, Internet-Telefonie – Voice over IP (VoIP), Stuttgart 2010.

Weiser, M., The Computer for the 21st Century, Specialized elements of hardware and software, connected by wires, radio waves and infrared, will be so ubiquitous, that no one will notice their presence, Scientific American 1991, S. 94 ff.;
abrufbar unter: http://www.ubiq.com/hypertext/weiser/SciAmDraft3.html;
zitiert als *Weiser* 1991, S.

Weisser, N.-F., Das Gemeinsame Terrorismusabwehrzentrum (GTAZ) – Rechtsprobleme, Rechtsform und Rechtsgrundlage, NVwZ 2011, 142.

Welsing, R., Das Recht auf informationelle Selbstbestimmung im Rahmen der Terrorabwehr, Darstellung anhand einer Untersuchung der präventiven Rasterfahndung, Marburg 2009.

Wernsmann, R., § 4 AO, in: *Hübschmann, W./ Hepp, E./ Spitaler, A.* (Hrsg.), Abgabenordnung - Finanzgerichtsordnung, Kommentar, Köln 1995;
zitiert als *Wernsmann* in *Hübschmann/Hepp/Spitaler,* AO/FGO, § 4 AO, Rn.

Werthebach, E./Droste, B., Art. 73 in *Dolzer, R. / Kahl, W./ Waldhoff, C./ Graßhof, K.* (Hrsg.), Bonner Kommentar zum Grundgesetz, Heidelberg 1998;
zitiert als *Werthebach/Droste*, BK-GG, 1998, Art. 73 Rn.

Weßlau, E., Vorfeldermittlungen, Probleme der Legalisierung "vorbeugender Verbrechensbekämpfung" aus strafprozessrechtlicher Sicht, Berlin 1989.

Westphal, D., Die Richtlinie zur Vorratsspeicherung von Verkehrsdaten, Brüsseler Stellungnahme zum Verhältnis von Freiheit und Sicherheit in der "Post-911-Informationsgesellschaft", EuR 2006, 706.

Westphal, D., Leitplanken für die Vorratsdatenspeicherung – Abrücken von „Solange", Das Urteil des BVerfG vom 2. 3. 2010, EuZW 2010, 494.

Wettern, M., Umsetzung der Vorratsdatenspeicherung an den Hochschulen, nichts hören - nichts sehen; reicht nicht, DUD 2009, 343.

Wieland, J., Art. 12, in: Grundgesetz, Kommentar, *Dreier, H.* (Hrsg.), Bnd. 1, Tübingen 2004; zitiert als *Wieland*, in: *Dreier*, GG 2004, Art. 12 Rn.

Wiesemann, H. P., IT-rechtliche Rahmenbedingungen für „intelligente" Stromzähler und Netze, Smart Meter und Smart Grids, MMR 2011, 355.

Will, R., Die Menschenwürde: Zwischen Versprechen und Überforderung, in: *Roggan, F./ Hirsch, B.* (Hrsg.), Mit Recht für Menschenwürde und Verfassungsstaat, Festgabe für Dr. Burkhard Hirsch anlässlich der Verleihung des Fritz-Bauer-Preises der Humanistischen Union am 16.9.2006 in Freiburg, Berlin 2006, 29 – 46;
zitiert als *Will* 2006.

Williams, M. C., Words, Images, Enemies: Securitization and International Politics, International Studies Quarterly 2003, 511.

Wilms, H., Elena (Elektronischer Entgeltnachweis) und das Recht auf informationelle Selbstbestimmung, Baden-Baden 2010.

Wintrich, J., Über Eigenart und Methode verfassungsgerichtlicher Rechtsprechung, in: *Bachof, H./ Becker, E./ Ebers, G./ Foohs, L./ u.a.* (Hrsg.), Festschrift für Herrn Geheimrat Professor Dr. Wilhelm Laforet anläßlich seines 75. Geburtstages, München 1952, S. 227 ff;
zitiert als *Wintrich* 1952, S.

Wolff, H., Vorratsdatenspeicherung - Der Gesetzgeber gefangen zwischen Europarecht und Verfassung?, NVwZ 2010, 751.

Wollweber, H., Wie lange reicht der Vorrat? NJW 2012, NJW-aktuell Nr. 25, 14.

Wolter, J., Menschenwürde, Kernbereich privater Lebensgestaltung und Recht auf Leben (Schwerpunkt: Wohnungsüberwachung im Strafprozess- und Polizeirecht), in: Festschrift für *Wilfried Küper* zum 70. Geburtstag, *Hettinger, M.* (Hrsg.) Heidelberg 2007; 707-722;
zitiert als *Wolter* 2007, S.

Wüstenberg, D., Vorratsdatenspeicherung und Grundrechte, MMR-Int 2006, 91.

Zeh, J./ Trojanow, I., Angriff auf die Freiheit, Sicherheitswahn, Überwachungsstaat und der Abbau bürgerlicher Rechte, München 2009.

Ziebarth, W., Grundrechtskonforme Gestaltung der Vorratsdatenspeicherung, Überlegungen zu einer europa-, verfassungs- und datenschutzrechtskonformen Umsetzung, DUD 2009, 25.

Zimmermann, U. W., Sicherheitsvorsorge vor Ort. Eine verschiedenen Trägern zustehende, vernetzt wahrzunehmende Aufgabe auch in den Bereichen „Innerer Sicherheit" und Öffentlicher Un-Ordnung in der Kommune. Würzburg 2005; abrufbar unter:
http://opus.bibliothek.uni-wuerzburg.de/volltexte/2006/1927/pdf/Sicherheitsvorsorge_vor_Ort.pdf.

Zöller, M., Die Jagd nach den Verbindungsdaten, in: *Wolter, J./Schenke, W.-R. /Rieß, P./Zöller, M.* (Hrsg.), Datenübermittlungen und Vorermittlungen - Festgabe für *Hans Hilger,* Heidelberg 2003, 291-323;
zitiert als *Zöllner* 2003, S.

Zöller, M., Vorratsdatenspeicherung zwischen nationaler und europäischer Strafverfolgung, GA 2007, 392.

Zöller, M., Der Austausch von Strafverfolgungsdaten zwischen den Mitgliedstaaten der Europäischen Union, ZIS 2011, 64.