

MARKUS THIEL

Die „Entgrenzung“
der Gefahrenabwehr

Jus Publicum

205

Mohr Siebeck

JUS PUBLICUM
Beiträge zum Öffentlichen Recht

Band 205



Markus Thiel

Die „Entgrenzung“ der Gefahrenabwehr

Grundfragen von Freiheit und Sicherheit
im Zeitalter der Globalisierung

Mohr Siebeck

Markus Thiel, geboren 1973; Studium der Rechtswissenschaften in Köln und der Verwaltungswissenschaften in Speyer; 1999 Promotion zum Dr. iur. und 2003 Promotion zum Dr. rer. publ.; 2010 Habilitation; derzeit Privatdozent an der Heinrich-Heine-Universität Düsseldorf.

e-ISBN PDF 978-3-16-151286-5
ISBN 978-3-16-150576-8
ISSN 0941-0503 (Jus Publicum)

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

© 2011 Mohr Siebeck Tübingen.

Das Werk einschließlich aller seiner Teile ist urheberrechtlich geschützt. Jede Verwertung außerhalb der engen Grenzen des Urheberrechtsgesetzes ist ohne Zustimmung des Verlags unzulässig und strafbar. Das gilt insbesondere für Vervielfältigungen, Übersetzungen, Mikroverfilmungen und die Einspeicherung und Verarbeitung in elektronischen Systemen.

Das Buch wurde von Gulde-Druck in Tübingen aus der Garamond-Antiqua gesetzt und auf alterungsbeständiges Werkdruckpapier gedruckt und von der Buchbinderei Spinner in Ottersweier gebunden.

Vorwort

Die vorliegende Schrift ist im Wintersemester 2009/2010 von der Juristischen Fakultät der Heinrich-Heine-Universität Düsseldorf als schriftliche Habilitationsleistung angenommen worden. Rechtsprechung und Literatur sind im Wesentlichen bis Oktober 2010 berücksichtigt; später ergangene Entscheidungen und veröffentlichtes Schrifttum sind im wissenschaftlichen Apparat nur nachgetragen, wenn sie unmittelbar einschlägig waren. Da das Sicherheitsrecht, wie sich im Laufe der Untersuchung zeigen wird, einem stetigen Wandel unterworfen ist, kann eine rechtswissenschaftliche Abhandlung die Gesetzeslage nur in einer „Momentaufnahme“ abbilden – der Verfasser hofft gleichwohl, dass seine Ausführungen zu vielen der zeitlosen grundlegenden Rechtsfragen auch über die Lebensdauer des ephemeren Normenbestands hinaus Gewicht und Geltung haben werden.

Mein besonderer Dank gilt vor allem meinem verehrten akademischen Lehrer, Herrn Univ.-Prof. Dr. *Johannes Dietlein*. Während meiner langjährigen Tätigkeit an seinem Lehrstuhl für Öffentliches Recht und Verwaltungslehre hat er mein juristisches Denken und meine wissenschaftliche Arbeit entscheidend geprägt, mir stets aber auch genügend Freiräume für eigene Wege eröffnet.

Herzlich danken möchte ich außerdem Herrn Univ.-Prof. Dr. *R. Alexander Lorz*, LL.M. für die Erstellung des Zweitgutachtens und seine wertvollen und wohlwollenden inhaltlichen Hinweise. Nicht allein an ihnen zeigt sich die äußerst anregende, kollegiale und erfreuliche Arbeitsatmosphäre der Düsseldorfer Juristischen Fakultät.

Meiner Tante, Frau *Gerda Charlotte Judith*, bin ich für ihre großzügige Unterstützung durch die Übernahme der Druckkosten für diese Schrift zu großem Dank verpflichtet.

Dem Mohr Siebeck-Verlag danke ich für die Aufnahme meiner Habilitationsschrift in seine Reihe *Jus Publicum*.

Ich widme diese Arbeit meinen lieben Eltern in Dankbarkeit.

Köln, Dezember 2010

Markus Thiel

Inhaltsverzeichnis

Vorwort	V
Einleitung	1
1. Teil: Herausforderungen an das Recht der inneren und äußeren Sicherheit.	5
A. Die „Informationsgesellschaft“ und ihre Gefährdungen	6
I. Ausprägung und Charakteristika der „Informationsgesellschaft“	6
1. Die gesellschaftliche Bedeutung der „Information“.	6
2. Anforderungen an die Rechtsordnung	8
3. Wachsende Bedeutung der Vorsorge	12
4. Informationsgesellschaft und Steuerungsfunktion des Rechts	14
5. Rechtliche Gestaltung der Informationsgesellschaft als politische Aufgabe	17
6. Eignung traditioneller Kategorien des Rechts zur Bewältigung der Informationsgesellschaft	20
7. Internationalisierung und Globalisierung	22
II. Die „Informationsgesellschaft“ und ihre rechtliche Bedeutung	24
III. „Informationsgesellschaft“ und „Risikogesellschaft“	27
IV. „Internet-Devianz“	29
B. „Internationaler Terrorismus“.	30
I. Begriff des „Terrorismus“.	31
II. Besonderes Bedrohungspotenzial des „Internationalen Terrorismus“.	35
III. Reaktionen des Gesetzgebers.	39
1. Die „Anti-Terror-Pakete“ I und II	41
2. Insbesondere: Die Änderung des Bundesverfassungs- schutzgesetzes.	43
IV. Nivellierung der Grenzen von innerer und äußerer Sicherheit .	45
V. Notwendigkeit intensivierter Kooperation	46

C. „Organisierte Kriminalität“	46
2. Teil: Der Begriff der „Gefahrenabwehr“	51
A. Gefahrenbegriff.	51
I. Schutzgüter und Schutzkomponenten	52
1. Öffentliche Sicherheit	52
2. Öffentliche Ordnung.	54
II. Hinreichende Wahrscheinlichkeit bzw. Gewissheit eines Schadenseintritts, „Störung“	65
B. Abgrenzungen	67
I. Vorsorge	67
1. „Vorverlagerung“ staatlichen Handelns	68
2. Vorsorge als Reaktion auf „Ungewissheit“	70
3. Vorsorge als Rechtsprinzip	75
4. „Vorsorge“ in einfachgesetzlichem Gewand: das Beispiel des Immissionsschutzrechts	77
a) Die Vorsorgepflichten des Anlagenbetreibers nach § 5 Abs. 1 Nr. 2 BImSchG.	77
b) Begriffliche Konturierung	79
5. Vorsorgeziele	81
a) Vermeidung von Gefahrenlagen – „Gefahrenvorsorge“	81
b) Schaffung einer „Pufferzone“ vor der Gefahrenschwelle	82
c) „Verteilungsgerechtigkeit“ und „Ressourcenschonung“	83
d) „Sanierungskomponente“	84
6. Überdehnung des Vorsorgegedankens?	84
a) Vorsorgepflichten als Innovationshemmnis?	84
b) Zu extensive Handhabung des Vorsorgegedankens?	85
7. Verfassungsrechtliche Bindungen von Vorsorgemaßnahmen	90
8. Abgrenzung von Gefahrenabwehr und Vorsorge?	91
II. Repressives Handeln.	95
III. Daseinsvorsorge	96
IV. Vorbeugende Bekämpfung von Straftaten.	100
1. Verhütung von Straftaten	101
2. Verfolgungsvorsorge	102
V. Staatliche Infrastrukturverantwortung	114
1. „Kritische“ Infrastrukturen	114
2. „Verletzlichkeit der Informationsgesellschaft“	116
3. Reichweite staatlicher Infrastrukturverantwortung	118

4. Insbesondere: Schutz vor schädigendem Zugriff	123
5. Eigensicherung und Indienstnahme	125
a) Gesetzliche Eigensicherungspflichten.	125
b) Eigensicherung oder Indienstnahme am Beispiel des nordrhein-westfälischen Hafensicherheitsgesetzes	127
C. „Sicherheitsvorsorge“ als „dritte Aufgabenkategorie“?.	134
 3. Teil: Das Grunddilemma der Gefahrenabwehr: Freiheit oder Sicherheit?	 137
A. Freiheit als Wert mit Verfassungsrang	138
B. Sicherheit als Wert mit Verfassungsrang	140
I. Begriff der Sicherheit	141
II. Verfassungsrechtliche Bedeutung der Sicherheit	143
1. Ideengeschichtlicher Überblick	144
2. Sicherheit als Gemeinwohlgut	147
3. Staatsaufgabe Sicherheit	149
a) Staatsziel Sicherheit	149
b) Subjektives Recht auf Sicherheit	150
c) Insbesondere: „Grundrecht auf Sicherheit“?.	154
III. Beteiligung Privater an Gefahrenabwehraufgaben	159
1. „Privatisierung“ der Gefahrenabwehr?.	159
2. Insbesondere: „Haftungsintermediäre“ im Internet	167
C. Der Ausgleich zwischen Freiheit und Sicherheit – Allgemeiner Vorrang der Freiheit?	179
D. Der Ausgleich von Freiheit und Sicherheit als genuine Aufgabe des Gesetzgebers	182
 4. Teil: Ausdifferenzierung gefahrenabwehrrechtlicher Eingriffsermächtigungen	 187
A. Einleitung	187
B. Gefahrenabwehr oder Förderung des subjektiven Sicherheitsgefühls?	188

C. Das Gefahrenabwehrrecht als „reaktives“ Recht	193
D. Grundrechtliche Vorgaben für gesetzliche Eingriffsermächtigungen zur Gefahrenabwehr	194
I. Menschenwürdegarantie (Art. 1 Abs. 1 GG)	195
1. Schutz des Kernbereichs privater Lebensgestaltung und „Informationseingriffe“	195
a) Der Kernbereichsschutz in der Rechtsprechung des Bundesverfassungsgerichts	195
b) Inkonsequenz des Kernbereichsschutzkonzepts des Bundesverfassungsgerichts?	198
2. Lebensrettende Aussageerzwingung und Folterverbot	201
3. Ermächtigung zum Abschuss entführter Passagiermaschinen (§ 14 Abs. 3 a.F. LuftSiG)	216
II. Das (Grund-)Recht auf informationelle Selbstbestimmung (Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG)	221
1. Dogmatische Herleitung – das „Volkszählungsurteil“ des Bundesverfassungsgerichts	222
2. Gewährleistungsgehalte des (Grund-)Rechts auf informationelle Selbstbestimmung	224
a) Abwehrrechtliche Gewährleistungselemente.	224
aa) Grundlagen	224
bb) Verfassungsgerichtliche Konturierung des Grundrechts auf informationelle Selbstbestimmung	229
(1) Kontroll- und Überwachungsmaßnahmen nach dem Außenwirtschaftsgesetz (BVerfGE 110, 33 ff.)	229
(2) Automatisierte Erfassung von Kraftfahrzeug-Kennzeichen (BVerfGE 120, 378 ff.)	231
(3) Rasterfahndung zu präventiv-polizeilichen Zwecken (BVerfGE 115, 320 ff.)	241
b) Objektiv-rechtliche Funktionen, teilhabe- und leistungsrechtliche Gewährleistungselemente	259
c) „Recht auf Vergessen“	262
3. Kritik des Rechts auf informationelle Selbstbestimmung	264
III. Das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme („Computer-Grundrecht“)	268
1. Die Entscheidung des Bundesverfassungsgerichts zur „Online-Durchsuchung“ (BVerfGE 120, 274 ff.)	268
2. Herleitung und Inhalt des „Computer-Grundrechts“	271
a) Ausprägung des allgemeinen Persönlichkeitsrechts	271
b) Grundrechtliche Schutzlücke	274

aa) Art. 10 Abs. 1 GG	274
bb) Art. 13 Abs. 1 GG	275
cc) Allgemeines Persönlichkeitsrecht, Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG	277
dd) Das Recht auf informationelle Selbstbestimmung	277
c) Sachlicher Schutzbereich	279
d) Kriterien der Eingriffsintensität	280
e) Beschränkungsmöglichkeiten – Anforderungen an die Gefahrenlage	280
f) „Computer-Grundrecht“ und grundrechtliche Schutzpflichten	281
3. Kritik des Urteils des Bundesverfassungsgerichts zur „Online-Durchsuchung“	284
a) Befugnis des Bundesverfassungsgerichts zur Konturierung eines „neuen“ Grundrechts	284
b) Bestehen einer grundrechtlichen Schutzlücke	287
aa) Recht auf informationelle Selbstbestimmung	287
bb) Art. 13 Abs. 1 GG	292
c) Persönlicher Schutzbereich des Grundrechts.	293
d) Schutzwürdiges Vertrauen in Vertraulichkeit und Integrität informationstechnischer Systeme	294
e) Modifikation des Gefahrenbegriffs	295
aa) Die Konstruktion des Bundesverfassungsgerichts	295
bb) Alternative Lösungsansätze im Schrifttum	298
(1) „Abstrakte Gefahr“	298
(2) „Gefahrenverdacht“	299
(3) „Risiko“	300
f) Prozedurale Anforderungen	304
g) Unzulässigkeit der „Online-Durchsuchung“?	304
IV. Das Grundrecht auf Wahrung des „Telekommunikations- geheimnisses“ (Art. 10 Abs. 1 GG).	305
1. Gewährleistungsgehalt	305
a) Schutz des „Telekommunikationsgeheimnisses“	306
b) Informationspflichten.	306
c) Verhältnis zum Recht auf informationelle Selbstbestimmung	310
2. Die Entscheidung des Bundesverfassungsgerichts zum sog. „IMSI-Catching“ (BVerfG, NJW 2007, 351 ff.)	312
a) Repressive und präventive Einsatzermächtigungen	312
b) Technische Einwände gegen das „IMSI-Catching“	314
c) Grundrechtliche Bewertung des „IMSI-Catchings“	316
3. „Vorratsdatenspeicherung“ nach §§ 113 a, 113 b TKG	323

V. Das Grundrecht auf Unverletzlichkeit der Wohnung (Art. 13 Abs. 1 GG)	328
1. Gewährleistungsgehalt	328
2. „Großer Lauschangriff“	329
5. Teil: Veränderungen der föderalen Kompetenzordnung	333
A. Kompetenzfragen der Novelle des Bundeskriminalamtgesetzes.	333
I. Die Neuregelung des Bundeskriminalamtgesetzes.	333
II. Kompetenzfragen	335
III. Exkurs: Weitere Einwände gegen die Novelle des Bundeskriminalamtgesetzes	340
1. Regelung von „Online-Durchsuchung“ und „Quellen- Telekommunikationsüberwachung“	340
2. Eilfallkompetenz	342
3. Richtervorbehalt und Begründungserfordernis	345
4. Zuständigkeit zur Prüfung möglicher Kernbereichs- verletzungen bei der „Online-Durchsuchung“	346
5. Zeugnisverweigerungsrechte	347
B. Kooperation zwischen Bund und Ländern im Bereich des Katastrophenschutzes	351
C. Einsatz der Bundeswehr im Inneren	353
D. Aufgabenerweiterung von Bundesgrenzschutz bzw. Bundespolizei	361
6. Teil: Relativierung des Trennungsgebotes	367
A. Tendenzen zur Relativierung des Trennungsgrundsatzes	368
I. Repressive Kriminalitätsbekämpfung	368
II. Präventiver Bereich	370
B. Herleitung und Rang des Trennungsgebotes	372
I. Einfachgesetzlicher Bestand	372
II. Verfassungsrang des Trennungsgebotes?	374
1. Ansätze in der Rechtsprechung	374
2. Dogmatische Herleitung eines Trennungsgebotes mit Verfassungsrang.	379

a) Herleitung aus dem „Polizeibrief“ der alliierten Militärgouverneure	380
b) Herleitung aus geltendem Verfassungsrecht	381
C. Wirkungen des Trennungsgebotes	385
I. Folgen des Gebots organisatorischer Trennung	385
II. Gebot informationeller Trennung?	386
1. Informationelle Zusammenarbeit als Folge organisatorischer Trennung	387
2. Beispiele informationeller Zusammenarbeit	390
a) „Projektbezogene gemeinsame Dateien“	390
b) „Gemeinsames Terrorabwehrzentrum“	391
c) „Antiterrordatei“	394
 7. Teil: Internationalisierung und Europäisierung der Gefahrenabwehr	 399
A. Grenzüberschreitende Kooperation	400
I. IKPO – „Interpol“	403
II. Europol	405
III. „Schengen-Besitzstand“	409
1. Schengener Übereinkommen und Schengener Durchführungsübereinkommen	409
2. „Schengener Informationssystem“ (SIS)	411
3. Erweiterung des „Schengen-Besitzstands“ durch den „Vertrag von Prüm“	413
4. „Schengener Grenzkodex“	417
5. Europäische Agentur für die operative Sicherheit an den Außengrenzen – „FRONTEX“	418
a) Verordnungsermächtigung	418
b) Funktion und Aufgaben von „FRONTEX“	419
c) Rechtsschutzfragen	422
IV. Bilaterale Zusammenarbeit	424
V. Datenschutz im Rahmen internationaler polizeilicher Zusammenarbeit	425

B. Bundeswehreinätze im Ausland	432
I. Beteiligung an ESVP-Einsätzen der Europäischen Union.	432
II. Einsatz der Bundeswehr im Rahmen von ESVP-Missionen zur Bekämpfung der Seepiraterie	433
1. Rechtlicher Rahmen der Pirateriebekämpfung	434
a) Pirateriebekämpfung nach Völkergewohnheitsrecht	434
b) Pirateriebekämpfung nach geschriebenem Völkerrecht.	435
2. Die ESVP-Mission „Atalanta“	437
a) Resolutionen des Sicherheitsrates	438
b) Operation „Atalanta“	441
c) Deutsches Mandat und Bundeswehreinatz	442
d) Verfassungsrechtliche Grundlage für den Einsatz der Bundeswehr	445
e) (Verfassungs-)rechtliche Bewertung der Operation „Atalanta“	451
C. Einsatz deutscher Polizeikräfte in Auslandsmissionen	457
I. „Wahrnehmungskompetenz“	460
II. Auslandseinsatz der Bundespolizei und Art. 87 a Abs. 2 GG	467
III. Parlamentsvorbehalt für den Auslandseinsatz von Polizeikräften?	470
„Entgrenzung“ der Gefahrenabwehr – eine Grenzüberschreitung?	473
Literaturverzeichnis	481
Stichwortverzeichnis	565

Einleitung

Das Recht der inneren und äußeren Sicherheit scheint an Kontur zu verlieren. In verschiedenen Bereichen ist eine „Entgrenzung“ der Tätigkeit der Polizei- und Verfassungsschutzbehörden des Bundes und der Länder sowie der Streitkräfte festzustellen: So erfassen etwa Polizisten im Vorfeld konkreter Gefahrenlagen automatisch Kraftfahrzeugkennzeichen und schleusen heimlich „Bundestrojaner“ in die Personalcomputer ahnungsloser Bürger ein, um zur Bekämpfung des internationalen Terrorismus persönliche Daten auszuspähen. Die Bundespolizei wird sukzessive mit weit reichenden Befugnissen ausgestattet und zu Auslandseinsätzen entsandt, die Bundeswehr gerät im Rahmen eines ESVP-Einsatzes der Europäischen Union in bewaffnete Auseinandersetzungen mit Piraten am „Horn von Afrika“. Bei Europol und in internationalen gemeinsamen Zentren zu Zwecken der Terrorismusbekämpfung werden personenbezogene Daten deutscher Staatsangehöriger gesammelt, gespeichert und weiterverarbeitet. Deutsche Polizisten finden Verwendung im Rahmen internationaler Einsätze zur Sicherung der Außengrenzen der Europäischen Union. Die Trennlinie zwischen innerer und äußerer Sicherheit scheint zunehmend brüchig zu werden.

Sind diese Modifikationen der „Sicherheitsarchitektur“ durch eine gewandelte Gefährdungssituation gerechtfertigt, oder begegnen sie durchgreifenden verfassungsrechtlichen Bedenken? Es lässt sich nicht bestreiten, dass sich die Bewertung der Sicherheitslage in Deutschland, Europa und der Welt angesichts der in den Terroranschlägen des 11. September 2001 erstmals manifest gewordenen neuartigen Bedrohungspotenziale in den vergangenen Jahren zu Recht deutlich verändert hat. Im Zeitalter der Globalisierung¹ und der sich stetig intensivierenden Nutzung moderner Informations- und Kommunikationstechnik in der „digitalen Welt“² sind die nationalen staatlichen Sicherheitsakteure vor besondere Herausforderungen gestellt. Denn neben die neuartigen Ge-

¹ Zum Begriff etwa *U. Beck*, Was ist Globalisierung? Irrtümer des Globalismus – Antworten auf Globalisierung, 2007; *I. Kerner*, Globalisierung, in: G. Göhler/M. Iser/I. Kerner (Hrsg.), Politische Theorie. 22 umkämpfte Begriffe zur Einführung, 2004, S. 190ff.; vgl. zu den verfassungsrechtlichen Herausforderungen die Beiträge von *G. Nolte* und *R. Poscher*, VVDStRL Bd. 67 (2008), S. 129ff. und S. 160ff.

² Zu den Aufgaben der Polizei in der „digitalen Welt“ s. *J. Ziercke*, Kriminalistik 2008, 76ff.; s. auch *M. Gercke*, MMR 2008, 291ff., zur Bekämpfung der Internetkriminalität als Aufgabe der Strafverfolgungsbehörden.

fahrenlagen durch den naturwissenschaftlich-technischen Fortschritt treten weitere Gefährdungspotenziale, die etwa vom internationalen Terrorismus und der „Organisierten Kriminalität“ ausgehen. Diese Erscheinungen sind eng miteinander verknüpft: Denn einerseits bedienen sich Terroristen wie organisierte Kriminelle moderner Informations- und Kommunikationsmittel, wie sich etwa am aktuellen Beispiel der technisch „hochgerüsteten“ Piraten vor der Küste Somalias zeigt, zum anderen reagiert der Gesetzgeber auf die entsprechenden Bedrohungen unter anderem durch den Erlass höchst heterogener (und hinsichtlich ihrer verfassungsrechtlichen Unbedenklichkeit oftmals zweifelhafter) Befugnisnormen, die den Gefahrenabwehrbehörden den Einsatz moderner Informations- und Kommunikationstechnik erlauben. Flankiert werden diese Legislativmaßnahmen beispielsweise durch sicherheitspolitische Überlegungen, mittels einer Änderung des Grundgesetzes den Weg für den Einsatz der Streitkräfte im Inneren – etwa im Falle drohender bzw. bereits erfolgter Terroranschläge – frei zu machen, sowie durch die stetige Erweiterung der Aufgaben und Befugnisse der Bundespolizei.

Die Frage nach der Ausgestaltung der nationalen und internationalen „Sicherheitsarchitektur“ der Zukunft erweist sich als sensibel und diffizil. Denn der Gesetzgeber hat bei der gesetzlichen „Justierung“ des Verhältnisses von Freiheit und Sicherheit vielfältige verfassungsrechtliche Bindungen zu berücksichtigen und zugleich sowohl den Sicherheitsbedürfnissen in der Bevölkerung als auch den Vorgaben des Grundgesetzes bezüglich der Freiheit als Wert mit Verfassungsrang Rechnung zu tragen. Wie regelmäßig im Zusammenhang mit der Diskussion um die rechtliche Bewältigung des naturwissenschaftlich-technischen Fortschritts werden Stimmen laut, die dem Recht angesichts der neuartigen Gefährdungslagen insgesamt seine Steuerungsfähigkeit³ absprechen – nicht zuletzt auch deshalb, weil sich die verfassungsrechtlichen Direktiven unter Umständen als „Fesseln“ für die Entwicklung eines schlagkräftigen und effizienten öffentlichen Sicherheitsrechts erweisen können. Versagt also das Recht als Mittel der Gewährleistung und Regulierung sowie der „Hegung“ (privater) Gewalt, weil etwa die dezidierten grundrechtlichen Vorgaben beispielsweise den Erlass wirksamer, aber auch besonders einschneidender Eingriffsnormen weitgehend sperren, oder weil die Qualität der entsprechenden einfachgesetzlichen Normen angesichts der Komplexität der zu regelnden Lebenssachverhalte zu wünschen übrig lässt? Ist der Staat darüber hinaus angesichts dieser Entwicklungen darauf verwiesen, sich auf die Bereitschaft der Bevölkerung zur Gewaltlosigkeit zu verlassen? Wird künftig – in Abwandlung des Diktums von *Ernst-Wolfgang Böckenförde*⁴ – auch der „Sicherheitsstaat“

³ Zur „Steuerungskapazität“ des Rechts etwa *D. Neumann*, *Vorsorge und Verhältnismäßigkeit*, 1994, S. 206 ff.

⁴ *E.-W. Böckenförde*, *Staat, Gesellschaft, Freiheit. Studien zur Staatstheorie und zum Verfassungsrecht*, 1976, S. 60.

von Voraussetzungen leben müssen, die er selbst nicht garantieren kann? Im Gefahrenabwehrrecht verlegt sich der Gesetzgeber, wie bereits angedeutet, anstelle einer solchen Resignation weitgehend auf eine Vorverlagerung normativer Sicherungsmaßnahmen in den Bereich der Gefahrenvorsorge. Ob und inwieweit diese Maßnahmen sowie die entsprechenden informations- und kommunikationsbezogenen Eingriffsermächtigungen als verfassungskonform zu gelten haben, soll diese Untersuchung zeigen.

Angesichts der Verschiebungen der zeitlichen bzw. räumlichen „Ansatzpunkte“ gefahrenabwehrrechtlicher Bestimmungen kann von einer „*Entgrenzung*“ der Gefahrenabwehr, ja des Rechts der inneren und äußeren Sicherheit insgesamt gesprochen werden. Dies zeigt sich auch jenseits der Schaffung neuer Eingriffsermächtigungen anhand weiterer sicherheitsrelevanter Bereiche. Insgesamt lassen sich mehrere tatsächliche und rechtliche Entwicklungstendenzen ausmachen, die im Folgenden zu vier Ausprägungen typisiert werden sollen:⁵ Die Ausdifferenzierung einfachgesetzlicher gefahrenabwehrrechtlicher Eingriffsermächtigungen (u. 4. Teil), die Veränderungen in der föderalen Kompetenzordnung (u. 5. Teil), die Relativierung des sog. „Trennungsgebotes“ bezüglich Polizei- und Verfassungsschutzbehörden (u. 6. Teil) sowie die Internationalisierung und Europäisierung des Gefahrenabwehrrechts (u. 7. Teil).

Die staatstheoretischen und verfassungsrechtlichen Aspekte eines Rechts auf Sicherheit bzw. der damit korrespondierenden staatlichen Pflichten sind bereits und gerade auch in der jüngeren Vergangenheit ausführlich und präzise behandelt worden,⁶ ebenso der Themenkreis der Strafverfolgung und Gefahrenabwehr im Internet⁷ und die Rechtsfragen im Zusammenhang mit der „Bewältigung“ neuartiger Technologien.⁸ Eine umfassende Untersuchung der verfassungsrechtlichen, namentlich der grundrechtlichen Vorgaben für das Handeln

⁵ Eine ähnliche Typisierung nimmt *H.-J. Lange*, in: S. Huster/K. Rudolph (Hrsg.), *Vom Rechtsstaat zum Präventionsstaat*, 2008, S. 64 (65 ff.), für die Terrorismusbekämpfung vor; er ergänzt unter Auslassung der Internationalisierung als weitere Entwicklungstendenz die „Zunahme der gesellschaftlichen Kontrolle“.

⁶ *M. Möstl*, *Die staatliche Garantie für die öffentliche Sicherheit und Ordnung. Sicherheitsgewährleistungen im Verfassungsstaat, im Bundesstaat und in der Europäischen Union*, 2002; *P.-T. Stoll*, *Sicherheit als Aufgabe von Staat und Gesellschaft. Verfassungsordnung, Umwelt- und Technikrecht im Umgang mit Unsicherheit und Risiko*, 2003; zu neueren Entwicklungen im Sicherheitsrecht jüngst *M. Kötter*, *Pfade des Sicherheitsrechts. Begriffe von Sicherheit und Autonomie im Spiegel der sicherheitsrechtlichen Debatte der Bundesrepublik Deutschland*, 2008.

⁷ *M. Germann*, *Gefahrenabwehr und Strafverfolgung im Internet*, 2000; *A. Greiner*, *Die Verhinderung verbotener Internet-Inhalte im Wege polizeilicher Gefahrenabwehr*, 2001; *E. Perrey*, *Gefahrenabwehr und Internet. Befugnisse der Polizei im Lichte eines Rechts auf informationelle Selbstbestimmung*, 2002. – Allgemein zur Gefahrenabwehr vgl. etwa *R. Poscher*, *Gefahrenabwehr. Eine dogmatische Rekonstruktion*, 1999.

⁸ S. etwa nur die Beiträge von *J. Ipsen*, *D. Murswiek* und *B. Schlink*, *VVDStRL Bd. 48* (1990), S. 177 ff., S. 207 ff. und S. 235 ff.; s. auch *L. Jaeckel*, *Gefahrenabwehr und Risikodogmatik. Moderne Technologien im Spiegel des Verwaltungsrechts*, 2010, S. 5 ff.

der staatlichen „Sicherheitsakteure“ unter Berücksichtigung der aktuellen Entwicklungen in der Rechtspraxis und unter Einbeziehung der neuesten Judikatur des Bundesverfassungsgerichts zu den als „Informationseingriffe“ bezeichneten Maßnahmen der Gefahrenabwehr fehlt jedoch bislang.

In dieser Untersuchung werden zunächst die besonderen gegenwärtig bestehenden Gefährdungen herausgestellt (u. 1. Teil). Es schließt sich eine Bestimmung des Begriffs der „Gefahrenabwehr“ an (u. 2. Teil). Die Reaktionen des Gesetzgebers auf die neuartigen Gefährdungen unterliegen, obwohl er grundsätzlich selbst über das „Austarieren“ des Spannungsverhältnisses zwischen Freiheit und Sicherheit entscheiden kann (u. 3. Teil), einer Vielzahl verfassungsrechtlicher Bindungen, die jeweils am Beispiel der bereits genannten vier Entwicklungstendenzen sowie einzelner gefahrenabwehrrichtlicher Maßnahmen erörtert und verdeutlicht werden sollen (u. 4.–7. Teil). Die Untersuchung schließt mit einer zusammenfassenden Bewertung der aufgezeigten tatsächlichen Entwicklungen und Rechtsfragen.

1. Teil

Herausforderungen an das Recht der inneren und äußeren Sicherheit

Im Zeitalter der Globalisierung sind durch die tatsächlichen Entwicklungen besondere Herausforderungen an das Recht der inneren und äußeren Sicherheit sowie an die zur Durchsetzung dieses Rechts berufenen Sicherheitsbehörden gestellt. Diese Herausforderungen lassen sich im Wesentlichen in drei Kategorien einteilen, die im Folgenden als Referenzbereiche dienen sollen: Erstens die besonderen Gefährdungen, die durch die Ausprägung einer „Informationsgesellschaft“ entstehen, namentlich durch die vermehrte Nutzung moderner Informations- und Kommunikationstechnik auch zu verbotenen oder gar strafbaren Zwecken; die „Informationsgesellschaft“ – präziser: ihre infrastrukturellen Funktionsgrundlagen – erweisen sich dabei als in besonderer Weise „verletzlich“ (s. u. A.). Von eminenter Bedeutung ist dabei insbesondere die sog. „Internet-Devianz“, also die missbräuchliche Verwendung des Netzes. Eine zweite Kategorie bilden die im Zusammenhang mit dem internationalen Terrorismus auftretenden neuartigen Bedrohungen (s. u. B.). Und schließlich ergeben sich aus der „Organisierten Kriminalität“ weitere spezifische Gefahrenlagen (s. u. C.).

Die drei Kategorien stehen nicht isoliert nebeneinander, sondern sind eng miteinander verknüpft: In allen Bereichen erhöht die Möglichkeit der Nutzung moderner Informations- und Kommunikationstechnik das Bedrohungspotenzial, und hinsichtlich aller drei Erscheinungsformen können (und müssen) die für die Gefahrenabwehr zuständigen Behörden ihrerseits zur Erfüllung ihrer Aufgaben auf die neuartigen technischen Möglichkeiten zurückgreifen. Darüber hinaus sind sie namentlich im Zusammenhang mit der Bekämpfung des internationalen Terrorismus und der „Organisierten Kriminalität“ auf eine umfassende Erhebung von Informationen sowie auf deren Austausch im Wege behördlicher Kooperation angewiesen.

A. Die „Informationsgesellschaft“ und ihre Gefährdungen

I. Ausprägung und Charakteristika der „Informationsgesellschaft“

Charakteristisch für das Zeitalter der Globalisierung ist unter anderem die Ausprägung einer sog. „Informationsgesellschaft“. Die gesellschaftlichen Gegebenheiten in Deutschland sind wegen des stetigen Fortschritts im Bereich der Informations- und Kommunikationstechnik einem tief greifenden Wandel unterworfen. Deutschland befinde sich, so hört und liest man oft, auf dem Weg in die „Informationsgesellschaft“.¹ Nicht selten wird davon ausgegangen, man sei dort bereits angekommen.² Der Übergang von einer international kooperierenden nationalen Industriegesellschaft zur ebenso hoch gepriesenen wie scharf attackierten globalen Informationsgesellschaft geschieht fließend. Ob und inwieweit jedoch eine solche Informationsgesellschaft schon heute Status quo oder nur Zukunftsmusik ist, hängt von den Kriterien ab, anhand derer man eine Qualifizierung der Gesellschaft vornehmen möchte.

1. Die gesellschaftliche Bedeutung der „Information“

Die *information society* ist als Begriff, Schlagwort und Argumentationstopos indes bereits in aller Munde – Wirtschafts- und Umweltwissenschaftler, Informatiker und Soziologen, Ingenieure und Juristen nähern sich den Chancen und Risiken einer mehr und mehr durch Information und Kommunikation geprägten Gesellschaft mit den ihren Disziplinen jeweils eigenen Methoden und Mitteln.³ Sie alle ringen um eine optimale, für die Zukunft tragfähige Ausgestaltung der *Informationsgesellschaftsordnung*. Allein die stetig wachsende Be-

¹ S. etwa schon die Beiträge in *J. Tauss/J. Kollbeck/J. Mönikes* (Hrsg.), *Deutschlands Weg in die Informationsgesellschaft. Herausforderungen und Perspektiven für Wirtschaft, Wissenschaft, Recht und Politik*, 1996; ferner *T. Dreier*, in: *Freundesgabe f. A. Büllesbach*, 2002, S. 65 ff.; *O. Depenbeuer*, AfP 1997, 669 ff.; *U. Sieber*, CR 1995, 100 (110 f.); s. auch schon *A. Roßnagel/P. Wedde/V. Hammer/U. Pordesch*, *Die Verletzlichkeit der „Informationsgesellschaft“*, 2. Aufl. 1989.

² *M. Kloepfer*, *Informationsrecht*, 2002, § 1 Rdnrn. 1 ff.; s. auch *K. Stobrer*, BayVBl. 2005, 489 ff.; *T. Würtenberger*, in: *D. Leipold* (Hrsg.), *Rechtsfragen des Internet und der Informationsgesellschaft*, 2002, S. 3 ff.

³ Aus dem kaum überschaubaren allgemeinen und speziellen Schrifttum s. etwa nur *A. Mattelart*, *Kleine Geschichte der Informationsgesellschaft*, 2003; *G. Wersig*, *Die Komplexität der Informationsgesellschaft*, 1996; zu verschiedenen theoretischen (sozialwissenschaftlichen) Ansätzen eingehend *J. Steinbicker*, *Zur Theorie der Informationsgesellschaft*, 2001; aus rechtswissenschaftlicher Sicht s. die Überblicke bei *M. Kloepfer/A. Neun*, EuR 2000, 512 ff.; zum sicherheitspolitischen Forschungsstand vgl. *J. Troy*, in: *M. H. W. Möllers/R. C. v. Ooyen* (Hrsg.), *Jahrbuch Öffentliche Sicherheit 2008/2009*, 2009, S. 53 ff.; s. auch den Überblick über den Zugang verschiedener Disziplinen bei *J. Tauss/J. Kollbeck/J. Mönikes*, in: *dies.* (Hrsg.), *Deutschlands Weg in die Informationsgesellschaft*, 1996, S. 14 ff.

deutung des Internets und die steigende Nutzungsquote⁴ verursachen dabei Probleme, die zwingend zu lösen sind: So stellt etwa die sog. „Internet-Deviananz“⁵ im Sinne eines Missbrauchs des Netzes für rechtswidrige Zwecke für die Gefahrenabwehr- und Strafverfolgungsbehörden eine der großen Herausforderungen der Gegenwart dar. Beispielhaft genannt seien nur strafbare Inhalte auf Webseiten⁶ wie etwa rechtsradikales, volksverhetzendes Gedankengut,⁷ Kinderpornographie oder illegale Glücksspielangebote.

Versteht man die Informationsgesellschaft als eine auf Informations- und Kommunikationstechnik basierende „Transformationsgesellschaft“ und „Informationsökonomie“, die durch eine Durchdringung sämtlicher Lebensbereiche mit dieser Technik („Informatisierung“)⁸ gekennzeichnet ist, verdeutlicht dies freilich nur ansatzweise die dahinter stehenden, künftig zu bewältigenden Konflikte und Probleme. Nicht ohne Grund gilt das Merkmal der Komplexität als wesentliches Kennzeichen der gegenwärtigen Transformationsgesellschaft.⁹ Obwohl die Fortentwicklung (zu) einer Informationsgesellschaft eben dieser Komplexität durch eine Verringerung von Ungewissheiten und Unsicherheiten wehren soll,¹⁰ führen die Fülle an Informationen und die Möglichkeiten eines grenzüberschreitenden, globalen Informationsaustauschs ihrerseits zu einer Erhöhung der Komplexität. Die Nutzung namentlich des Internets hat sich zunehmend zu einer (in verschiedenen Bereichen bereits unverzichtbaren) „Kulturfertigkeit“ entwickelt, das *World Wide Web* wird – wie all-

⁴ Dazu etwa *M. Gercke*, MMR 2008, 291 (293); *R. Röger*, ZRP 1997, 203 (204); zur weltweiten Verbreitung s. auch *A. Roßnagel*, MMR 2002, 67ff. – Das Internet ist freilich nicht „global“; s. zum sog. „*digital divide*“ in internationaler Hinsicht *G. Walter*, Internetkriminalität. Eine Schattenseite der Globalisierung, 2008, S. 7f.; ähnlich *R. Röger*, a.a.O.: „Kommunikationsmittel der Elite“; a. A. *A. Roßnagel*, a.a.O.

⁵ Zur Computerkriminalität allgemein *S. Beukelmann*, NJW-Spezial 2004 Heft 3, 104ff.; *U. Sieber*, CR 1995, 100ff.; *ders.*, BB 1982, 1433ff.; zur Medienethik des Internets *M. Sandborth*, CR 1998, 311ff.; zur öffentlich-rechtlichen Beurteilung s. *P. G. Mayer*, Das Internet im öffentlichen Recht. Unter Berücksichtigung europarechtlicher und völkerrechtlicher Vorgaben, 1999.

⁶ Zur Indizierung solcher Internet-Angebote und den strafrechtlichen Folgen *D. Beisel/B. Heinrich*, CR 1997, 360ff.

⁷ Zur strafrechtlichen Behandlung rechtsextremistischer Propaganda aus dem Ausland s. *K. Ringel*, CR 1997, 302ff.; s. auch *B. Breuer*, MMR 1998, 141ff.; zur Verbreitung strafrechtlich verbotener Schriften *M. Löbnig*, JR 1997, 496ff.

⁸ Zu diesem Begriff schon *S. Nora/A. Minc*, Die Informatisierung der Gesellschaft, 1979; *G. Wersig*, Informatisierung und Gesellschaft. Wie bewältigen wir die neuen Informations- und Kommunikationstechnologien, 1983; s. ferner *F. Schoch*, VVDStRL Bd. 57 (1998), S. 158 (160ff.). – Aus „Verwaltungssicht“ s. etwa *M. Hamer*, Informatisierung des Verwaltungsprozesses. Berücksichtigung der Möglichkeiten moderner Informations- und Kommunikationstechniken bei der Gestaltung und Auslegung der Normen des Verwaltungsprozessrechts, 2002.

⁹ Vgl. die Darstellung zu verschiedenen Ansätzen bei *G. Wersig*, Die Komplexität der Informationsgesellschaft, 1996, S. 9ff.

¹⁰ Eingehend *G. Wersig*, Die Komplexität der Informationsgesellschaft, 1996, S. 9ff.

gemein der Gebrauch der Informationstechnik als Grundrechtsentfaltung gedeutet werden kann¹¹ – als Faktor der Meinungsbildung,¹² der Zugang für möglichst breite Bevölkerungsschichten als Element der Daseinsvorsorge qualifiziert,¹³ und unter dem Banner der Verwaltungsvereinfachung, der Effizienz und der Wirtschaftlichkeit werden in neuartige Handlungsformen wie das *Electronic Government*¹⁴, die *Electronic Administration*, den *Electronic Commerce*¹⁵ und sogar in die *Electronic Democracy*¹⁶ große, nicht selten übertriebene Hoffnungen gesetzt.

2. Anforderungen an die Rechtsordnung

Teil der Debatte um die künftige Konturierung der Informationsgesellschaft sind die vielfältigen Diskussionen um die Anpassung der *Rechtsordnung* an den stetigen Fortschritt namentlich der Kommunikations- und Informationstechnik. Für die Rechtswissenschaften erweist sich freilich die Bewältigung der teilweise neuartigen Probleme einer mehr und mehr von Informationen und Informationsaustausch beeinflussten Lebenswirklichkeit, der „Aufstieg neuer Wissenstechnologien“¹⁷, als besonders schwierig.¹⁸ So sieht sich insbesondere das

¹¹ Dazu *K. Haefner*, in: A. Roßnagel (Hrsg.), *Freiheit im Griff. Informationsgesellschaft und Grundgesetz*, 1989, S. 31 ff.

¹² *W. Mecklenburg*, ZUM 1997, 525 (530 ff.), unter Hinweis auf die Rechtsprechung des BVerfG zur Bedeutung des Rundfunks: BVerfGE 12, 205 (260 f.); zur Presse ähnlich BVerfGE 20, 162 (174 f.).

¹³ Zur Bedeutung des Internets und zu seinen sozialen Funktionen vgl. *W. Mecklenburg*, ZUM 1997, 525 ff.

¹⁴ *M. Kloepfer*, *Informationsrecht*, 2002, § 1 Rdnrn. 33 ff.; ferner aus dem umfangreichen Schrifttum etwa *G. Britz*, in: W. Hoffmann-Riem/E. Schmidt-Aßmann/A. Voßkuhle (Hrsg.), *Grundlagen des Verwaltungsrechts*, Bd. II, 2008, Rdnrn. 1 ff.; *M. Eifert*, *Electronic Government. Das Recht der elektronischen Verwaltung*, 2006; *T. Fetzer*, in: C. Prins (Hrsg.), *Designing E-Government*, 2007, S. 185 ff.; *J. v. Lucke/H. Reinermann*, in: H. Reinermann/J. v. Lucke (Hrsg.), *Electronic Government in Deutschland*, 2. Aufl. 2002, S. 1 ff.; *H. Hill*, BayVBl. 2003, 737 ff.; *U. Schliesky*, NVwZ 2003, 1322 ff.; *ders.*, LKV 2005, 89 ff.; auf die „geringe Distanz“ des Staates zur Informations- und Kommunikationstechnik weist *B. Schlink*, VVDStRL Bd. 48 (1990), S. 235 (236 ff., 240), hin. – Zum Grundrechtsschutz gegen „aufgedrängtes E-Government“ *D. Heckmann*, MMR 2006, 3 ff.

¹⁵ *M. Kloepfer*, *Informationsrecht*, 2002, § 1 Rdnrn. 20 ff.

¹⁶ *M. Kloepfer*, *Informationsrecht*, 2002, § 1 Rdnrn. 31 f.; *B. Holznagel/A. Grünwald/A. Hanßmann*, *Elektronische Demokratie*, 2001; ferner *N. Bremke*, LKV 2004, 102 ff.; *O. R. Rüß*, MMR 2000, 73 ff.; *ders.*, ZRP 2001, 518 ff. (insbesondere zu Wahlen im Internet – „e-Voting“); dazu eingehend etwa *A. Hanßmann*, *Möglichkeiten und Grenzen von Internetwahlen*, 2004; *M. Will*, *Internetwahlen. Verfassungsrechtliche Möglichkeiten und Grenzen*, 2002.

¹⁷ *K.-H. Ladeur*, DÖV 2009, 45 (46).

¹⁸ S. grundlegend schon *W. Zöllner*, *Informationsordnung und Recht*, 1990; ferner *H. P. Bull*, *Die Grundprobleme des Informationsrechts*, 1985; *A. Roßnagel*, ZRP 1997, 26 ff.; s. auch *T. Hoeren*, NJW 1998, 2849: „Dematerialisierung“. – Zu den öffentlich-rechtlichen Rahmenbedingungen einer Informationsordnung *I. Ebsen*, DVBl. 1997, 1039 ff.; s. auch *O. Depenheuer*, AfP 1997, 669 ff.; *I. Geis*, NJW 1997, 288; *R. Röger*, ZRP 1997, 203 ff.

klassischer Weise an den Kategorien von „Gefahr“ und „Störer“,¹⁹ von ordnungsrechtlicher Verantwortlichkeit und der Inanspruchnahme des „Nichtstörers“, von Rechtsgüterabwägungen und Verhältnismäßigkeitsgesichtspunkten orientierte Gefahrenabwehrrecht mit neuen Herausforderungen konfrontiert. Einerseits bewirkt die „Entthronung der Materie“²⁰ durch das digitale Zeitalter das Auftreten neuartiger Gefahrenlagen und Risiken, die sich mit dem herkömmlichen Eingriffsinstrumentarium nur schwerlich angemessen beseitigen bzw. vermeiden lassen, andererseits werden den zur Gefahrenabwehr berufenen Behörden durch die Informations- und Kommunikationstechnik neue Möglichkeiten zur Bewältigung ihrer (sich in verschiedenen Bereichen sukzessive erweiternden²¹) Aufgaben an die Hand gegeben. Man denke nur an die Informationsbeschaffung durch behördliches „Surfen“ im Internet, die Überwachung moderner Kommunikationsmittel und die durch die globale Vernetzung erheblich erleichterte und beschleunigte Kooperation mit ausländischen Behörden etwa im Bereich der Strafverfolgung,²² aber auch an die Integration biometrischer Daten in Ausweispaapiere.²³ Die staatliche „Datenmacht“ im Sinne eines Informationsvorsprungs des Hoheitsträgers hinsichtlich (personenbezogener) Daten erweist sich damit auch als wichtige Voraussetzung für die Gewährleistung von Sicherheit.²⁴ Andererseits stellt gerade das Internet – insbesondere wegen seiner Internationalität, der Netzwerkstruktur und der „Flüchtigkeit“ seiner virtuellen Inhalte – unter rechtlichen Aspekten eine Herausforderung für die Rechtsordnung und ihre „regulatorische Imaginationskraft“ dar.²⁵ *Karl-*

¹⁹ Zur Abkehr von dieser Dogmatik durch die Verstärkung von Polizeibefugnissen im informationellen Vorfeld etwa *M. Möstl*, DVBl. 2007, 581 (583); zur dogmatischen Einordnung des Störerbegriffs in einer zunehmend technisierten Gesellschaft *J. Kokott*, DVBl. 1992, 749 ff.

²⁰ *E. Dyson/G. Gilder/G. Keyworth/A. Toffler*, Cyberspace and the American Dream: A Magna Charta for the Knowledge Age, Information Society 1996, S. 295 ff.

²¹ S. dazu u. 4. Teil.

²² S. dazu u. 7. Teil.

²³ *C. Mager*, Terrorismusbekämpfung zwischen Freiheit und Sicherheit, 2005, S. 191 ff.; *S. Mittel*, in: M.H.W. Möllers/R.C. v. Ooyen (Hrsg.), Jahrbuch Öffentliche Sicherheit 2008/2009, 2009, S. 153 (164 ff.); zu den gemeinschaftsrechtlichen Vorgaben *A. Roßnagel/G. Hornung*, DÖV 2005, 983 ff.; s. auch *dies.*, DÖV 2009, 301 ff. – Biometrische Daten sind personenbezogene Daten und unterfallen dem Schutz des Rechts auf informationelle Selbstbestimmung gemäß Art. 2 Abs. 1 i. V.m. Art. 1 Abs. 1 GG; zu diesem Grundrecht eingehend u. 4. Teil, D. II.

²⁴ Eingehend *K. v. Lewinski*, in: F. Arndt u. a. (Hrsg.), Freiheit – Sicherheit – Öffentlichkeit. 48. Assistententagung Öffentliches Recht, 2009, S. 196 (201 ff.); *K. Stobrer*, BayVBl. 2005, 489 (490).

²⁵ *M. Herberger*, NJW 1998, 2801; zu den Akteuren im Internet vgl. *S. Ernst*, JuS 1997, 776 ff. – Nicht selten wird betont, dass transnationale Netze wie das Internet einer staatlichen Regulierung fast nicht zugänglich seien, s. etwa *W. Hoffmann-Riem*, AöR Bd. 123 (1998), S. 513 (533); ferner *A. Roßnagel*, ZRP 1997, 26 ff.; *J. Scherer*, AfP 1996, 213 ff.; s. auch *O. Deppenheuer*, AfP 1997, 669 (672): „prinzipielle Unbeherrschbarkeit der sich global entfaltenden

Heinz Ladewig hat zu Recht auf die Notwendigkeit einer Regulierung des Internets durch „lernfähiges Recht“ hingewiesen.²⁶

Sowohl auf die neuartigen Gefahrenpotenziale als auch auf die verbesserten eigenen technischen Möglichkeiten zum Zwecke der Gefahrenabwehr reagiert der Gesetzgeber durch eine stetige Anpassung allgemeiner und besonderer ordnungsrechtlicher Regelwerke. Eine Folge ist etwa die Aufnahme neuer (informations- und kommunikationsbezogener) Standardermächtigungen in die Polizei- und Ordnungsgesetze der Länder. Dies trägt der Tatsache Rechnung, dass Polizeiarbeit heute im Wesentlichen vom Umgang mit Informationen bestimmt ist²⁷ und deren Gewinnung, Verarbeitung und Speicherung zu späterer Verwendung daher eine zentrale Rolle spielen. Gefahrenabwehrbezogenes Informationsrecht reguliert vorrangig die Erhebung, Übermittlung und Nutzung von Informationen; Ansatzpunkte sind dabei Informations- und Kommunikationsinfrastruktur, Übertragungswege und Speicherorte. So sind etwa die gefahrenabwehrrechtlichen Standardermächtigungen zur Datenerhebung und Datenverarbeitung als „spezifisches (Polizei-)Informationsrecht“ qualifiziert worden.²⁸ Der technische Fortschritt hat die inhaltliche Qualität der nutzbaren Informationen freilich weitestgehend unverändert gelassen. „Der Läufer von Marathon meldete keinen besseren Sieg als der drahtlose Telegraph“.²⁹

Grundlegend verändert haben sich jedoch Menge, „Dichte“, Übertragungsgeschwindigkeit und Nutzungsmöglichkeiten von Informationen; ein Umstand, der dazu geführt hat, dass das Bundesverfassungsgericht in seiner Judikatur zu den sog. „Informationseingriffen“ Gesetzgeber und Behörden beharrlich zu einem zurückhaltenden und behutsamen Umgang mit personenbezogenen (und damit grundrechtssensiblen) Daten mahnt. Denn nicht selten geraten neu in die gefahrenabwehrrechtlichen Regelwerke aufgenommene Standardermächtigungen – namentlich solche mit „Informationsbezug“ – trotz (oder gerade auch wegen) ihrer detaillierten tatbestandlichen Fassung in Kollision mit verfassungsrechtlichen, namentlich grundrechtlichen Vorgaben.

Die einfachgesetzlichen Rahmenbedingungen zur Schaffung und Aufrechterhaltung eines gewissen Grades an Sicherheit wandeln sich also in Anpassung an technischen Fortschritt und neuartige Bedrohungspotenziale³⁰ stetig. Regu-

Informationsgesellschaft“; zur Kontrollierbarkeit des Internets aus technischer Sicht etwa H. Federrath, ZUM 1999, 177 ff.

²⁶ K.-H. Ladewig, ZUM 1997, 372 (375 ff.).

²⁷ Vgl. C. Gusy, Polizeirecht, 7. Aufl. 2009, Rdnr. 185; zur Entwicklung und zur Praxis polizeilicher Informationstätigkeit s. T. Petri, in: H. Lisken/E. Denninger (Hrsg.), Handbuch des Polizeirechts, 4. Aufl. 2007, Rdnrn. H 60 ff.

²⁸ D. Peitsch, ZRP 1992, 127 ff.; R. Pitschas, ZRP 1993, 174 ff.; F. Schoch, in: E. Schmidt-Aßmann/F. Schoch (Hrsg.), Besonderes Verwaltungsrecht, 14. Aufl. 2008, 2. Kap. Rdnr. 244.

²⁹ E. Jünger, Der Arbeiter. Herrschaft und Gestalt, 1932/1982, S. 180.

³⁰ Eine deutliche Verlagerung zugunsten der Sicherheitsgewährleistung ist nach den terroristischen Anschlägen vom 11. September 2001 auf die Vereinigten Staaten von Amerika und

lierungsbestrebungen zur künftigen dauerhaften Gewährleistung von Sicherheit erfassen dabei sowohl die nationale als auch die europäische Ebene; die Gestalt der „Sicherheitsarchitektur“ ist in dauerndem Wandel begriffen; ihre rechtlichen Grundlagen werden nicht selten als „Bekämpfungsrecht“³¹ und ihrer „offensiven“, häufig grundrechtsbeschränkenden Wirkung wegen mit kritischem Blick gesehen. Diese Entwicklung, oftmals pointiert als „Spurwechsel von der Freiheit zu Sicherheit“³² bezeichnet, stellt auch an das Verfassungsrecht, namentlich die Grundrechtsdogmatik, besondere Herausforderungen.

Die Kritik an gesetzlichen Ermächtigungsnormen namentlich zu „Informationseingriffen“ vermengt sich nicht selten mit einer allgemeinen Schelte der Gefahrenabwehrbehörden. Der Vertrauensvorschuss, den sie hinsichtlich eines rechtsstaatgemäßen Verhaltens genossen haben, schwindet zusehends. Schon *Gustav Radbruch* hat die These von der Überparteilichkeit des Staates als „Lebenslüge des Obrigkeitsstaats“³³ bezeichnet – die Gegner erweiterter gefahrenabwehrrechtlicher Befugnisse schlagen in dieselbe Kerbe: Man fürchtet die Ausprägung eines „Überwachungsstaates“ unter Zurückdrängung oder Vernachlässigung rechtsstaatlicher Bindungen und die willkürliche Ausweitung gesetzlicher Eingriffsbefugnisse zu Lasten des Grundrechtsschutzes, denen – wehret den Anfängen! – im Interesse der Freiheit gesteuert werden müsse.

Jenseits aller Polemik hat das Bundesverfassungsgericht den Gefährdungen, die dem Bürger aus der stetigen Anpassung und Erweiterung insbesondere der gefahrenabwehrrechtlichen Eingriffsermächtigungen erwachsen, durch eine Erweiterung des sozusagen „ungeschriebenen“ Grundrechtekanons Rechnung getragen und beispielsweise dem allgemeinen Persönlichkeitsrecht aus Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG – selbst schon vom Bundesverfassungsgericht aus der Zusammenschau mehrerer ausdrücklich normierter Grundrechtspositionen entwickelt³⁴ –, als dessen Ausprägung seit längerem ein Recht auf informationelle Selbstbestimmung anerkannt ist,³⁵ ein Grundrecht auf Vertraulich-

nach den folgenden massiven Anschlägen (z. B. 11. April 2002 auf Djerba, 12. Oktober 2002 auf Bali, 11. März 2004 in Madrid, 7. Juli 2005 in London) zu beobachten gewesen. Im Schrifttum ist daher häufig von einem gewandelten „Sicherheitsparadigma“ die Rede. – Vgl. eingehend *C. Mager*, Terrorismusbekämpfung zwischen Freiheit und Sicherheit, 2005; *C. Gussy*, VVDStRL Bd. 63 (2004), S. 151 (153 m. w. N. in Fn. 2); *C. Calliess*, DVBl. 2003, 1096 ff.; *K. Nehm*, NJW 2002, 2665 ff.; zur internationalen Terrorismusbekämpfung aus völkerrechtlicher Sicht s. *C. Tomuschat*, DÖV 2006, 357 ff.

³¹ *G. Frankenberg*, KritJ 2005, S. 370 ff.

³² *G. Frankenberg*, KritJ 2005, S. 370 (385).

³³ *G. Radbruch*, Die politischen Parteien im System des deutschen Verfassungsrechts, in: *G. Anschütz/R. Thoma* (Hrsg.), Handbuch des deutschen Staatsrechts, Bd. 1, 1930, S. 285 (289).

³⁴ Zur dogmatischen Figur der „Verbindung“ von Grundrechten vgl. eingehend *M. M. Meinke*, In Verbindung mit. Die Verbindung von Grundrechten miteinander und mit anderen Bestimmungen des Grundgesetzes in der Rechtsprechung des Bundesverfassungsgerichts, 2006.

³⁵ S. u. 4. Teil, D. II.

keit und Integrität informationstechnischer Systeme³⁶ entnommen. Dieses setzt etwa der sog. „Online-Durchsuchung“, der im Wege technischer „Infiltration“ erfolgenden heimlichen behördlichen Durchsicht und Überwachung privater Computer und anderer Systeme, die zur Speicherung persönlichkeitsrelevanter Informationen geeignet sind und genutzt werden, verhältnismäßig enge Grenzen.

3. Wachsende Bedeutung der Vorsorge

Doch nicht nur im Zusammenhang mit den Regelungen zur Gefahrenabwehr sind permanente Anpassungstendenzen festzustellen. Der Gesichtspunkt der Gefahrenvermeidung³⁷ tritt angesichts einer zunehmenden Schwierigkeit, die Folgewirkungen des naturwissenschaftlich-technischen Fortschritts hinreichend sicher zu prognostizieren, auch in den rechtlichen Rahmenbedingungen in den Vordergrund.³⁸ Das klassische „Gefahrenabwehrrecht“ weicht nicht nur im Bereich des Umweltrechts einer umfassenden Gefahrenvorsorge³⁹ bzw. „Ri-

³⁶ BVerfGE 120, 274 ff.; s. dazu eingehend u. 4. Teil, D. III.

³⁷ Zur begrifflichen Unterscheidung von der Gefahrenabwehr s. schon F. Ossenbühl, NVwZ 1986, 161 (162).

³⁸ Zum Problem der rechtlichen Fassung technischer Risiken s. bereits A. Roßnagel, UPR 1986, 46 ff.

³⁹ Zu diesem Wandel eingehend I. Appel, Staatliche Zukunfts- und Entwicklungsvorsorge, 2005, S. 50 ff.; U. Di Fabio, in: Festschrift f. G. Ritter, 1997, S. 807 ff.; D. Grimm, KritV 1986, S. 38 (40 ff.); C. Gusy, VVDStRL Bd. 63 (2004), S. 151 (158); G. Lübke-Wolff, in: J. Bizer/H.-J. Koch (Hrsg.), Sicherheit, Vielfalt, Solidarität. Ein neues Paradigma des Verfassungsrechts?, 1998, S. 47 ff.; D. Neumann, Vorsorge und Verhältnismäßigkeit, 1994, S. 23 ff.; R. Poscher, Die Verwaltung Bd. 41 (2008), S. 345 (346 ff.); U. K. Preuß, in: D. Grimm (Hrsg.), Staatsaufgaben, 1994, S. 523 ff.; M. Soiné, DÖV 2000, 173 (174), auch zum Begriff der „Vorbereitung auf die Gefahrenabwehr“; R. Wahl/I. Appel, in: R. Wahl (Hrsg.), Prävention und Vorsorge. Von der Staatsaufgabe zu den verwaltungsrechtlichen Instrumenten, 1995, S. 1 (13 ff.); zum Begriff der Gefahrenvorsorge grundlegend schon G. Roth, Die Gefahrenvorsorge im sozialen Rechtsstaat, 1968, S. 9 f.; kritisch noch H. P. Bull, Die Staatsaufgaben nach dem Grundgesetz, 2. Aufl. 1977, S. 424, der aber auch die Entwicklung vom punktuellen und reaktiven Staatshandeln zu vorsorgender Tätigkeit konstatiert. – Aus dem nahezu unüberschaubaren Schrifttum zu einzelnen gefahrenabwehrrechtlichen Teilregelungsbereichen und zur „Informationsvorsorge“ beispielhaft M. Albers, Die Determination polizeilicher Tätigkeit in den Bereichen der Straftatenverhütung und der Verfolgungsvorsorge, 2001, S. 97 ff., 116 ff., 250 ff., 347 ff.; J. Aulehner, Polizeiliche Gefahren- und Informationsvorsorge. Grundlagen, Rechts- und Vollzugsstrukturen, dargestellt auch im Hinblick auf die deutsche Beteiligung an einem Europäischen Polizeiamt (EUROPOL), 1998, S. 47 ff., 545 ff.; D. Grimm, a.a.O., S. 38 (40 ff.); M. Kloepfer, Informationsrecht, 2002, § 4 Rdnrn. 37 ff.; R. Pitschas, in: ders. (Hrsg.), Kriminalprävention und „Neues Polizeirecht“. Zum Strukturwandel des Verwaltungsrechts in der Risikogesellschaft, 2002, S. 241 (242 ff.); H.-H. Trute, in: Gedächtnisschrift f. B. Jeand’Heur, 1999, S. 403 (405 ff.); M. A. Zöller, Informationssysteme und Vorfeldmaßnahmen von Polizei, Staatsanwaltschaft und Nachrichtendiensten. Zur Vernetzung von Strafverfolgung und Kriminalitätsverhütung im Zeitalter von multimedialer Kommunikation und Persönlichkeitsschutz, 2002, S. 77 ff.

sikovorsorge⁴⁰ – schon 1982 hat *Wolfgang Martens* festgestellt, dass die Gefahrenabwehr die Evidenz verloren habe, die lange Zeit mit diesem Begriff verbunden war.⁴¹ Auch der Vorsorgegedanke ist freilich nicht neu; so hat bereits 1938 *Ernst Forsthoff* festgestellt, der „prämoderne Polizeistaat“ konnte

„Kant tadeln, Schiller zensurieren und die Verbreitung deterministischer Lehren verbieten, er konnte gewiß bis in die Einzelheiten hinein bestimmen, wie gelebt werden sollte. Aber die Vorsorge dafür, daß überhaupt gelebt werden kann, lag nicht annähernd in gleichem Umfang bei ihm, wie heute.“⁴²

Ausgehend von den frühen sektorspezifischen umweltrechtlichen Kodifikationen wie etwa dem Atomgesetz und dem Bundes-Immissionsschutzgesetz, hat der Vorsorgegedanke inzwischen nahezu alle Bereiche des Ordnungsrechts erfasst. Dies führt – namentlich im Zusammenhang mit dem noch immer nicht abschließend und zufriedenstellend definierten und konkretisierten Begriff des „Risikos“, der in den Rechtswissenschaften eine beachtliche Karriere⁴³ absolviert hat – zu erheblichen Schwierigkeiten bei der Normsetzung und -anwendung – der „Präventionsstaat“⁴⁴ (von *Ernst Forsthoff* zu Recht bereits als Komplement zur Industriegesellschaft bezeichnet⁴⁵) fordert den Rechtsstaat.⁴⁶ Zu weit ginge es aber, von einem „Paradigmenwechsel“ von der Gefahrenabwehr zur umfassenden Risikosteuerung auszugehen.⁴⁷ Denn die traditionellen präventiv-polizeilichen Tätigkeitsbereiche werden durch Vorsorgemaßnahmen keineswegs völlig in den Hintergrund gedrängt, sondern besitzen im Gegenteil insbesondere durch die Erweiterung der gesetzlichen Befugnisse hinsichtlich von „Informationseingriffen“ jedenfalls in der Praxis erhebliche Bedeutung.

⁴⁰ S. allgemein etwa *W. Köck*, AÖR Bd. 121 (1996), S. 1 ff.; *R. Wahl/I. Appel*, in: *R. Wahl* (Hrsg.), *Prävention und Vorsorge*, 1995, S. 1 (13 ff.), zur „Staatsaufgabe Risikovorsorge“; zur Risikovorsorge im Gefahrenabwehrrecht der Informationsgesellschaft *D. Kugelmann*, *Polizei- und Ordnungsrecht*, 2006, 1. Kap. Rdnrn. 121 ff.; zur Kopplung von „Risiko“ und „Vorsorge“ jüngst *L. Jaeckel*, *Gefahrenabwehr und Risikodogmatik*, 2010, S. 277 ff.

⁴¹ *W. Martens*, DÖV 1982, 89 ff. – Zur Unzulänglichkeit traditioneller Gefahrenabwehr pointiert *W. Hoffmann-Riem*, ZRP 2002, 497 (499).

⁴² *E. Forsthoff*, *Die Verwaltung als Leistungsträger*, 1938, S. 8.

⁴³ Dazu *I. Appel*, NuR 1996, 227 ff.

⁴⁴ Zu diesem Begriff *E. Denninger*, *KritJ* 1988, S. 1 ff.

⁴⁵ *E. Forsthoff*, *Der Staat der Industriegesellschaft*. Dargestellt am Beispiel der Bundesrepublik Deutschland, 2. Aufl. 1971, S. 164 ff.

⁴⁶ Zu rechtsstaatlichen Defiziten im Zusammenhang mit Verdachtsgewinnungseingriffen s. *W. Hoffmann-Riem*, ZRP 2002, 497 (499 f.).

⁴⁷ So aber *J. Aulehner*, *Polizeiliche Gefahren- und Informationsvorsorge*, 1998, S. 548; dagegen *C. Gusy*, *VVDStRL* Bd. 63 (2004), S. 151 (189); *M. Möstl*, *Die staatliche Garantie für die öffentliche Sicherheit und Ordnung. Sicherheitsgewährleistung im Verfassungsstaat, im Bundesstaat und in der Europäischen Union*, 2002, S. 196; s. auch *E. Denninger*, in: *S. Huster/K. Rudolph* (Hrsg.), *Vom Rechtsstaat zum Präventionsstaat*, 2008, S. 85 (88 m. Fn. 1): Ein solcher „allgemeiner Paradigmenwechsel hin zu einer umfassenden Risikosteuerung wäre unter dem Grundgesetz nicht zulässig.“

Konzepte und Maßnahmen der Risikosteuerung flankieren diese klassischen Betätigungsfelder der Gefahrenabwehrbehörden lediglich.

4. Informationsgesellschaft und Steuerungsfunktion des Rechts

Die dargestellte Problematik der Normsetzung weist Weiterungen auf. Denn die *rechtliche* Bewältigung der modernen Gesellschaft sieht sich mit gravierenden Schwierigkeiten konfrontiert. Das Recht droht seine Steuerungsfunktion insgesamt zu verlieren.⁴⁸ Nicht nur die namentlich hinsichtlich illegaler Angebote im Internet zu beklagenden erheblichen Vollzugsdefizite mindern die Tauglichkeit gesetzlicher Regelungen zum Zwecke der Gefahrenabwehr möglicherweise sogar bis unter die verfassungsrechtlich relevante Geeignetheitsschwelle herab,⁴⁹ und die nationale Rechtsordnung hat das Problem des „Auswanderns in andere Rechtsordnungen“ zu bewältigen, das sie unter Umständen selbst fördert⁵⁰ – das Recht als Steuerungsinstrument sieht sich ganz allgemein einer fundamentalen Kritik gegenüber: Von vielen Teilnehmern der „Net-Community“ wird etwa – verbunden mit Phantasien von einer „Basisdemokratie“, einem „herrschaftsfreien Diskurs“ im Netz – eine „Rechtsfreiheit“ des Internets, ein eigenen, systemimmanenten normativen Regelungen unterworfenen und damit rechtsexemter virtueller Raum gefordert⁵¹ und auf den vermehrten Einsatz von Selbstregulierungsmechanismen („*netiquette*“ etc.) unter Zurückdrängung herkömmlicher normativ-regulativer Instrumente⁵² bzw. in Form

⁴⁸ Zum Verlust der Steuerungsfähigkeit des Rechts im Zusammenhang mit der „Risikoregulierung“ s. etwa R. Pitschas, *Verwaltungsverantwortung und Verwaltungsverfahren. Strukturprobleme, Funktionsbedingungen und Entwicklungsperspektiven eines konsensualen Verwaltungsrechts*, 1990, S. 48 ff.; ders., in: Festschrift f. H. Siedentopf, 2008, S. 285 ff.: „überforderte[r] Risikostaat“; G.-P. Calliess, *Prozedurales Recht*, 1999, S. 60 ff.; ferner D. Grimm, in: ders. (Hrsg.), *Wachsende Staatsaufgaben*, S. 291 (294 ff.); T. Ellwein/J. J. Hesse, *Der überforderte Staat*, 1994, S. 67 ff.; zu den rechtlichen Rahmenbedingungen für neuartige Informations- und Kommunikationsdienste s. G. M. Bröhl, CR 1997, 73 ff.

⁴⁹ S. die Beiträge in S. Huster/K. Rudolph (Hrsg.), *Vom Rechtsstaat zum Präventionsstaat*, 2009.

⁵⁰ H.-H. Trute, VVDStRL Bd. 57 (1998), S. 216 (248), sieht hier einen gewissen „Funktionsverlust des Nationalstaates“.

⁵¹ Dazu R. Wenning, JurPC Web-Dok. 16/1997; vgl. schon D. Johnson/D. Post, *Stanford Law Review* Bd. 48 (1996), S. 1367 ff.; s. auch G. Roellecke, *NJW* 1996, 1801 ff. – Zur Vorstellung von „rechtsfreien Räumen“ und zu ihrer Nutzung als Rechtfertigungsfigur s. allgemein C. Herbst/O. W. Lembcke, in: *Jahrbuch für Recht und Ethik* Bd. 14 (2006), S. 385 ff.

⁵² T. Hoeren hat kritisch darauf hingewiesen, dass es „die“ *netiquette* gar nicht gebe, s. *NJW* 1998, 2849 (2852); ders., in: J. Becker (Hrsg.), *Rechtsprobleme internationaler Datenetze*, 1996, S. 35 ff.; jedenfalls komme ihr keinerlei verbindliche Wirkung zu; ähnlich H.-H. Trute, VVDStRL Bd. 57 (1998), S. 216 (247), der angesichts der Pluralisierung der Nutzungsinteressen von einer Harmlosigkeit der Selbstverpflichtungen ausgeht; J. Scherer, *AFP* 1996, 213 (214), erklärt die Funktionalität der Selbstregulierung im Internet für „empirisch widerlegt“. – Zur Selbstregulierung in der Zivilgesellschaft G. Winter, *KritJ* 1998, S. 518 (523 ff.); zu den Defiziten der überkommenen administrativen Steuerung H.-H. Trute, a.a.O., S. 262 ff.; zur technischen Selbstregulierung im Internet H. Kube, in: J. Isensee/P. Kirchhof (Hrsg.),

eines Konzepts „regulierter Selbstregulierung“ gesetzt.⁵³ Für das Internet sind namentlich von *Lawrence Lessig* in den Vereinigten Staaten von Amerika verschiedene Einflussfaktoren pointiert herausgearbeitet worden.⁵⁴ Steuerungsfunktionen entfalten nicht nur das (positive) Recht („*Law*“), sondern auch gesellschaftliche Normen („*Norms*“), die Kräfte des Marktes („*Market*“) sowie schließlich die „Architektur“ des Internets („*Architecture*“). Diese Einflussfaktoren wirken auf das Internet ein, Normen, der Markt und die Architektur des Netzes sind zudem ihrerseits wieder durch das Recht beeinflussbar. Das Vertrauen der Rechtsunterworfenen in die Eignung von Rechtsnormen zur Regulierung der modernen Informationsgesellschaft schwindet zwar gleichwohl; zugleich wird aber der gewährleistende Charakter namentlich der Grundrechte in den Vordergrund gestellt und eingefordert.

Der Ruf nach einem Rückbau einfachgesetzlicher Regularien im informations- und kommunikationstechnischen Bereich hat dabei mehrere Ursachen. Die Bewältigung des wissenschaftlichen und technischen Fortschritts durch das (Verwaltungs-)Recht gilt als genuin staatliche Aufgabe.⁵⁵ Die These einer weitgehenden (faktischen) Rechtsfreiheit der technischen Entwicklung, der der Staat „ihren Lauf lässt“⁵⁶ oder gar lassen muss, ist nach heutigem Verständnis objektiver Staatsaufgaben und grundrechtlicher Schutzpflichten nicht haltbar. Vom grundgesetzlich konstituierten „Präventionsstaat“⁵⁷ wird die Übernahme einer Verantwortung für die Folgen wissenschaftlichen und technischen Fortschritts verlangt.⁵⁸ Das Recht als Steuerungsmittel technischer Entwicklungen

Handbuch des Staatsrechts der Bundesrepublik Deutschland, Bd. IV, 3. Aufl. 2006, § 91 Rdnr. 9.

⁵³ S. etwa *W. Hoffmann-Riem*, AÖR Bd. 123 (1999), S. 531 (537 ff.); *K.-H. Ladeur*, ZUM 1997, 372 ff.; *R. Uerpmann-Witzack*, AVR Bd. 47 (2009), S. 261 (280 f.); eingehend *E. Billmeier*, Die Düsseldorf-Sperrungsverfügung. Ein Beispiel für verfassungs- und gefahrenabwehrrechtliche Probleme der Inhaltsregulierung in der Informationsgesellschaft, 2006, S. 67 ff.; *Z. Talidou*, Regulierte Selbstregulierung im Bereich des Datenschutzes, 2005; *A. C. Thoma*, Regulierte Selbstregulierung im Ordnungsverwaltungsrecht, 2008; ferner *T. A. Deegen*, Freiwillige Selbstkontrolle der Access-Provider, 2007.

⁵⁴ *L. Lessig*, Code and Other Laws of Cyberspace, 1999 (dt.: Code und andere Gesetze des Cyberspace, 2001, übers. v. *M. Bischoff*).

⁵⁵ *D. Murswiek*, Die staatliche Verantwortung für die Risiken der Technik, 1985; *J. Ipsen*, VVDStRL Bd. 48 (1990), S. 177 (179); *P. Kirchhof*, NVwZ 1988, 97 ff. – Eine spezifisch umweltbezogene Technologiebewältigung fordert die Staatszielbestimmung in Art. 20 a GG; dazu vgl. etwa *D. Murswiek*, NVwZ 1996, 222 ff.; *R. Steinberg*, NJW 1996, 1985 ff., insb. 1990 ff.; *R. Pitschas*, in: *M. Kloepfer* (Hrsg.), Technikentwicklung und Technikrechtsentwicklung, 2000, S. 73 (82 ff.), leitet die Aufgabe der Technologiebewältigung aus dem Sozialstaatsprinzip her.

⁵⁶ So aber etwa noch *E. Forsthoff*, Der Staat Bd. 9 (1970), S. 145 (151 ff.); dagegen *J. Ipsen*, VVDStRL Bd. 48 (1990), S. 177 (179).

⁵⁷ Eingehend dazu *E. Denninger*, KritJ 1988, S. 1 ff.; *D. Grimm*, KritV 1986, S. 38 ff.; *J. Ipsen*, VVDStRL Bd. 48 (1990), S. 177 (179).

⁵⁸ Aus historischer Sicht *J. Ipsen*, VVDStRL Bd. 48 (1990), S. 177 (178 mit Fn. 5); *R. Grauert*, in: *Festschrift f. J. Broermann*, 1982, S. 457 (478 f.); *R. Wolf*, Der Stand der Technik,