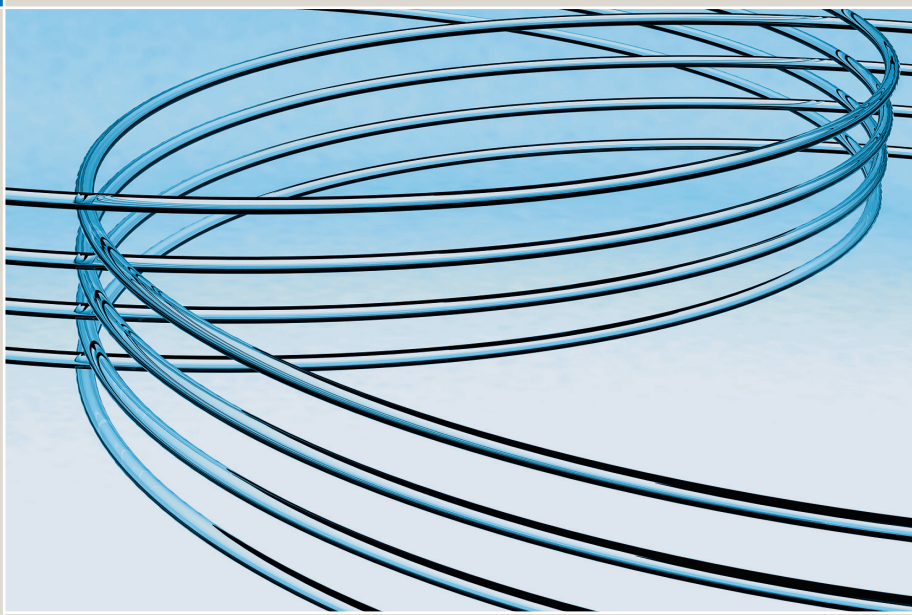
17

HSIEH

Schriften zum Recht der Inneren Sicherheit



E-Mail-Überwachung zur Gefahrenabwehr

BOORBERG

E-Mail-Überwachung zur Gefahrenabwehr

Präventiv-polizeilicher Zugriff auf Internet-basierte Telekommunikation als neue polizeirechtliche Problematik im Digitalzeitalter am Beispiel der E-Mail-Überwachung zur Gefahrenabwehr

von
Dr. Shuo-Chun Hsieh

RICHARD BOORBERG VERLAG
STUTTGART • MÜNCHEN
HANNOVER • BERLIN • WEIMAR • DRESDEN

Bibliografische Information der Deutschen Nationalbibliothek

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

ISBN 978-3-415-04627-6 E - ISBN 978-3-415-05051-8

Scharrstraße 2
70563 Stuttgart
www.boorberg.de

Satz: Thomas Schäfer, www.schaefer-buchsatz.de
Druck und Verarbeitung: e. kurz + co druck und medientechnik gmbh, Kernerstraße 5, 70182 Stuttgart

Vorwort

Die vorliegende Arbeit wurde im Wintersemester 2009/2010 von der Juristischen Fakultät der Albert-Ludwigs-Universität Freiburg im Breisgau als Dissertation angenommen. Gesetze, Rechtsprechung und Schrifttum befinden sich im Wesentlichen auf dem Stand vom Dezember 2009. Das Urteil zur Vorratsdatenspeicherung, das das Bundesverfassungsgericht am 2. 3. 2010 verkündete, wird auch berücksichtigt. Die Abkürzungen der in dieser Arbeit zitierten Polizei- und Ordnungsgesetze folgen dem Abkürzungsverzeichnis in *Bodo Pieroth/Bernhard Schlink/Michael Kniesel*, Polizei- und Ordnungsrecht, 5. Aufl., 2008. Hinsichtlich der übrigen Abkürzungen wird verwiesen auf *Hildebert Kirchner*, Abkürzungsverzeichnis der Rechtssprache, 6. Aufl., 2008.

Mein herzlicher Dank gilt Herrn Professor Dr. Friedrich Schoch, der diese Arbeit mit viel Geduld betreut hat. Er hat mir großen Freiraum bei der Auswahl des Themas und der Bearbeitung der Dissertation gelassen. Für die zügige Erstellung des Zweitgutachtens danke ich Herrn Professor Dr. Thomas Würtenberger. Herrn Prof. Dr. Dirk Heckmann und Herrn Prof. Dr. Thomas Würtenberger bin ich für die freundliche Aufnahme dieser Arbeit in die von ihnen herausgegebene Reihe der Schriften zum Recht der Inneren Sicherheit großen Dank schuldig. Bei Frau Dr. Stefanie Mutschler bedanke ich mich herzlich für das mühevolle Korrekturlesen des Manuskripts. Dank gebührt auch meinen Freunden, die zur Fertigstellung dieser Arbeit beigetragen haben.

Mein größter Dank gilt schließlich meinen lieben Eltern. Ohne ihre dauerhafte Unterstützung und unendliche Liebe hätte ich nur schwer in Deutschland promovieren können. Ihnen ist dieses Buch gewidmet.

Kaohsiung, Taiwan, im Juni 2010 *Shuo-Chun Hsieh*

Inhaltsübersicht

Inhaltsverzeichnis

1. Kapitel: Einleitung

A. Ausgangslage

I. Präventiv-polizeiliche E-Mail-Überwachung als Gegenstand der Untersuchung

Seit einigen Jahren entwickelt sich die Gefahrenabwehr in der virtuellen Welt, die durch den Computer und das Internet gebildet wird, zu einem aktuellen Thema des Polizeirechts, weil das Internet wegen bestehender Missbrauchsmöglichkeiten einen Gefahrenträger darstellt[1] und damit als ein neues Zuständigkeitsfeld der Polizei im Digitalzeitalter angesehen wird[2]. In Bezug auf die technisch denkbaren Möglichkeiten der Gefahrenabwehr im Internet[3] ist die präventiv-polizeiliche Überwachung der Internet-basierten Telekommunikation besonders beachtenswert, wenn man berücksichtigt, dass zahlreiche „gefährliche" Informationen (z. B. extremistische oder terroristische Nachrichten) durch verschiedene Formen der Kommunikation, die auf Internet-Technik basierten, heimlich übermittelt und ausgetauscht werden. Da sich der E-Mail-Verkehr zur häufigsten und wichtigsten Internet-basierten Telekommunikation[4] entwickelt[5], wird erwartet, dass die Beobachtung der E-Mail-Kommunikation eine effektive Maßnahme zur Gefahrenabwehr darstellt. Vor allem ist rechtlich nicht zu übersehen, dass die telekommunikationsrechtlichen Vorschriften die Möglichkeit der technischen Vorbereitung für die präventiv-polizeiliche E-Mail-Überwachung bereits geschaffen haben und Regelungen der präventiv-polizeilichen Telekommunikationsüberwachung schon in die Polizei- und Ordnungsgesetze der meisten Bundesländer eingefügt wurden. Die damit aufgeworfenen Rechtsfragen der präventiv-polizeilichen E-Mail-Überwachung erscheinen diskussionswürdig.

Unter der präventiv-polizeilichen E-Mail-Überwachung, die den Forschungsgegenstand dieser Arbeit darstellt, versteht man eine zur Gefahrenabwehr durchgeführte verdeckte polizeiliche Informationserhebung durch die Überwachung der E-Mail-Kommunikation. Davon zu unterscheiden ist

1 Zum Gefährdungspotenzial im Internet *Würtenberger/Heckmann*, PolR BW, Rn. 544.
2 Dazu siehe 2. Kapitel A II.
3 Dazu siehe 2. Kapitel C I.
4 Der E-Mail-Verkehr stellt eine Form der Telekommunikation dar. Dazu 2. Kapitel B I.
5 *Determann*, Kommunikationsfreiheit, S. 45 ff.; *Dürscheid*, in: Ziegler/Dürscheid, Kommunikationsform E-Mail, S. 93 (101); *Greiner*, Verhinderung verbotener Internetinhalte, S. 15 f.; *Kleine-Voßbeck*, Electronic Mail, S. 12; *Petri*, in: Lisken/Denninger, HPolR, H Rn. 343.

die repressive E-Mail-Überwachung nach § 100a StPO[6], weil die repressive E-Mail-Überwachung nicht die Gefahrenabwehr, sondern die Strafverfolgung betrifft. Zu betonen ist ferner, dass nicht jeder präventiv-polizeiliche Zugriff auf E-Mail-Inhalte dem Begriff der E-Mail-Überwachung entspricht. Ein präventiv-polizeiliches Mitlesen der bereits abgerufenen E-Mails durch den verdeckten Zugriff auf Computer der Zielpersonen (Online-Durchsuchung) ist keine präventiv-polizeiliche E-Mail-Überwachung, weil es dabei nicht um die Überwachung einer laufenden E-Mail-Kommunikation geht. Schließlich gehören die Verarbeitung und die Verwendung der durch die präventiv-polizeiliche E-Mail-Überwachung gewonnenen Daten nicht zum Erörterungsbereich dieser Arbeit. Denn sie erstrecken sich nicht auf die polizeiliche Informationserhebung, sondern auf polizeiliche Maßnahmen, die nach dem Abschluss der Informationserhebung durchgeführt werden.

II. Telekommunikationsrechtliche Vorkehrungen für die Umsetzung der Telekommunikationsüberwachung

Die rechtliche Möglichkeit der technischen Vorkehrung für die Umsetzung der E-Mail-Überwachung in Deutschland wird durch telekommunikationsrechtliche Vorschriften bestimmt. Mit der Telekommunikations-Überwachungsordnung (TKÜV) vom 22. 1. 2002[7] wurde erstmals festgelegt, dass E-Mail-Nachrichten überwacht werden können[8]. Die Betreiber von E-Mail-Servern (E-Mail-Provider) haben nach der TKÜV 2002 die Technik zur E-Mail-Überwachung (Überwachungseinrichtungen) vorzuhalten[9]. Diese in der TKÜV 2002 vorgesehene Vorhaltepflicht wurde in § 110 Telekommunikationsgesetz (TKG) vom 22. 6. 2004[10] übernommen. Nach § 110 Abs. 1 S. 1 TKG sind E-Mail-Provider, die den Betreibern von Telekommunikationsanlagen entsprechen[11], verpflichtet, auf eigene Kosten technische Einrichtungen zur Umsetzung einer E-Mail-Überwachung vorzuhalten[12]. Die Verpflichtung und ihre Ausnahmen werden durch die neue TKÜV vom

6 Zur strafprozessualen E-Mail-Überwachung nach § 100a StPO *Meininghaus*, Zugriff auf E-Mails, S. 77 ff.; *Nack*, in: Hannich, StPO, § 100a Rn. 19 ff.; *Störing*, Strafprozessuale Zugriffsmöglichkeiten, S. 121 ff.

7 BGBl. 2002 I, S. 458.

8 *Bock*, in: Geppert/Piepenbrock/Schütz/Schuster, TKG, § 110 Rn. 92.

9 *Bock* (Fn. 8), § 110 Rn. 92.

10 BGBl. 2004, S. 1190.

11 Die E-Mail-Provider fallen in den Adressatenkreis des § 110 Abs. 1 S. 1 TKG, weil sie durch ihre Server und Router, die dem Begriff der Telekommunikationsanlage (§ 3 Nr. 23 TKG) entsprechen, E-Mail-Übertragungsdienste, die sich als Telekommunikationsdienste (§ 3 Nr. 24 TKG) ansehen lassen, für die Öffentlichkeit anbieten (*Säcker*, in: Säcker, TKG, § 3 Rn. 73; *Fetzer*, in: Arndt/Fetzer/Scherer, TKG, § 3 Rn. 86).

12 Zur Verfassungsmäßigkeit des § 110 TKG *Klesczewski*, in: Säcker, TKG, § 110 Rn. 21 ff.

3. 11. 2005[13], die ihre gesetzliche Ermächtigungsgrundlage in § 110 Abs. 2 TKG findet[14], näher konkretisiert[15]. Gemäß § 3 Abs. 2 Nr. 5 TKÜV können sich Betreiber von Telekommunikationsanlagen, an die nicht mehr als 10000 Teilnehmer[16] oder sonstige Nutzungsberechtigte angeschlossen sind, von dieser Verpflichtung befreien.

Die Vorkehrung für die Umsetzung der E-Mail-Überwachung erschöpft sich nicht darin. Durch das Gesetz zur Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen sowie zur Umsetzung der Richtlinie 2006/24/EG[17], das zur Umsetzung der Richtlinie über die Vorratsdatenspeicherung 2006/24/EG[18] in nationales Recht umgesetzt wurde und am 1. 1. 2008 in Kraft getreten ist[19], weitet sich die Verpflichtung der E-Mail-Provider aus. Gemäß § 113a Abs. 1 und 3 TKG (= Art. 2 des Gesetzes zur Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen sowie zur Umsetzung der Richtlinie 2006/24/EG) werden Anbieter der E-Mail-Dienste verpflichtet, sechs Monate die von ihnen verarbeiteten Verkehrsdaten der E-Mail-Kommunikation (E-Mail-Adresse und IP-Adresse[20] sowie die Zeitpunkte der Nutzung von E-Mail-Diensten) zu speichern (sog. Vorratsdatenspeicherung)[21]. Da die nach § 113a TKG gespeicherten Daten für bestimmte Zwecke an die zuständigen Stellen übermittelt werden dürfen (§ 113b TKG[22]), können die zuständigen Stellen diese Daten verwenden, um eine weitere Überwachung der E-Mail-Kommunikation durchzuführen. Insoweit lässt sich die Vorratsdatenspeicherung (§ 113a TKG) ebenfalls als eine Vorkehrung für die Umsetzung der E-Mail-Überwachung ansehen[23]. Allerdings

13 BGBl. 2005, S. 3136.

14 *Kühling/Elbracht*, Telekommunikationsrecht, 2008, Rn. 424.

15 *Eckhardt*, in: Heun, Handbuch Telekommunikationsrecht, B Rn. 140 ff.

16 Nach der Legaldefinition in § 3 Nr. 20 TKG ist „Teilnehmer" jede natürliche oder juristische Person, die mit einem Anbieter von Telekommunikationsdiensten einen Vertrag über die Erbringung derartiger Dienste geschlossen hat.

17 BGBl. 2007, S. 3198.

18 RL 2006/24/EG v. 15. 3. 2006, ABl. EG Nr. L 105 v. 13. 4. 2006, S. 54 ff.

19 Vgl. dazu *Bär*, MMR 2008, S. 215 ff.; *Fahr*, DStR 2008, S. 375 ff.; *Puschke/Singelnstein*, NJW 2008, S. 113 ff.

20 Die Speicherung der lokalen IP-Adresse ist auch sinnvoll für die Überwachung der durch das W-LAN-System übermittelten E-Mail, da man mit der IP-Adresse ermitteln kann, welche Nutzer zu einem bestimmten Zeitpunkt im W-LAN angemeldet waren. Dadurch kann der Kreis der später näher zu Überwachenden eingegrenzt werden (vgl. *Hornung*, MMR 2007 Heft 12, S. XIII; a. A. *Gietl*, MMR 2007, S. 630 (633)).

21 *Bär*, MMR 2008, S. 307 f.; *Graulich*, NVwZ 2008, S. 485 ff.

22 § 113b TKG ist ebenfalls durch das am 1. 1. 2008 in Kraft getretene „Gesetz zur Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen sowie zur Umsetzung der Richtlinie 2006/24/EG" im Telekommunikationsgesetz eingefügt worden.

23 Durch sein Urteil vom 10. 2. 2009 erklärte der Europäische Gerichtshof (EuGH), dass die RL 2006/24/EG zu Recht auf der Grundlage des EG-Vertrags erlassen wurde (EuGH, Urteil vom

erklärte das Bundesverfassungsgericht §§ 113a und 113b TKG für nichtig, weil sie gegen Art. 10 Abs. 1 GG (Fernmeldegeheimnis) verstoßen[24].

Zu beachten ist, dass die Regelungen über die Vorkehrung für die Umsetzung der E-Mail-Überwachung nicht mit den gesetzlichen Ermächtigungsvorschriften zur E-Mail-Überwachung gleichgesetzt werden können. § 110 TKG regelt nur die technischen und organisatorischen Vorkehrungen für die Umsetzung von Überwachungsmaßnahmen. Da § 110 TKG über Vorkehrungen für die Umsetzung von Überwachungsmaßnahmen hinaus keine Befugnis zum Zugriff auf die E-Mail-Kommunikation schafft, stellt er selbst keine Ermächtigungsgrundlage der E-Mail-Überwachung dar[25]. Vielmehr begründet er nur eine verwaltungsrechtliche Pflicht der Anbieter der E-Mail-Dienste. In diesem Zusammenhang ist festzuhalten, dass telekommunikationsrechtliche Vorschriften (TKG, TKÜV) die technische Vorbereitung für den Zugriff auf den E-Mail-Verkehr ermöglichen. Sie ermächtigen den Staat jedoch nicht, die E-Mail-Kommunikation zu überwachen.

III. Einfügung der Ermächtigungsvorschriften zur Telekommunikationsüberwachung in Polizei- und Ordnungsgesetze

Ob die E-Mail-Überwachung zulässig ist, hängt davon ab, ob eine gesetzliche Vorschrift, in der die Informationserhebung durch den Zugriff auf die E-Mail-Kommunikation seine Rechtsgrundlage finden kann, vorliegt. Zwar sind TKG und TKÜV selbst keine Ermächtigungsgrundlagen zur E-Mail-Überwachung, jedoch zeigen sie, in welchem Bereich und nach welchen gesetzlichen Vorschriften die Telekommunikationsüberwachung, die den Oberbegriff zur E-Mail-Überwachung darstellt, gegenwärtig in Deutschland vorgesehen ist. Aus § 110 Abs. 1 Satz 6 TKG und § 1 Nr. 1 TKÜV ist zu entnehmen, dass die Telekommunikationsüberwachung derzeit ihre Rechtsgrundlagen in §§ 100a und 100b der Strafprozessordnung, §§ 3, 5 und 8 des Artikel 10-Gesetzes, §§ 23a bis 23c und 23e des Zollfahndungsdienstgesetzes, im § 20 l des Bundeskriminalamtgesetzes sowie im Landesrecht finden kann. Da das hier genannte Landesrecht als das Polizeirecht verstanden wird[26], kann eine präventiv-polizeiliche E-Mail-Überwachung durch-

10. 2. 2009 – Rs. C-301/06, MMR 2009, S. 244 ff.). Die Frage, ob die RL 2006/24/EG zur Verletzung der Grundrechte führt, hat der EuGH nicht behandelt (dazu *Terhechte*, EuZW 2009, S. 199 (201 f.)).

24 BVerfG, 1 BvR 256/08 vom 2. 3. 2010, Rn. 183 ff., http://www.bverfg.de/entscheidungen/rs20100302_1bvr025608.html.

25 *Bock* (Fn. 8), § 110 Rn. 1; *Eckhardt* (Fn. 15), B Rn. 100; *Klesczewski* (Fn. 12), § 110 Rn. 4; *Löwnau*, in: Scheurle/Mayen, TKG, § 110 Rn. 1.

26 Vgl. *Bock* (Fn. 8), § 110 Rn. 53 ff.; *Eckhardt* (Fn. 15), B Rn. 100; *Klesczewski* (Fn. 12), § 110 Rn. 20. Insoweit stellen die polizei- und ordnungsgesetzlichen Vorschriften zur Telekom-

geführt werden, soweit polizei- und ordnungsgesetzliche Vorschriften der Polizei eine solche Befugnis einräumen.

Ursprünglich war die Telekommunikationsüberwachung den Polizei- und Ordnungsgesetzen fremd[27]. Zurzeit bestehen allerdings in den meisten Bundesländern ausdrückliche Ermächtigungsvorschriften zur präventiv-polizeilichen Telekommunikationsüberwachung: In Baden-Württemberg[28], Bayern[29], Brandenburg[30], Hamburg[31], Hessen[32], Mecklenburg-Vorpommern[33], Niedersachsen[34], Rheinland-Pfalz[35], Saarland[36], Schleswig-Holstein[37] und Thüringen[38] wurden Regelungen über den Zugriff auf Telekommunikationsdaten in die Polizei- und Ordnungsgesetze eingefügt. Diese eröffnen die rechtliche Möglichkeit der Informationserhebung durch den Zugriff auf den E-Mail-Verkehr. Die mit diesen neuen Befugnisnormen verbundenen Rechtsprobleme sind Gegenstand dieser Arbeit.

IV. Problemstellung

1. Verfassungsrechtliche Problematik

Ausgangspunkt für die folgenden Diskussionen ist, dass die präventiv-polizeiliche E-Mail-Überwachung stark in Grundrechte eingreift. Die Intensität des Eingriffs ergibt sich daraus, dass der präventiv-polizeiliche Zugriff auf die E-Mail-Kommunikation eine verdeckte Informationserhebung ohne Wissen des Betroffenen darstellt. Auf der verfassungsrechtlichen Ebene ist zunächst die Frage aufgeworfen, in welches Grundrecht durch die präventiv-polizeiliche E-Mail-Überwachung eingegriffen wird. Da der E-Mail-Verkehr eine Telekommunikation ist, kommt zunächst das Fernmeldegeheimnis (Art. 10 Abs. 1 GG) in Betracht. Allerdings ist die Frage nach dem Grundrechtsschutz der E-Mail-Kommunikation komplizierter. Die Besonderheit der E-Mail-Kommunikation ist, dass sich die Übermittlung einer E-Mail technisch in drei Phasen aufteilen lässt[39]. Unklar ist, ob der Vorgang der E-Mail-Kommunikation unterbrochen ist und damit nicht durch das

munikationsüberwachung neben den Gesetzen über die Dienste und der StPO die dritte Säule der Telekommunikationsüberwachung dar (vgl. *Saurer*, NVwZ 2005, S. 275 (276 f.)).

27 *Petri* (Fn. 5), H Rn. 305; *W.-R. Schenke*, PolR, Rn. 197a.

28 § 23a bwPolG.

29 Art. 34a-34c bayPAG.

30 § 33b bbgPolG.

31 §§ 10a-10d hambGDatPol.

32 § 15a hessSOG.

33 § 34a mvSOG.

34 § 33a ndsSOG.

35 § 31 rpPOG.

36 § 28b saarlPolG.

37 § 185a shLVwG.

38 § 34a thürPAG.

39 Dazu siehe 4. Kapitel A I 3 c).

Fernmeldegeheimnis geschützt ist, wenn die abgeschickte E-Mail in der Mailbox des Empfängers „ruht" und noch nicht vom Empfänger abgerufen wird (2. Phase der E-Mail-Übertragung). In der Konstellation, dass die Polizei durch den Mail-Filter die im Mailserver ruhende und noch nicht abgerufene E-Mail abfängt, ist diese Frage besonders bedeutsam. Neben dem Fernmeldegeheimnis könnte die präventiv-polizeiliche E-Mail-Überwachung in andere Grundrechte der betroffenen Nutzer der E-Mail-Dienste eingreifen. An diesem Punkt ist vor allem zu diskutieren, ob auch das Recht auf informationelle Selbstbestimmung und das durch das Urteil des Bundesverfassungsgerichts vom 27. 2. 2008[40] neu entwickelte „Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme" (sog. „Computergrundrecht"[41]) durch den präventiv-polizeilichen Zugriff auf die E-Mail-Kommunikation beeinträchtigt werden. Zu betonen ist, dass die zu beantwortende Frage nach den betroffenen Grundrechten nicht allein die Grundrechte der Telekommunikationsteilnehmer betrifft. Berücksichtigt man, dass die polizei- und ordnungsrechtlichen Ermächtigungsvorschriften zur Telekommunikationsüberwachung Mitwirkungspflichten der Dienstanbieter regeln[42], führt diese Indienstnahme auch zu einem Eingriff in die Berufs(ausübungs)freiheit der E-Mail-Provider.

Wie oben bereits ausgeführt wurde, findet die präventiv-polizeiliche Telekommunikationsüberwachung derzeit nur in wenigen Bundesländern noch keine ausdrückliche gesetzliche Ermächtigungsgrundlage. Unter dem Aspekt des Gesetzesvorbehalts ist fraglich, ob sich die Polizei in diesen Bundesländern auf die polizei- und ordnungsgesetzlichen Vorschriften über den verdeckten Einsatz technischer Mittel bzw. über die Datenerhebung in oder aus Wohnungen[43] als Rechtsgrundlagen für präventiv-polizeiliche E-Mail-Überwachung stützen kann. Außerdem wird in der strafprozessualen Literatur teilweise vertreten, dass § 94 StPO (Beschlagnahme) die Rechtsgrundlage des Zugriffs auf E-Mails, die in der Mailbox des Empfängers ruhen und noch nicht abgerufen wurden, darstellt[44]. Da alle Polizei- und Ordnungsgesetze Regelungen zur Durchsuchung von Sachen und zur Beschlagnahme enthalten[45], stellt sich die Frage, ob diese in der strafprozessualen Literatur teilweise vertretene Auffassung überzeugend ist und

40 BVerfGE 120, 274 ff.

41 So wörtlich *Hufen*, Grundrechte, § 12 Rn. 5; *J. Ipsen*, Grundrechte, Rn. 325a; *Künast*, NJW 2009, S. 1723 (1724); *Kutscha*, LKV 2008, S. 481 (484); *Manssen*, Grundrechte, Rn. 225.

42 § 23a Abs. 5 bwPolG; Art. 34b bayPAG; § 33b Abs. 6 bbgPolG; § 10a Abs. 3 hambGDatPol; § 15a Abs. 1, Abs. 2 hessSOG; § 34a Abs. 6 mvSOG; § 33a Abs. 7 ndsSOG; § 31 Abs. 6 rpPOG; § 28b Abs. 2 saarlPolG; § 185a Abs. 4 shLVwG; § 34a Abs. 1 thürPAG.

43 § 25 Abs. 1 S. 1 Nr. 2 berlASOG; § 33 bremPolG; § 17 nwPolG; § 39 sächsPolG; § 17 saSOG.

44 So *Bär*, MMR 2000, S. 472 (474 f.); *Nack* (Fn. 6), § 100a Rn. 22.

45 Nachweise bei *Schenke* (Fn. 27), Rn. 151 mit Fn. 356, Rn. 158 mit Fn. 382.

die polizei- und ordnungsgesetzlichen Ermächtigungsvorschriften zur Durchsuchung von Sachen und zur Beschlagnahme bei der Prüfung der Rechtsgrundlage die präventiv-polizeiliche E-Mail-Überwachung rechtfertigen können. Falls dies abzulehnen ist, ist zu fragen: Kann die Generalklausel der Informationserhebung in Polizei- und Ordnungsgesetzen[46] oder die polizeirechtliche Generalklausel, die die allgemeine Ermächtigung der notwendigen Maßnahmen zur Gefahrenabwehr darstellt[47], aufgrund ihrer Subsidiarität und Auffangwirkung[48] als die Ermächtigungsgrundlage für die präventiv-polizeiliche E-Mail-Überwachung betrachtet werden?

Auch die in Polizei- und Ordnungsgesetzen der meisten Bundesländer neu eingefügten Regelungen über die Telekommunikationsüberwachung, in denen die präventiv-polizeiliche E-Mail-Überwachung eine Ermächtigungsgrundlage finden kann, führen selbst zu heftigen verfassungsrechtlichen Debatten um deren verfassungsrechtliche Zulässigkeit. Hinsichtlich der formellen Verfassungsmäßigkeit ist zu prüfen, ob der Landesgesetzgeber hierzu die Kompetenz hatte. Diese Frage nach der Gesetzgebungskompetenz ist von Bedeutung, wenn das Ziel der polizei- und ordnungsgesetzlichen Vorschriften, nach denen die Polizei eine präventive E-Mail-Überwachung durchführen kann, nicht nur die klassische Gefahrenabwehr, sondern auch die vorbeugende Bekämpfung von Straftaten betrifft. Gemäß § 33a Abs. 1 Nr. 2 und 3 ndsSOG a. F. durften personenbezogene Daten zum Zweck der sog. Strafverfolgungsvorsorge durch eine Telekommunikationsüberwachung erhoben werden. Diese Vorschrift wurde allerdings vom Bundesverfassungsgericht durch seine Entscheidung vom 27. 7. 2005[49] für nichtig erklärt, da die Strafverfolgungsvorsorge gegenständlich den Bereich des Strafverfahrens (Art. 74 Abs. 1 Nr. 1 GG), in dem der Bundesgesetzgeber bereits durch §§ 100a ff. StPO die Überwachung der Telekommunikation umfassend geregelt habe, betreffe[50]. In diesem Zusammenhang sind die Länder nicht befugt, „die Polizei zur Telekommunikationsüberwachung zum Zwecke der Vorsorge für die Verfolgung von Straftaten zu ermächtigen“[51]. Zwar wird § 33a Abs. 1 Nr. 2 und 3 ndsSOG a. F. wegen der Unvereinbarkeit mit Art. 74 Abs. 1 Nr. 1 GG durch das oben genannte Urteil des Bundesverfassungsgerichts als verfassungswidrig angesehen, jedoch kann wohl eine ähnliche Zielsetzung der Telekommunikationsüberwachung nach wie vor in anderen Ländern vorgefunden werden. In Baden-Württem-

46 Nachweise bei *Schenke* (Fn. 27), Rn. 181 mit Fn. 444.
47 Nachweise bei *Pieroth/Schlink/Kniesel*, PolR, § 7 Rn. 1 mit Fn. 1.
48 *Pieroth/Schlink/Kniesel* (Fn. 47), § 7 Rn. 11 f.
49 BVerfGE 113, 348 ff.
50 BVerfGE 113, 348 (367 ff.).
51 BVerfGE 113, 348 (Leitsatz 2).

berg[52], Bayern[53], Brandenburg[54], Saarland[55] und Thüringen[56] kann sich die präventiv-polizeiliche Telekommunikationsüberwachung zur vorbeugenden Bekämpfung von Straftaten bzw. zur Verhütung von Straftaten gegen potenzielle Straftäter richten. Insoweit knüpft die präventiv-polizeiliche Telekommunikationsüberwachung in diesen fünf Bundesländern (auch) an zukünftig mögliche Begehungen der Straftaten an. Hierbei stellt sich die Frage, ob die polizei- und ordnungsgesetzlichen Vorschriften, nach denen die Polizei eine Telekommunikationsüberwachung zur Bekämpfung von Straftaten bzw. zur Verhütung von Straftaten durchführen kann, die Grenze zur Strafverfolgung überschreiten. Über die formelle Verfassungsmäßigkeit hinaus ist die Frage aufgeworfen, ob die polizei- und ordnungsgesetzlichen Ermächtigungsvorschriften zur Telekommunikationsüberwachung, die eine etwaige Rechtsgrundlage des präventiv-polizeilichen Zugriffs auf den E-Mail-Verkehr darstellen, materiell mit dem Grundgesetz vereinbar sind. Hinsichtlich der materiellen Verfassungsmäßigkeit ist vor allem zu prüfen, ob diese polizei- und ordnungsgesetzlichen Ermächtigungsvorschriften zur Telekommunikationsüberwachung hinreichend bestimmt sind oder eine verfassungsrechtlich unzulässige Blankettermächtigung schaffen.

2. Verwaltungsrechtliche Problematik

Wie oben bereits ausgeführt wurde, liegt der Ausgangspunkt für die Diskussion dieser Arbeit darin, dass der präventiv-polizeiliche Zugriff auf die E-Mail-Kommunikation zu einem intensiven Grundrechtseingriff führt. Diese schwere Beeinträchtigung der Grundrechte ergibt sich nicht nur aus den abstrakt-generellen polizei- und ordnungsgesetzlichen Regelungen über die Telekommunikationsüberwachung. Vielmehr wird in das Grundrecht auch stark eingegriffen, wenn die Polizei aufgrund dieser Ermächtigungsvorschriften konkrete Maßnahmen zur Überwachung eines E-Mail-Verkehrs ergreift. Aus diesem Grund ist die verwaltungsrechtliche Problematik der Durchführung einer präventiv-polizeilichen E-Mail-Überwachung nicht zu übersehen.

Auf der verwaltungsrechtlichen Ebene stellen die Rechtsverhältnisse zwischen der überwachenden Polizeibehörde, den betroffenen Nutzern der E-Mail-Dienste und den E-Mail-Providern, die bei der Durchführung einer präventiv-polizeilichen E-Mail-Überwachung mithelfen müssen, die zu klärenden zentralen Rechtsfragen dar. In Bezug auf das Rechtsverhältnis zwischen der überwachenden Polizeibehörde und den betroffenen Nutzern

52 § 23a Abs. 1 S. 1 Nr. 2 bwPolG.
53 Art. 34a Abs. 1 S. 1 Nr. 2 bayPAG.
54 § 33b Abs. 1 in Verbindung mit § 33a Abs. 1 bbgPolG.
55 § 28b Abs. 1 S. 1 Nr. 2 saarlPolG.
56 § 34a Abs. 3 S. 1 Nr. 2 thürPAG.

der E-Mail-Dienste ist festzuhalten, dass dieses Rechtsverhältnis, das durch die Maßnahme präventiv-polizeilicher E-Mail-Überwachung begründet wird, ein Verwaltungsrechtsverhältnis ist. Umstritten ist jedoch die Rechtsnatur der Maßnahme präventiv-polizeilicher E-Mail-Überwachung. Ob diese heimliche polizeiliche Maßnahme der Informationserhebung als Verwaltungsakt oder Realakt einzustufen ist, ist zu klären. Ferner wird die Frage nach der Rechtsposition der betroffenen Nutzer der E-Mail-Dienste aufgeworfen. Dabei geht es um die polizeirechtliche Verantwortlichkeit der betroffenen Nutzer der E-Mail-Dienste. In einigen polizei- und ordnungsgesetzlichen Ermächtigungsvorschriften zur Telekommunikationsüberwachung fallen die potenziellen Straftäter und die Kontakt- und Begleitpersonen in den Kreis der Zielpersonen[57]. Die Frage, ob sie dem Begriff des Störers im Sinne des Polizeirechts entsprechen, ist von großer Wichtigkeit. Denn die Polizei kann nur im Falle eines polizeilichen Notstands mit Maßnahmen präventiv-polizeilicher E-Mail-Überwachung gegen Nichtstörer vorgehen. Auch die Nichtzielpersonen können durch die Durchführung präventiv-polizeilicher E-Mail-Überwachung betroffen sein. Dies ist der Fall, wenn eine unbeteiligte Person Partner der E-Mail-Kommunikation einer Zielperson ist oder wenn die E-Mail einer unbeteiligten Person über den kontrollierten E-Mail-Knoten, in dem die Polizeibehörde ein Überwachungsprogramm einsetzt, übermittelt wird. Da die E-Mails dieser unbeteiligten mitbetroffenen Personen auch durch den im kontrollierten E-Mail-Knoten eingesetzten E-Mail-Filter überprüft werden und damit ein Verwaltungsrechtsverhältnis begründet wird, stellt sich die Frage, ob in dieser Situation nichtverantwortliche Dritte in Anspruch genommen werden. Berücksichtigt man, dass die präventiv-polizeiliche E-Mail-Überwachung eine verdeckte Informationserhebung ohne Wissen des Betroffenen darstellt, ist nicht zu leugnen, dass das Rechtsverhältnis zwischen der überwachenden Polizeibehörde und den betroffenen Nutzern der E-Mail-Dienste asymmetrisch ist. Aufgrund der Heimlichkeit des Zugriffs auf die E-Mail-Kommunikation ist der Rechtsschutz im laufenden Überwachungsverhältnis faktisch schwierig. In diesem Zusammenhang sieht der Gesetzgeber die Anordnung der Überwachung unter Richtervorbehalt als eine Mindestsicherung im Verfahren, durch die die Willkür der polizeilichen Entscheidung über den Zugriff auf die E-Mail-Kommunikation verhindert werden kann, an[58]. Fraglich ist jedoch, ob der Richtervorbehalt ein probates

57 § 23a Abs. 1 S. 1 Nr. 2 bwPolG; Art. 34a Abs. 1 S. 1 Nr. 2 und 3 bayPAG; § 33b Abs. 1 und Abs. 2 S. 2 in Verbindung mit § 33a Abs. 1 Nr. 2 bbgPolG; § 28b Abs. 1 S. 1 Nr. 2 saarlPolG; § 34a Abs. 3 S. 1 Nr. 2 und 3 thürPAG.

58 § 23a Abs. 3 S. 1 bwPolG; Art. 34c Abs. 1 i. V. m. Art. 34 Abs. 4 S. 1 bayPAG; § 33b Abs. 5 S. 1 bbgPolG; § 10c Abs. 1 S. 1 hambGDatPol; § 15a Abs. 4 S. 1 hessSOG; § 34a Abs. 4 S. 1 i. V. m. § 34 Abs. 3 S. 1 mvSOG; § 33a Abs. 4 S. 1 ndsSOG; § 31 Abs. 5 S. 1 rpPOG; § 28b Abs. 5 S. 1 saarlPolG; § 186 Abs. 1 S. 1 shLVwG; § 34a Abs. 5 S. 1 thürPAG.

Mittel zur Verbesserung der Asymmetrie des Rechtsverhältnisses zwischen der überwachenden Polizeibehörde und betroffenen Nutzern der E-Mail-Dienste ist, da den Zielpersonen bei der vorbeugenden Gerichtskontrolle wegen der Heimlichkeit der Überwachungsmaßnahme kein rechtliches Gehör gewährt wird.

Ist ein E-Mail-Provider verpflichtet, sich im Einzelfall an einer präventiv-polizeilichen E-Mail-Überwachung zu beteiligen, wird ein Verwaltungsrechtsverhältnis zwischen ihm und der überwachenden Polizeibehörde begründet. Es fragt sich, ob sich die generell-abstrakten polizei- und ordnungsgesetzlichen Regelungen über die Mitwirkungspflicht der Diensteanbieter als Entstehungsgrund dieses Verwaltungsrechtsverhältnisses betrachten lassen. Falls diese Frage zu verneinen ist, kommt die konkrete polizeiliche Anordnung in Betracht. Unklar ist jedoch, ob die Polizeibehörde durch Abschluss eines Verwaltungsvertrags mit E-Mail-Providern ein Rechtsverhältnis begründen kann, um einen Zugriff auf die E-Mail-Kommunikation zu ermöglichen. Ferner ist der polizeiliche Anspruch auf die technische Hilfe der E-Mail-Provider problematisch, wenn die Provider ihren Firmensitz nicht im Gebiet des Bundeslandes der überwachenden Polizeibehörde haben. Ob die überwachende Polizeibehörde einen solchen „grenzüberschreitenden" Anspruch erheben kann, ist zu untersuchen. Darüber hinaus wirkt der E-Mail-Provider einerseits an der Wahrnehmung der polizeilichen Aufgabe der Gefahrenabwehr mit. Andererseits ist er Adressat der polizeilichen Anordnung. Zu diskutieren ist die verwaltungsorganisationsrechtliche Rechtsposition und polizeirechtliche Verantwortlichkeit des E-Mail-Providers, der bei der Durchführung einer E-Mail-Überwachung verpflichtet wird.

Da sich die E-Mail-Provider an der Erfüllung polizeilicher Aufgaben der Gefahrenabwehr beteiligen, stellt sich die Frage, ob ein Verwaltungsrechtsverhältnis zwischen den E-Mail-Providern und den betroffenen Nutzern der E-Mail-Dienste vorliegt. Zu klären ist ferner die Frage, ob die E-Mail-Provider für ihre Kunden das Fernmeldegeheimnis des Art. 10 Abs. 1 GG geltend machen und daher die technische Mitwirkung ablehnen können.

Auf der verwaltungsrechtlichen Ebene wird schließlich die Frage nach dem gerichtlichen Rechtsschutz aufgeworfen. Dabei handelt es sich nicht nur um den Rechtsschutz gegen den polizeilichen Zugriff auf die E-Mail-Kommunikation, sondern auch um den Rechtsschutz gegen die polizeiliche Anordnung, nach der die E-Mail-Provider bei der Durchführung präventiv-polizeilicher E-Mail-Überwachung mithelfen müssen. Unter dem Gesichtspunkt der statthaften Klageart weist die Frage nach gerichtlichem Rechtsschutz einen engen Zusammenhang mit der Rechtsnatur des Entstehungsgrundes der oben genannten Verwaltungsrechtsverhältnisse auf.

B. Gang der Untersuchung

Die obigen Rechtsfragen, die sich auf die präventiv-polizeiliche E-Mail-Überwachung beziehen, werden in dieser Arbeit systematisch behandelt.

Zunächst wird im 2. Kapitel die Gefahrenabwehr im Internet, die den Ausgangspunkt des präventiv-polizeilichen Zugriffs auf die E-Mail-Kommunikation darstellt, dargelegt. Zu erörtern ist nicht nur die Frage, warum sich die Gefahrenabwehr im Internet zu einem zentralen Thema des Polizeirechts in der Informationsgesellschaft entwickelt hat, sondern auch die Frage, welche polizeilichen Maßnahmen technisch und rechtlich die Gefahren im Internet abwehren können.

Im 3. Kapitel wird der verfolgte Zweck der in den Polizei- und Ordnungsgesetzen geregelten Telekommunikationsüberwachung untersucht. Der Kern der Diskussion ist die Frage, ob die präventiv-polizeiliche Telekommunikationsüberwachung, die zur vorbeugenden Straftatenbekämpfung im Vorfeld der Gefahr durchgeführt wird, die Grenze zur Strafverfolgung, die die repressive Aufgabe der Polizei darstellt, überschreitet.

Die Frage, in welche Grundrechte durch eine präventiv-polizeiliche E-Mail-Überwachung eingegriffen wird, wird im 4. Kapitel behandelt. Zu diskutieren ist nicht nur der Eingriff in Grundrechte der betroffenen Kommunikationsteilnehmer, sondern auch der Grundrechtseingriff, zu dem die polizei- und ordnungsgesetzlichen Regelungen über die Mitwirkungspflicht der Diensteanbieter führen.

Sodann ist im 5. Kapitel zu untersuchen, ob diese verdeckte polizeiliche Maßnahme zur Informationserhebung verfassungsrechtlich gerechtfertigt werden kann. Zu prüfen ist nicht nur die formelle, sondern auch die materielle Verfassungsmäßigkeit des präventiv-polizeilichen Zugriffs auf die E-Mail-Kommunikation.

Das Dreiecksverhältnis, das bei der Durchführung einer präventiv-polizeilichen E-Mail-Überwachung vorliegt, wird im 6. Kapitel entfaltet. Dabei handelt es sich um Rechtsverhältnisse zwischen der überwachenden Polizeibehörde, den betroffenen Nutzern der E-Mail-Dienste und den betroffenen Anbietern der E-Mail-Dienste. In diesem Kapitel werden die verwaltungsrechtlichen Fragen, die sich aus dem präventiv-polizeilichen Zugriff auf die E-Mail-Kommunikation ergeben, behandelt.

Im 7. Kapitel wird der gerichtliche Rechtsschutz gegen die Maßnahme der präventiv-polizeilichen E-Mail-Überwachung und die polizeiliche Anordnung, durch die die Polizeibehörde den E-Mail-Providern die Mitwirkungspflicht auferlegt, dargelegt. Die Rechtsnatur des streitigen polizeilichen Handelns, die ein Ergebnis des 6. Kapitels darstellt, ist hierbei von großer Bedeutung.

2. Kapitel: Gefahrenabwehr im Internet als Ausgangspunkt präventiv-polizeilicher E-Mail-Überwachung

Die Entstehung des Internets führt zu revolutionären Veränderungen des modernen Lebens. Jedenfalls hat das Internet wegen seiner Verbreitung und seines Missbrauchs eine große Bedeutung in der Informationsgesellschaft: Es ist sowohl Informationsträger als auch Gefahrenträger. In diesem Zusammenhang entwickelt sich das Internet zu einem neuen Zuständigkeitsraum der Polizei, deren Aufgabe die Gefahrenabwehr ist. Wie die Polizei die Gefahren, die im Internet entstehen und durch das Internet verbreitet werden, effektiv abwehren kann, ist eine Herausforderung für das Polizeirecht im Digitalzeitalter. Sieht man die Überwachung der Internet-basierten Telekommunikation als eine der Möglichkeiten der Gefahrenabwehr im Internet, ist die Diskussion über Rechtsfragen der präventiv-polizeilichen E-Mail-Überwachung bedeutsam. Denn der E-Mail-Verkehr wird als die wichtigste und häufigste Internet-basierte Telekommunikation betrachtet. Im Folgenden wird die Verknüpfung zwischen der Gefahrenabwehr im Internet und der präventiv-polizeilichen E-Mail-Überwachung dargelegt.

A. Internet als neuer Zuständigkeitsraum der Polizei

I. Internet als Informationsträger

1. Entstehung des Internets

In der Informationsgesellschaft werden unzählige Informationen geschaffen, übermittelt, empfangen, gespeichert und genutzt. Nunmehr übernehmen neue Medien, die technisch und inhaltlich weit über die klassischen Kommunikationsformen und Informationsformate hinausgehen[1], die Aufgabe zur Informationsbeschaffung und -verarbeitung[2]. Aufgrund der Hilfe der Informations- und Kommunikationstechnik[3] können „Neue Medien“

1 *Kube*, in: Isensee/Kirchhof, HStR, Bd. 4, § 91 Rn. 1.

2 Diese Entwicklung zur Informationsgesellschaft führt zur Schwierigkeit der Abgrenzung zwischen Medien- und Informationsrecht (vgl. *Petersen*, Medienrecht, § 1 Rn. 5 ff.; *Petersen/Schoch*, JURA 2005, S. 681 ff.).

3 Eine Besonderheit der neuen Medien ist die Verwendung der Computer- und Digitaltechnik (vgl. *Fechner*, Medienrecht, 12. Kapitel Rn. 3; *Haug*, Internetrecht, Rn. 1).

den Informationsaustausch beschleunigen[4]. Zwar lässt sich der Inhalt des Begriffs „Neue Medien" nicht genau erfassen[5], es ist jedoch unstreitig, dass das Internet das bekannteste „Neue Medium" darstellt und im Vordergrund steht[6].

In Bezug auf die Entstehungsgeschichte des Internets kann das ARPANET (The Advanced Research Projects Agency Network), das im Jahre 1966 vom Verteidigungsministerium der Vereinigten Staaten entwickelt wurde, als der Urahn des heutigen Internets betrachtet werden[7]. Da der Zweck der Einrichtung von ARPANET nur war, die Funktionsfähigkeit des Netzwerks beim Ausfall einzelner Rechner zu sichern, scheiterte die Kommunikation zwischen den Netzen an den inkompatiblen Kommunikationsprotokollen[8]. Als das ARPANET 1983 das 1974 entwickelte TCP/IP (Transmission Control Protocol/Internet Protocol)[9], übernahm, war das Internet geboren[10].

Auf der Basis des TCP/IP entwickelte das Kernforschungszentrum in Genf (CERN) Anfang der 1990er Jahre das WWW (World Wide Web)[11]. Durch die Verwendung von HTTP (Hypertext Transfer Protocol) und HTML (Hypertext Markup Language) erlaubt das WWW die weltweite Datenübertragung von Texten, Bildern und Klängen zwischen Netzwerken[12]. Ferner bietet das WWW die technische Möglichkeit zum Hyperlink[13], der auf Inhalte fremder Webseiten verweisen und durch Anklicken direkt zu diesen fremden Webseiten verbinden kann[14]. Wegen dieser Funktion lässt sich das WWW nicht

4 Unter diesem Gesichtspunkt kann die Informationsgesellschaft als die Gesellschaft, die durch moderne Informations- und Kommunikationstechniken geprägt wird, betrachtet werden (vgl. *Hoffmann-Riem*, in: Hoffmann-Riem/Schmidt-Aßmann, Informationsgesellschaft, S. 9 (10); *Voßkuhle*, in: Hoffmann-Riem/Schmidt-Aßmann, Informationsgesellschaft, S. 349 (351 f.)).

5 *Beater*, Medienrecht, Rn. 269; *Dörr/Schwartmann*, Medienrecht, Rn. 292; *Fechner* (Fn. 3), 12. Kapitel Rn. 1 f.; vgl. auch *Kloepfer*, in: Isensee/Kirchhof, HStR, Bd. 3, § 42 Rn. 10.

6 *Beater* (Fn. 5), Rn. 270; *Fechner* (Fn. 3), 12. Kapitel Rn. 6.

7 Vgl. *Determann*, Kommunikationsfreiheit, S. 41 f.; *Germann*, Gefahrenabwehr und Strafverfolgung, S. 33; *Kloepfer*, Informationsrecht, § 1 Rn. 9; *Köhler/Arndt/Fetzer*, Recht des Internet, Rn. 1; *Kube* (Fn. 1), § 91 Rn. 3; *M. Sievers*, Schutz der Kommunikation, S. 29.

8 *Köhler/Arndt/Fetzer* (Fn. 7), Rn. 1; *Kube* (Fn. 1), § 91 Rn. 3.

9 Das TCP/IP ermöglicht den Datenaustausch zwischen unterschiedlichen Netzwerken. Auf diese Weise können die im Internet zusammengeschlossenen Rechner kommunizieren und Datenpakete über die Grenzen lokaler Computernetzwerke versenden (vgl. nur *Eberle*, in: Eberle/Rudolf/Wasserburg, Mainzer Rechtshandbuch, Kapitel I Rn. 46).

10 *Köhler/Arndt/Fetzer* (Fn. 7), Rn. 1; *Kube* (Fn. 1), § 91 Rn. 3; *Sievers* (Fn. 7), S. 31.

11 *Eberle* (Fn. 9), Kapitel I Rn. 47; *Kloepfer* (Fn. 7), § 1 Rn. 10; *Köhler/Arndt/Fetzer* (Fn. 7), Rn. 2; *Kube* (Fn. 1), § 91 Rn. 3; *Sievers* (Fn. 7), S. 33.

12 *Eberle* (Fn. 9), Kapitel I Rn. 47; *Kube* (Fn. 1), § 91 Rn. 4.

13 *Eberle* (Fn. 9), Kapitel I Rn. 47.

14 Vgl. *Fechner* (Fn. 3), 12. Kapitel Rn. 306; *Haug* (Fn. 3), Rn. 333; *Köhler/Arndt/Fetzer* (Fn. 7), Rn. 594; *Petersen* (Fn. 2), § 15 Rn. 27.

nur als ein wesentlicher Katalysator für die steigende Bedeutung des Internets[15], sondern auch als Synonym des Internets ansehen[16].

2. Internet als Informationsquelle im Sinne des Art. 5 Abs. 1 Satz 1 Hs. 2 GG

Wie bereits dargelegt wurde, kann das Internet mittels des WWW weltweit Daten oder Informationen[17] übertragen. Insoweit haben territoriale Grenzen immer weniger Bedeutung für den Informationsaustausch[18]. Jeder, der einen Internet-Zugang hat, kann aufgrund der Digitalisierung der Daten[19] über Internet jede vorher nur durch bestimmte herkömmliche Medien[20] empfangene Informationen in der ganzen Welt erhalten und herunterladen. Deswegen sind die Informationen im Internet grundsätzlich weltweit abrufbar[21].

Aus dieser Sicht lässt sich das Internet als Informationsquelle im Sinne des Art. 5 Abs. 1 Satz 1 Hs. 2 GG (Informationsfreiheit) ansehen[22]. Unter Informationsquellen versteht man alle denkbaren Informationsträger[23]. Ferner müssen die Informationsquellen im Sinne des Art. 5 Abs. 1 Satz 1 Hs. 2 GG allgemein zugänglich sein. Dies bedeutet, dass Informationsquellen technisch geeignet und bestimmt sind, der Allgemeinheit, also einem individuell nicht bestimmbaren Personenkreis, Informationen zu verschaffen[24]. Da das Internet nach seiner technischen Entwicklung eine weltumspan-

15 *Köhler/Arndt/Fetzer* (Fn. 7), Rn. 2.

16 Vgl. *Beater* (Fn. 5), Rn. 271; *Hornung*, MMR 2004, S. 3 (4).

17 Zum begrifflichen Unterschied zwischen Daten und Informationen *Hoffmann-Riem* (Fn. 4), S. 9 (12); *Petersen/Schoch* (Fn. 2), S. 681 (682); kritisch *Stern*, in: Stern, Staatsrecht, Bd. IV/1, S. 236.

18 Vgl. *Kube* (Fn. 1), § 91 Rn. 5; *Schoch*, VVDStRL 57 (1998), S. 158 (171); *Trute*, VVDStRL 57 (1998), S. 216 (244).

19 Digitalisierung bedeutet „die Umwandlung jedweder Art von Information (z. B. Texte, Musik, Sprache oder Bilder) in einen Binärcode". Ihr Vorteil besteht darin, dass die Daten „in Gestalt von elektrischen Impulsen ohne Qualitätsverlust übertragen werden können" (vgl. *Fechner* (Fn. 3), 12. Kapitel Rn. 3).

20 Z. B. Zeitung, Film, Fernsehen, Hörfunk etc.

21 *Kube* (Fn. 1), § 91 Rn. 5.

22 *Bethge*, in: Sachs, GG, Art. 5 Rn. 54; *Hufen*, Grundrechte, § 26 Rn. 6; *J. Ipsen*, Grundrechte, Rn. 431; *Jarass*, in: Jarass/Pieroth, GG, Art. 5 Rn. 16; *Kannengießer*, in: Schmidt-Bleibtreu/Hofmann/Hopfauf, GG, Art. 5 Rn. 9; *Schoch*, JURA 2008, S. 25 (28); *Sodan*, in: Sodan, GG, Art. 5 Rn. 13; *Starck*, in: von Mangoldt/Klein/Starck, GG, Bd. 1, Art. 5 Rn. 42; *Stern* (Fn. 17), S. 1404; *Zippelius/Würtenberger*, Staatsrecht, § 26 Rn. 45.

23 *Bethge* (Fn. 22), Art. 5 Rn. 54; *Jarass* (Fn. 22), Art. 5 Rn. 15; *Manssen*, Grundrechte, Rn. 333; *Pieroth/Schlink*, Grundrechte, Rn. 606; *Schoch* (Fn. 22), S. 25 (28); *Schulze-Fielitz*, in: Dreier, GG, Bd. 1, Art. 5 I, II Rn. 77; *Starck* (Fn. 22), Art. 5 Rn. 42; *Stern* (Fn. 17), S. 1403.

24 BVerfGE 27, 71 (83 f.); 90, 27 (32); 103, 44 (60); *Bethge* (Fn. 22), Art. 5 Rn. 55; *Ipsen* (Fn. 22), Rn. 430; *Jarass* (Fn. 22), Art. 5 Rn. 16; *Manssen* (Fn. 23), Rn. 334; *Schoch* (Fn. 22), S. 25 (28 f.); *Schulze-Fielitz* (Fn. 23), Art. 5 I, II Rn. 77; *Sodan* (Fn. 22), Art. 5 Rn. 13; *Starck* (Fn. 22), Art. 5 Rn. 44; *Stern* (Fn. 17), S. 1405; *Zippelius/Würtenberger* (Fn. 22), § 26 Rn. 45.

nende Allgemeinzugänglichkeit hat, werden die passive Entgegennahme der Informationen und die aktive Beschaffung und Speicherung von Informationen im Internet durch Art. 5 Abs. 1 Satz 1 Hs. 2 GG geschützt[25]. Dies bedeutet aber nicht, dass sich die grundrechtliche Relevanz des Internets in der Informationsfreiheit erschöpft. Vielmehr ist der Umstand, dass das Internet als eine Informationsquelle betrachtet wird, zugleich von Bedeutung für den Schutz anderer Grundrechte. Denn die im Internet übermittelten Informationen können die Vorstufe anderer Grundrechte (z. B. Meinungsfreiheit des Art. 5 Abs. 1 Satz 1 Hs. 1 GG oder Fernmeldegeheimnis des Art. 10 Abs. 1 GG) darstellen. In diesem Zusammenhang wird das Internet aufgrund seines Charakters als Informationsquelle zu einem bedeutsamen Raum der Grundrechte[26].

Zu beachten ist die Tatsache, dass das Internet eine Informationsquelle darstellt, die weit über die individuelle Ebene hinausgeht. Vor allem ist der Beitrag des Internets zur Demokratie in der Informationsgesellschaft nicht zu übersehen. Die Information(sfreiheit) ist eine der wichtigsten Voraussetzungen für die öffentliche Meinungsbildung in einer freiheitlichen Demokratie[27]. Erst mit der Hilfe der Informationsfreiheit „wird der Bürger in den Stand gesetzt, sich selbst die notwendigen Voraussetzungen zur Ausübung seiner persönlichen und politischen Aufgaben zu verschaffen, um im demokratischen Sinne verantwortlich handeln zu können“[28]. Da das Internet die Möglichkeit des weltumspannenden Informationsaustauschs bietet, befördert es wegen der Kommunikationsmöglichkeiten zwischen fremden Kulturen die pluralistische öffentliche Meinungsbildung[29]. Insoweit stellt das Internet trotz seiner virtuellen Eigenart nicht nur einen Raum der Grundrechte, sondern auch einen Vermittler der Wechselwirkung zwischen öffentlicher Meinung und Staatswillen[30] im digitalen Zeitalter dar.

---

25 Die „Unterrichtung“ im Sinne des Art. 5 Abs. 1 S. 1 Hs. 2 GG umfasst den gesamten Prozess des Sich-Informierens (Informationsrezeption, -speicherung, und -beschaffung), vgl. *Bethge* (Fn. 22), Art. 5 Rn. 53; *Hufen* (Fn. 22), § 26 Rn. 7; *Jarass* (Fn. 22), Art. 5 Rn. 17; *Manssen* (Fn. 23), Rn. 336; *Pieroth/Schlink* (Fn. 23), Rn. 610; *Schoch* (Fn. 22), S. 25 (30 f.); *Schulze-Fielitz* (Fn. 23), Art. 5 I, II Rn. 83; *Sodan* (Fn. 22), Art. 5 Rn. 14; *Stern* (Fn. 17), S. 1413.

26 *Kube* (Fn. 1), § 91 Rn. 6.

27 BVerfGE 7, 198 (208); 27, 71 (81); *Bethge* (Fn. 22), Art. 5 Rn. 51; *Michael/Morlok*, Grundrechte, Rn. 215; *Schulze-Fielitz* (Fn. 23), Art. 5 I, II Rn. 83; *Starck* (Fn. 22), Art. 5 Rn. 39.

28 BVerfGE 27, 71 (81 f.).

29 Vgl. *Schmitt Glaeser*, in: Isensee/Kirchhof, HStR, Bd. 3, § 38 Rn. 16. Zum Pluralismus der Demokratie *Badura*, in: Isensee/Kirchhof, HStR, Bd. 2, § 25 Rn. 32; *Böckenförde*, in: Isensee/Kirchhof, HStR, Bd. 3, § 34 Rn. 6; *Brenner*, in: Isensee/Kirchhof, HStR, Bd. 3, § 44 Rn. 2; *Isensee*, in: Isensee/Kirchhof, HStR, Bd. 2, § 15 Rn. 73.

30 Zur Wechselwirkung zwischen öffentlicher Meinung und Staatswillen *Kloepfer* (Fn. 5), § 42 Rn. 22.

II. Internet als Gefahrenträger

1. Gefahren im Internet

Obwohl das Internet die obigen positiven Funktionen hat, wird es wegen seines Missbrauchs allmählich zu einem Gefahrenträger. Auf der Basis der Technikentwicklung, die sich im schnellen Tempo verändert, entstehen zunehmend Gefahren im Internet[31]. Insoweit ist es nicht zu leugnen, dass die zunehmende Computer-Kriminalität bzw. Internet-Kriminalität[32] auf dem Vormarsch ist. Vor allem kommt immer wieder das Eindringen von Hackern in fremde Computer und Webseiten vor. Ferner bedroht die Verbreitung von Trojaner-Programmen den Schutz der im Computer gespeicherten personenbezogenen Daten und Betriebsgeheimnisse. In dieser Lage bietet das Internet eine gefährliche Voraussetzung für einen Hacker-Angriff.

Darüber hinaus nehmen die verbotenen Inhalte des Internets zu. Beispielsweise lässt sich Pornografie einfach im Internet ansehen und herunterladen[33]. Die Gewalt verherrlichenden Webseiten und Online-Spiele haben zudem schädlichen Einfluss auf Kinder und Jugendliche[34]. Zu befürchten ist nicht zuletzt, dass sich der Rassismus und Hassreden durch extreme Blogs oder Online-Foren immer weiter ausdehnen.

Immer weniger zu übersehen ist, dass das Internet den internationalen Terrorismus unterstützt. Da die Kommunikation durch Internet eine weltumspannende Besonderheit ist, können Terroristen, die sich in der ganzen Welt befinden, leichter miteinander Informationen austauschen. Verwenden sie beim Informationsaustausch die anonymen Internetdienste (z. B. E-Mail, Chatroom und VoIP), wird die Bekämpfung des Terrorismus äußerst schwierig[35].

Diese Gefährdungslagen bestehen zwar im Internet, auf dem die virtuelle Welt basiert, jedoch können sie polizeiliche Schutzgüter[36], also öffentliche

---

31 Vgl. dazu *Germann* (Fn. 7), S. 185 ff.; *Greiner*, Verhinderung verbotener Internetinhalte, S. 4 ff.; *Sieber*, MMR-Beilage 2/1999, S. 1 (2); *Würtenberger/Heckmann*, PolR BW, Rn. 544.

32 Die Computer-Kriminalität wird begrifflich von der Internet-Kriminalität unterschieden. „Computer-Kriminalität umfasst das deliktische Handeln, bei dem der Computer Werkzeug oder Ziel der Tat ist". Im Vergleich dazu betrifft die Internet-Kriminalität „diejenigen strafrechtlich relevanten Handlungen, die durch Nutzung von Datennetzen (insbes. Internet) begangen werden" (vgl. *Eisenberg*, Kriminologie, § 47 Rn. 65, 69).

33 Vgl. *Determann* (Fn. 7), S. 100 f.; *Greiner* (Fn. 31), S. 8 f.

34 Vgl. *Determann* (Fn. 7), S. 96; *Greiner* (Fn. 31), S. 9.

35 Vgl. *Holznagel/Bonnekoh*, MMR 2005, S. 585 (590).

36 Zu polizeilichen Schutzgütern *Götz*, PolR, § 4 Rn. 1 ff.; § 5 Rn. 1 ff.; *Gusy*, PolR, Rn. 78 ff.; *Kugelmann*, PolR, Kapitel 4 Rn. 22 ff.; *Pieroth/Schlink/Kniesel*, PolR, § 8 Rn. 1 ff.; *W.-R. Schenke*, PolR, Rn. 53 ff.; *Schoch*, in: Schmidt-Aßmann/Schoch, BesVerwR, 2. Kapitel, Rn. 65 ff.; *Tettinger/Erbguth/Mann*, BesVerwR, Rn. 440 ff.; *Waechter*, NVwZ 1997, S. 729 ff.; *Würtenberger/Heckmann* (Fn. 31), Rn. 398 ff.

Sicherheit und öffentliche Ordnung, in der Realwelt mit hinreichender Wahrscheinlichkeit schädigen. Im Hinblick auf ihre Intensität sind sie nicht nur bloße Belästigungen[37]. Unter dem Blickwinkel ihrer großen Schädigungswahrscheinlichkeit[38] lassen sie sich auch nicht nur pauschal als Risiken ansehen[39]. Vielmehr können die im Internet bestehenden Gefährdungslagen ohne Weiteres Gefahren im Sinne des Polizeirechts sein[40]. Da die Zuständigkeit der Polizei das Entstehen von Gefahren voraussetzt[41], ist das Internet kein (virtueller) rechtsfreier Raum[42], sondern ein neuer Zuständigkeitsraum der Polizei im digitalen Zeitalter.

2. Erfüllung staatlicher Schutzpflicht durch die Gefahrenabwehr im Internet

Der Umstand, dass das Internet zu einem Gefahrenträger in der Informationsgesellschaft wird, bedingt die Notwendigkeit der polizeilichen Gefahrenabwehr im Internet. Unter dem Aspekt der Grundrechte ist die Gefahrenabwehr im Internet als eine neue Verantwortung des Staats[43] zu betrachten, da das Internet, wie sich bereits aus den vorhergehenden Bemerkungen ergibt, einen Raum der Grundrechtsausübung in der Informationsgesellschaft darstellt. Zweifellos ist, dass die im Internet bestehenden Gefahren überwiegend durch technische Schutzmaßnahmen zu verhindern sind[44]. Fraglich ist jedoch, ob die Polizei rechtlich das *darf*, was sie tech-

37 Zur Unterscheidung zwischen Gefahren und bloßen Belästigungen *Götz* (Fn. 36), § 6 Rn. 5; *Gusy* (Fn. 36), Rn. 104 f.; *Pieroth/Schlink/Kniesel* (Fn. 36), § 4 Rn. 3; *Schenke* (Fn. 36), Rn. 74; *Schoch* (Fn. 36), Rn. 84; *Würtenberger/Heckmann* (Fn. 31), Rn. 413.

38 Nach der herrschenden Meinung lässt sich die Anforderung an die Schädigungswahrscheinlichkeit der Gefahr durch die Je-desto-Formel beurteilen, vgl. *Götz* (Fn. 36), § 6 Rn. 7; *Gusy* (Fn. 36), Rn. 119; *Pieroth/Schlink/Kniesel* (Fn. 36), § 4 Rn. 7; *Schenke* (Fn. 36), Rn. 77; *Schoch* (Fn. 36), Rn. 89; a. A. *Leisner*, DÖV 2002, S. 326 (328 f.). Zu beachten ist, dass die zur Bestimmung des Grads der Schädigungswahrscheinlichkeit verwendete Je-desto-Formel von der Prüfung der Verhältnismäßigkeit des polizeilichen Eingriffs zu unterscheiden ist, *Götz* (Fn. 36), § 6 Rn. 8.

39 *Greiner* (Fn. 31), S. 31 Fn. 136. Im Vergleich zur hinreichenden Wahrscheinlichkeit des Gefahrbegriffs steht der Risikobegriff „für Ungewissheiten bei der Beurteilung von Schadensmöglichkeiten". Dies bedeutet, dass der Risikobegriff nur eine „entfernte Möglichkeit des Schadenseintritts" erfasst (vgl. *Di Fabio*, JURA 1996, S. 566 (570); *Schoch* (Fn. 36), Rn. 89. Zur Abgrenzung zwischen Gefahren und Risiken siehe auch *Götz* (Fn. 36), § 6 Rn. 9; *Pieroth/Schlink/Kniesel* (Fn. 36), § 4 Rn. 6).

40 Die Gefahr ist der zentrale Begriff des Polizeirechts (vgl. *Di Fabio* (Fn. 39), S. 566; *Pieroth/Schlink/Kniesel* (Fn. 36), § 4 Rn. 1).

41 Vgl. *Gusy* (Fn. 36), Rn. 101; *Kugelmann* (Fn. 36), Kapitel 4 Rn. 82; *Pieroth/Schlink/Kniesel* (Fn. 36), § 4 Rn. 1.

42 *Kugelmann* (Fn. 36), Kapitel 5 Rn. 159.

43 Zur neuen staatlichen Verantwortung für das Internet *Kube* (Fn. 1), § 91 Rn. 11 ff.

44 Vgl. *Sieber* (Fn. 31), S. 1 (2).

nisch *kann*[45]. Um diese Frage zu beantworten, ist die verfassungsrechtliche Grundlage der polizeilichen Gefahrenabwehr, also die Schutzpflicht des Staats[46], heranzuziehen.

a) Idee der staatlichen Schutzpflicht

Über die Abwehrfunktion gegen staatliche Eingriffe[47], die als primäre und traditionelle Dimension der Grundrechte angesehen wird[48], hinaus haben Grundrechte noch objektiv-rechtliche Gehalte[49]. Dazu hat das Bundesverfassungsgericht im Lüth-Urteil[50] festgestellt, dass „das Grundgesetz, das keine wertneutrale Ordnung sein will, in seinem Grundrechtsabschnitt auch eine objektive Wertordnung aufgerichtet hat und dass gerade hierin eine prinzipielle Verstärkung der Geltungskraft der Grundrechte zum Ausdruck kommt. Dieses Wertsystem, das seinen Mittelpunkt in der innerhalb der sozialen Gemeinschaft sich frei entfaltenden menschlichen Persönlichkeit und ihrer Würde findet, muss als verfassungsrechtliche Grundentscheidung für alle Bereiche des Rechts gelten; Gesetzgebung, Verwaltung und Rechtsprechung empfangen von ihm Richtlinien und Impulse.“[51] Wegen ihrer objektiven Dimension, die als eine zentrale juristische Entdeckung des deutschen Staatsrechts nach 1945 gilt[52], stellen Grundrechte nicht nur bloße Abwehrrechte gegen den Staat, sondern auch Elemente der objektiven Ordnung dar[53]. Dementsprechend weiten sich die Funktionen der Grundrechte aus. Zu diesen aus objektiv-rechtlichen Grundrechtsgehalten hergeleiteten neuen Grundrechtsfunktionen gehört auch die Schutzpflicht des Staates[54].

45 Diese Frage stellen etwa *Würtenberger/Heckmann* (Fn. 31), Rn. 543.

46 *Götz*, in: Isensee/Kirchhof, HStR, Bd. 4, § 85 Rn. 24; vgl. auch *Gusy* (Fn. 36), Rn. 73; *Würtenberger/Heckmann* (Fn. 31), Rn. 23.

47 Vgl. dazu *Cremer*, Freiheitsgrundrechte, S. 74 ff.; *Poscher*, Abwehrrechte; *Sachs*, in: Merten/Papier, HGR, Bd. 2, § 39.

48 *Dreier*, in: Dreier, GG, Bd. 1, Vorb. Rn. 84 ff.; *Jarass*, in: Merten/Papier, HGR, Bd. 2, § 38 Rn. 6; *Hufen* (Fn. 22), § 5 Rn. 1.

49 Vgl. *Jarass* (Fn. 48), § 38 Rn. 15 ff.; *Manssen* (Fn. 23), Rn. 49; *Michael/Morlok* (Fn. 27), Rn. 863; *Sachs*, in: Sachs, GG, vor Art. 1 Rn. 31 ff.; *Sodan* (Fn. 22), Art. 1 Vorb. Rn. 20 ff.

50 BVerfGE 7, 198 ff.

51 BVerfGE 7, 198 (205); kritisch dazu *Cremer* (Fn. 47), S. 217 f.: Die objektiv-rechtlichen Grundrechtsgehalte „bilden kein methodengerechtes Fundament für die Anerkennung grundrechtlicher Ansprüche jenseits der Abwehrfunktion“. Das Bundesverfassungsgericht hat „einen über den abwehrrechtlichen hinausgehenden objektiven Gehalt der Grundrechte nicht begründet“.

52 *Wahl*, in: Merten/Papier, HGR, Bd. 1, § 19 Rn. 1.

53 Vgl. *Böckenförde*, Der Staat 29 (1990), S. 1; *Hufen* (Fn. 22), § 5 Rn. 3; *Jarass* (Fn. 48), § 38 Rn. 5 f.; *Kopp*, NJW 1994, S. 1573; *Wahl* (Fn. 52), § 19 Rn. 2; *Zippelius/Würtenberger* (Fn. 22), § 17 Rn. 19 ff.

54 BVerfGE 115, 118 (160); *Böckenförde* (Fn. 53), S. 1 (12); *Jarass* (Fn. 48), § 38 Rn. 22; *Michael/Morlok* (Fn. 27), Rn. 864; *Sodan* (Fn. 22), Art. 1 Vorb. Rn. 25; *Wahl* (Fn. 52), § 19 Rn. 5. Diese aus objektiv-rechtlichen Grundrechtsdimensionen hergeleiteten neuen Grundrechtsfunktio-

Die Grundrechtsfunktion der staatlichen Schutzpflicht kehrt sozusagen die Stoßrichtung der Abwehrfunktion der Grundrechte um[55]. Nach der Schutzpflichtenlehre ist der Staat verpflichtet, die Verletzung der grundrechtlich geschützten Rechtsgüter, die von privaten Dritten ausgeht, zu unterbinden[56]. Eigentlich ist diese Schutzrichtung dem Grundgesetz nicht fremd. Art. 1 Abs. 1 Satz 2 GG zeigt deutlich, dass der Schutz der Menschenwürde die Verpflichtung aller staatlichen Gewalt ist. Außerdem ist der Staat nach Art. 6 Abs. 4 GG verpflichtet, Mütter zu schützen. Zu beachten ist allerdings, dass diese im Grundgesetz ausdrücklich normierten „speziellen Schutzaufträge", die zur subjektiv-rechtlichen Dimension der Grundrechte gehören, von der allgemeinen Schutzpflicht des Staats zu unterscheiden sind[57]. Im Gegensatz zu speziell normierten Schutzaufträgen ergibt sich die (allgemeine) Schutzpflicht des Staats aus den objektiv-rechtlichen Grundrechtsgehalten[58]. Vor allem hat das Bundesverfassungsgericht durch zahlreiche Entscheidungen[59] aus der objektiv-rechtlichen Grundrechtsdimension des Art. 2 Abs. 2 GG die Pflicht des Staats zum Schutz

---

nen umfassen zudem etwa die Drittwirkung der Grundrechte, die Grundrechtswirkung für Organisations- und Verfahrensgarantien und die Einrichtungsgarantien (vgl. dazu *Dreier* (Fn. 48), Vorb. Rn. 96 ff.; *Gostomzyk*, JuS 2004, S. 949 (950 ff.); *Michael/Morlok* (Fn. 27), Rn. 864; *Sachs* (Fn. 49), vor Art. 1 Rn. 30 ff.; *Sodan* (Fn. 22), Art. 1 Vorb. Rn. 22 ff.; 30 f.; *Zippelius/Würtenberger* (Fn. 22), § 17 Rn. 12 ff.; 42 ff.). Es wird vertreten, dass objektive Grundrechtsfunktionen alle diejenigen Funktionen seien, die sich nicht mit der abwehrrechtlichen Komponente erklären lassen (so *Manssen* (Fn. 23), Rn. 49). Ob diese Behauptung zutrifft, erscheint zweifelhaft. Denn sie setzt die subjektiv-rechtliche Dimension der Grundrechte mit der Abwehrfunktion der Grundrechte gleich. Zwar stellt die Abwehrfunktion der Grundrechte den zentralen subjektiv-rechtlichen Grundrechtsgehalt dar, jedoch beschränken sich die subjektiv-rechtlichen Dimensionen der Grundrechte nicht auf die Abwehrrechte. Über die Abwehrrechte hinaus können Leistungsrechte vielmehr auch zu subjektiv-rechtlichen Dimensionen gehören (z. B. Art. 6 Abs. 1 und 4 GG) (vgl. *Dreier* (Fn. 48), Vorb. Rn. 83, 89; *Michael/Morlok* (Fn. 27), Rn. 864; *Zippelius/Würtenberger* (Fn. 22), § 17 Rn. 5).

55 *Dreier* (Fn. 48), Vorb. Rn. 101.

56 *Jarass* (Fn. 48), § 38 Rn. 24; *Dreier* (Fn. 48), Vorb. Rn. 101; *Klein*, DVBl. 1994, S. 489 (490); *Manssen* (Fn. 23), Rn. 50; *Pieroth/Schlink* (Fn. 23), Rn. 110 ff. Aus der Perspektive der Staatstheorie ist die Schutzpflicht des Staats nicht neu. Denn der Staat als Garant einer Friedensordnung ist aufgrund seines Gewaltmonopols verpflichtet, die Sicherheit des Bürgers zu schützen (vgl. *Calliess*, in: Merten/Papier, HGR, Bd. 2, § 44 Rn. 20 f.; *Ipsen* (Fn. 22), Rn. 104; *Isensee*, in: Isensee/Kirchhof, HStR, Bd. 5, 2. Aufl., § 111 Rn. 83; *Trute*, in: Erbguth/Müller/Neumann, GS Jeand'Heur, 1999, S. 403 (413)).

57 *Dreier* (Fn. 48), Vorb. Rn. 89, 104; *Isensee* (Fn. 56), § 111 Rn. 96; a. A. *Manssen* (Fn. 23), Rn. 50.

58 Die Schutzpflicht des Staats lässt sich sogar als Zentralbegriff der objektiv-rechtlichen Grundrechtsdimension ansehen (vgl. *Böckenförde* (Fn. 53), S. 1 (12); *Dreier* (Fn. 48), Vorb. Rn. 102; *Klein* (Fn. 56), S. 489 (491)).

59 Z. B. BVerfGE 39, 1 (41); 46, 160 (164); 49, 89 (140 ff.); 53, 30 (57); 56, 54 (73); 77, 381 (402 f.); 79, 174 (201 f.).

von Leben und Gesundheit hergeleitet[60]. Dies bedeutet aber nicht, dass sich die Schutzpflicht des Staats in Art. 2 Abs. 2 GG erschöpft. Vielmehr können alle anderen Freiheitsrechte wegen ihrer objektiv-rechtlichen Grundrechtsdimension ebenso eine Schutzpflicht des Staats begründen[61].

b) Grenzen der Erfüllung der staatlichen Schutzpflicht

Trotz der Anerkennung der staatlichen Schutzpflicht besteht die Problematik darin, wie der Staat seine Schutzpflicht erfüllen soll, um sie nicht zu verletzen. In diesem Punkt gilt das sog. Untermaßverbot[62], d. h., der Staat „muss ein gewisses Minimum an Schutz garantieren“[63]. Es fragt sich jedoch, wie der Staat beurteilt, mit welcher Intensität er das Schutzminimum verwirklicht. Hinsichtlich dieser Frage ist anerkannt, dass der Staat (insbesondere der Gesetzgeber) einen weitgehenden Ermessensspielraum, dessen Ziel die effektive Erfüllung staatlicher Schutzpflicht ist[64], genießt[65]. In der Regel kann der Gesetzgeber aufgrund seiner Einschätzung von Grundrechtsgefährdungen die Art und Weise von Maßnahmen des Schutzes bestimmen. Aus diesem Grund wird die Schutzpflicht nur verletzt, wenn der Staat „Schutzvorkehrungen entweder überhaupt nicht getroffen hat oder offensichtlich die getroffenen Regelungen und Maßnahmen gänzlich ungeeignet oder völlig unzulänglich sind, das Schutzziel zu erreichen“[66].

Da der Staat die Grundrechte des Einzelnen vor den Gefahren, die sich aus der Tätigkeit eines Dritten ergeben, schützen muss, kann es notwendig sein, dass er bei Erfüllung seiner Schutzpflicht in Grundrechte Dritter eingreift[67]. In diesem Zusammenhang hat die staatliche Schutzpflicht eine komplizierte Struktur. Sie betrifft nämlich das Rechte-Dreieck Staat – Störer – Opfer[68]. Der Staat muss einerseits zum Schutz des Opfers gewisse Maß-

60 Vgl. *Isensee* (Fn. 56), § 111 Rn. 80; *Murswiek*, in: Sachs, GG, Art. 2 Rn. 24 f.; *Schulze-Fielitz* (Fn. 23), Art. 2 II Rn. 76 ff.

61 *Dreier* (Fn. 48), Vorb. Rn. 89, 104; *Isensee* (Fn. 56), § 111 Rn. 86; *Klein* (Fn. 56), S. 489 (491); *Murswiek* (Fn. 60), Art. 2 Rn. 25.

62 BVerfGE 88, 203 (254); *Dreier* (Fn. 48), Vorb. Rn. 103; *Jarass* (Fn. 22), Vorb. vor Art. 1 Rn. 54; *Manssen* (Fn. 23), Rn. 52 f.; *Michael/Morlok* (Fn. 27), Rn. 627; *Sachs* (Fn. 49), vor Art. 1 Rn. 36; *Zippelius/Würtenberger* (Fn. 22), § 17 Rn. 40.

63 *Manssen* (Fn. 23), Rn. 52.

64 *Isensee* (Fn. 56), § 111 Rn. 165.

65 Vgl. BVerfGE 77, 170 (214 f.); 79, 174 (202); 115, 118 (159); *Hufen* (Fn. 22), § 5 Rn. 6; *Jarass* (Fn. 22), Vorb. vor Art. 1 Rn. 6; *Manssen* (Fn. 23), Rn. 52; *Pieroth/Schlink* (Fn. 23), Rn. 113; *Schulze-Fielitz* (Fn. 23), Art. 2 II Rn. 86 ff.; *von Münch*, Staatsrecht, Bd. 2, Rn. 152; *Zippelius/Würtenberger* (Fn. 22), § 17 Rn. 39.

66 BVerfGE 79, 174 (202); vgl. auch BVerfGE 92, 26 (46); *Pieroth/Schlink* (Fn. 23), Rn. 113; *Sachs* (Fn. 49), vor Art. 1 Rn. 36; *Zippelius/Würtenberger* (Fn. 22), § 17 Rn. 40.

67 *von Münch* (Fn. 65), Rn. 151; *Zippelius/Würtenberger* (Fn. 22), § 17 Rn. 37; vgl. auch *Ipsen* (Fn. 22), Rn. 106.

68 *Isensee* (Fn. 56), § 111 Rn. 87.

nahmen ergreifen. Andererseits stellen diese staatlichen Schutzmaßnahmen Beschränkungen der Grundrechte des Störers dar. Deswegen ist es ungeeignet, wenn die Erfüllung staatlicher Schutzpflicht nur einseitig unter dem Aspekt des Untermaßverbots überprüft wird. Ausgehend vom Eingriff in Grundrechte des Störers soll die Erfüllung staatlicher Schutzpflicht vielmehr zugleich auch an das Übermaßverbot gebunden sein[69]. Zwar muss der Staat das Untermaß- und Übermaßverbot gleichzeitig berücksichtigen[70], allerdings lässt sich nicht leugnen, dass die Anforderungen des Untermaßverbots und Übermaßverbots keine gleiche Intensität besitzen[71]. Im Vergleich zu der Anforderung des Übermaßverbots, also zu detaillierten Prüfungsstufen der Verhältnismäßigkeit[72], ist das Untermaßverbot wegen des weitgehenden staatlichen Ermessensspielraums milder. Wenn man den Faktor, dass die Subjektivierung der (objektiven) Schutzpflicht schwierig ist[73], berücksichtigt, lässt sich der Unterschied der Intensität zwischen den Anforderungen des Untermaßverbots und Übermaßverbots erkennen[74].

Die Anerkennung des weiten staatlichen Ermessensspielraums bedeutet nicht, dass der Staat alle möglichen effektiven Mittel zur Erfüllung seiner Schutzpflicht wählen kann. Denn die Wahl kann „immer nur auf solche Mittel fallen, deren Einsatz mit der Verfassung in Einklang steht“[75]. Falls der Staat verfassungswidrige Schutzmittel auswählt, darf eine solche (verfassungswidrige) Erfüllung staatlicher Schutzpflicht nicht als die Rechtfertigung des Eingriffs in Grundrechte Dritter angesehen werden[76].

---

69 *Isensee* (Fn. 56), § 111 Rn. 165.

70 Das begriffliche Verhältnis zwischen dem Untermaßverbot und dem Übermaßverbot (Grundsatz der Verhältnismäßigkeit) ist bislang jedoch noch unklar (vgl. *Cremer* (Fn. 47), S. 311).

71 *Michael/Morlok* (Fn. 27), Rn. 627. Im Schrifttum wird vertreten, dass die effektive oder wirksame Erfüllung der Schutzpflicht die vollendete Pflichterfüllung bedeute. Deswegen könne die staatliche Schutzpflicht nicht „mindestens“ erfüllt werden. In Eingriffsfällen dürfe sie nicht „übererfüllt“ werden. Insoweit gebe es keine Spanne zwischen Mindestmaß (Untermaßverbot) und Höchstmaß (Übermaßverbot) (vgl. *Hain*, DVBl. 1993, S. 982 (983)). Diese Auffassung ist abzulehnen. Bei der Pflichterfüllung geht es nur darum, dass die Pflicht entweder erfüllt oder nicht erfüllt wird. Die Rechtspflicht kann aber nicht „übererfüllt“ werden (*Cremer* (Fn. 47), S. 312). Die These, dass die Schutzpflicht in Eingriffsfällen nicht übererfüllt werden dürfe, verwechselt das Verhältnis zwischen Staat und Opfer mit dem Verhältnis zwischen Staat und Störer. Der übermäßige Eingriff in das Grundrecht des Störers bedeutet keineswegs eine übermäßige Erfüllung der Schutzpflicht gegenüber dem Opfer.

72 Zu Prüfungsstufen der Verhältnismäßigkeit *Jarass* (Fn. 22), Art. 20 Rn. 83 ff.; *Pieroth/Schlink* (Fn. 23), Rn. 289 ff.; *Sachs* (Fn. 49), Art. 20 Rn. 149 ff.; *Sodan* (Fn. 22), Art. 1 Vorb. Rn. 62 ff.; *Zippelius/Würtenberger* (Fn. 22), § 19 Rn. 85 ff.

73 Vgl. dazu *Ipsen* (Fn. 22), Rn. 109.

74 Das heißt, dass die Schwierigkeit der Subjektivierung der Schutzpflicht die Intensität des Untermaßverbots abschwächt bzw. zum weitgehenden staatlichen Ermessensspielraum führt.

75 BVerfGE 115, 118 (160).

76 Vgl. BVerfGE 115, 118 (159 f.).

c) Staatliche Schutzpflicht im Internet

Die Grundrechtsfunktion der staatlichen Schutzpflicht gilt auch im Internet[77], weil das Internet, wie dargelegt wurde, zu einem Gefahrenträger in der Informationsgesellschaft wird. Der Staat ist verpflichtet, die grundrechtlichen Gefährdungslagen, die sich im Internet durch private Dritte ergeben, zu verhindern. Aus der objektiv-rechtlichen Dimension der Grundrechte, deren Schutzgüter durch die Gefahren im Internet verletzt werden können[78], lässt sich die staatliche Schutzpflicht im Internet herleiten. Aufgrund der zunehmenden Gefährdung der Grundrechte im Internet ist die staatliche Schutzpflicht im Internet zweifelsfrei angesprochen.

Wie bereits ausgeführt wurde, genießt der Staat (insbesondere der Gesetzgeber) bei der Erfüllung seiner Schutzpflicht einen weiten Ermessensspielraum. Freilich ist das Untermaßverbot zu beachten. Dieses verpflichtet den Gesetzgeber, hinreichende Ermächtigungsgrundlagen zu schaffen, um die staatliche Schutzpflicht im Internet effektiv und wirksam zu erfüllen[79]. Falls der Gesetzgeber die neuen grundrechtlichen Gefährdungslagen im Internet übersieht und deswegen keine genügenden gesetzlichen Grundlagen für Schutzmaßnahmen schafft, dürfte die staatliche Schutzpflicht unter dem Aspekt des Untermaßverbots verletzt werden.

Das Ziel der staatlichen Schutzpflicht liegt darin, die von privaten Dritten verursachte Verletzung der grundrechtlich geschützten Rechtsgüter zu verhindern. Ausgehend davon haben präventive Schutzmaßnahmen einen Vorrang gegenüber repressiven Schutzmaßnahmen[80]. Zwar bestehen im StGB bereits einige Regelungen gegen die Computerkriminalität[81], jedoch sind sie nur sekundär bei der Erfüllung staatlicher Schutzpflichten im Internet. Im Vergleich dazu spielt die Frage, ob die Polizei die Gefahren im Internet effektiv und wirksam präventiv abwehren kann, die primäre Rolle. Aus diesem Grund darf sich der Gesetzgeber nicht nur mit dem Erlass des Straf- und Strafprozessrechts zur nachträglichen Verfolgung von Computerkriminalität begnügen. Vielmehr muss er der Polizei hinreichende Befugnisse zur Gefahrenabwehr im Internet einräumen[82].

Wie gezeigt wurde, ist die Erfüllung der staatlichen Schutzpflicht nicht als Rechtfertigung für Grundrechtseingriffe zu betrachten, wenn der Staat verfassungsrechtlich unzulässige Schutzmaßnahmen durchführt. Dieser Grundsatz ist insbesondere bei der Wahl der Mittel zur Gefahrenabwehr

77 Vgl. *Greiner* (Fn. 31), S. 25 ff.; *Schulze-Fielitz* (Fn. 23), Art. 5 I, II Rn. 222 ff.

78 Die durch die Gefahren im Internet bedrohten Rechtsgüter sind z. B. Menschenwürde, persönliche Ehre, Jugendschutz, geistiges Eigentum (vgl. *Greiner* (Fn. 31), S. 32 ff.) und Kommunikationsfreiheit (vgl. *Schulze-Fielitz* (Fn. 23), Art. 5 I, II Rn. 222 ff.).

79 Vgl. *Greiner* (Fn. 31), S. 39.

80 *Greiner* (Fn. 31), S. 39; *Hermes*, Grundrecht, S. 263.

81 Vgl. dazu *Ernst*, NJW 2007, S. 2661 ff.; *Gröseling/Höfinger*, MMR 2007, S. 626 ff.

82 *Greiner* (Fn. 31), S. 39.

im Internet zu beachten. Auch wenn die Polizei neue Internet-Technik beherrschen kann, ist zu prüfen, ob auch Schutzmaßnahmen, die neue Internet-Technik einsetzen, verfassungsmäßig sind.

Die Frage, ob sich der Rahmen staatlicher Schutzpflicht auf die Gefahren aus dem Inland beschränkt, hat große Bedeutung bei der Gefahrenabwehr im Internet. Da das Internet weltumspannend funktioniert, kann ein Großteil der Gefahren im Internet von Störern im Ausland verursacht werden[83]. Wenn die Abwehr der Gefahren, die von Störern im Ausland verursacht werden, nicht in den Rahmen staatlicher Schutzpflicht fällt, dürfte der Schutz unvollständig sein[84]. Theoretisch ist auch schwer einzusehen, warum der Staat nicht verpflichtet ist, die Gefahren, die sich im Ausland ergeben, aber im Inland die Grundrechte bedrohen, abzuwehren.

B. E-Mail als Internet-basiertes Informations- und Kommunikationsmittel

Das Internet ist von den Internetdiensten zu unterscheiden[85]. Da die Internetdienste wie etwa WWW, E-Mail oder Chatrooms durch die moderne Informations- und Kommunikationstechnik eine Funktion der Informationsübertragung haben, lassen sie sich als Informations- und Kommunikationsmittel, die auf dem Internet basieren, ansehen[86]. Falls sich gefahrenabwehrrechtlich relevante Sachverhalte im Internet-basierten Informations- und Kommunikationsverkehr verbergen, muss die Polizei diesen aufgrund der staatlichen Schutzpflicht überwachen, um diese Gefahren abzuwehren[87]. Angesichts dessen, dass die E-Mail das häufigste und wichtigste Internet-basierte Informations- und Kommunikationsmittel ist[88], entwickelt sich die Problematik präventiver E-Mail-Überwachung zur Gefahrenabwehr zu einem zentralen Thema des Polizeirechts in der Informationsgesellschaft.

Wie bereits im ersten Kapitel dieser Arbeit ausgeführt wurde, schaffen telekommunikationsrechtliche Vorschriften in Deutschland die technischen Voraussetzungen für die Umsetzung der präventiv-polizeilichen E-Mail-Überwachung. Angesichts dieser Entwicklung ist die Bedeutung der E-Mail-Kommunikation im Bereich des Telekommunikationsrechts zu untersuchen. Die telekommunikationsrechtlichen Vorschriften, die die

83 Z. B. Ausländische pornografische Webseiten, Computerviren aus dem Ausland etc.

84 *Greiner* (Fn. 31), S. 30.

85 *Kube* (Fn. 1), § 91 Rn. 4.

86 *Petri*, in: Lisken/Denninger, HPolR, H Rn. 343.

87 Vgl. *Petri* (Fn. 86), H Rn. 344.

88 Vgl. *Determann* (Fn. 7), S. 45 ff.; *Dürscheid*, in: Ziegler/Dürscheid, Kommunikationsform E-Mail, S. 93 (101); *Greiner* (Fn. 31), S. 15 f.; *Kleine-Voßbeck*, Electronic Mail, S. 12; *Meininghaus*, Zugriff auf E-Mails, S. 9; *Petri* (Fn. 87), H Rn. 343.

technischen und organisatorischen Vorkehrungen für die Umsetzung der Telekommunikationsüberwachung regeln, können für die E-Mail-Dienste nur gelten, wenn der E-Mail-Verkehr dogmatisch einer Telekommunikation entspricht. Darüber hinaus darf die Bedeutung der E-Mail-Dienste im Bereich des Medienrechts auch nicht übersehen werden. Da das Internet wegen der Multimedialität und digitaler Technik als „Neue Medien" bzw. „Multimedia" betrachtet wird[89], geht es bei der Gefahrenabwehr durch präventive E-Mail-Überwachung nicht nur um das Polizeirecht, sondern auch um das Medienrecht[90]. Ob die E-Mail-Dienste dem neuen Rechtsbegriff „Telemedien" gleichkommen, ist diskussionswürdig für die Untersuchung der präventiven E-Mail-Überwachung. Denn wenn die E-Mail-Dienste dem Begriff der Telemedien entsprechen, wird folgende Frage aufgeworfen: Darf die präventiv-polizeiliche E-Mail-Überwachung in den Bundesländern, in denen keine polizei- und ordnungsgesetzlichen Ermächtigungsgrundlagen für die Telekommunikationsüberwachung bestehen, nach medienrechtlichen Vorschriften zur Telemedienüberwachung durchgeführt werden[91]? Um diese sich im Überlagerungsbereich zwischen Polizeirecht, Telekommunikationsrecht und Medienrecht befindende Problematik klären zu können, sind der E-Mail-Verkehr und die E-Mail-Dienste aus telekommunikationsrechtlicher und medienrechtlicher Sicht zu erörtern.

I. E-Mail und Telekommunikation

1. Begriff der Telekommunikation

Es gibt zwar keinen einheitlichen Begriff der Telekommunikation[92], jedoch lässt sich eine Legaldefinition im Telekommunikationsgesetz (TKG) vom 22. Juni 2004[93] finden. Gemäß § 3 Nr. 22 TKG ist die Telekommunikation der technische Vorgang des Aussendens, Übermittelns und Empfangens von Signalen mittels Telekommunikationsanlagen. Wenn nur § 3 Nr. 22 TKG allein bestünde, wäre diese Legaldefinition ein Zirkelschluss, weil die Definition der Telekommunikation selbst logisch die Voraussetzung für die Bestimmung der Telekommunikationsanlagen ist. Dieser logische Fehler wird durch die Legaldefinition der Telekommunikationsanlagen in § 3 Nr. 23 TKG vermieden. Nach der Definition in § 3 Nr. 23 TKG sind Telekommunikationsanlagen technische Einrichtungen oder Systeme, die als

89 *Beater* (Fn. 5), Rn. 270; *Eberle* (Fn. 9), Kapitel I Rn. 2; *Fechner* (Fn. 3), 12. Kapitel Rn. 6; *Kloepfer* (Fn. 7), § 3 Rn. 92; *Kube* (Fn. 1), § 91 Rn. 1.

90 Berücksichtigt man, dass es keine deutliche Abgrenzung zwischen Informations- und Medienrecht gibt (vgl. dazu *Petersen* (Fn. 2), § 1 Rn. 6), kann man hierbei auch von Informationsrecht sprechen.

91 Zu dieser Frage siehe unten C.II.2.

92 *Dörr/Schwartmann* (Fn. 5), Rn. 296; *Gersdorf*, in: Eberle/Rudolf/Wasserburg, Mainzer Rechtshandbuch, Kapitel III Rn. 114.

93 BGBl. 2004 I S. 1190.

Nachrichten identifizierbare elektromagnetische oder optische Signale senden, übertragen, vermitteln, empfangen, steuern oder kontrollieren können.

Neben der deutlichen einfach-gesetzlichen Definition ist zu berücksichtigen, dass Art. 87 f GG, der sich als besondere Gesetzgebungsermächtigung des Grundgesetzes ansehen lässt[94], die zentrale verfassungsrechtliche Grundlage des TKG darstellt[95]. Außerdem ergibt sich die ausschließliche Gesetzgebungskompetenz des Bundes im Bereich der Telekommunikation aus Art. 73 Abs. 1 Nr. 7 GG[96]. Auch diese verfassungsrechtlichen Bestimmungen verwenden den Begriff der Telekommunikation[97].

Im Rahmen der Verfassungsänderung ersetzte der Begriff der Telekommunikation im Jahr 1994 den früher in Art. 73 Nr. 7 und Art. 87 f a. F. GG verwendeten Begriff des Fernmeldewesens. Hier ging es nicht um eine sachliche Änderung, sondern um die Anpassung an die international gebräuchliche Terminologie[98]. Demzufolge kann auf die Auslegung des Begriffs des Fernmeldewesens nach Art. 73 Nr. 7 und Art. 87 f a. F. GG zurückgegriffen werden[99].

Das Bundesverfassungsgericht hat im ersten Fernsehurteil[100] festgestellt, dass Fernmeldewesen ein technischer, am Vorgang der Übermittlung von Signalen orientierter Begriff sei[101]. Insoweit lässt sich das Fernmeldewesen als die Übermittlung der Informationen auf fernmeldetechnischem Wege definieren[102]. Hinsichtlich der Fernmeldetechnik hat das Bundesverfassungsgericht in einem weiteren Urteil erklärt, dass die Informationsübermittlung durch Fernmeldeanlagen die körperlose Übermittlung von Information sei[103]. Es komme nicht darauf an, welche Technik verwendet

94 Vgl. *Manssen*, in: Manssen, Telekommunikations- und Multimediarecht, C § 1 Rn. 3; *Nettesheim*, in: Säcker, TKG, Einl. III Rn. 260.

95 Vgl. *Fechner* (Fn. 3), 12. Kapitel Rn. 102; *Kloepfer* (Fn. 7), § 11 Rn. 9; *Manssen* (Fn. 94), C § 1 Rn. 3; *Masing*, in: Isensee/Kirchhof, HStR, Bd. 4, § 90 Rn. 29; *Scheurle*, in: Scheurle/Mayen, TKG, § 1 Rn. 1.

96 *Kloepfer* (Fn. 7), § 11 Rn. 9; *Jürgen/Elbracht*, Telekommunikationsrecht, Rn. 31; *Manssen* (Fn. 94), C § 1 Rn. 3; *Nettesheim* (Fn. 94), Einl. III Rn. 250.

97 Über Art. 73 Abs. 1 Nr. 7 und Art. 87 f GG hinaus wird der Begriff der Telekommunikation auch in Art. 80 Abs. 2 GG verwendet.

98 *Dörr/Schwartmann* (Fn. 5), Rn. 296; *Gersdorf*, in: von Mangoldt/Klein/Starck, GG, Bd. 3, Art. 87 f Rn. 12; *Heintzen*, in: von Mangoldt/Klein/Starck, GG, Bd. 2, Art. 73 Rn. 61; *Kunig*, in: von Münch/Kunig, GG, Bd. 3, Art. 73 Rn. 30 f.; *Sannwald*, in: Schmidt-Bleibtreu/Hofmann/Hopfauf, GG, Art. 73 Rn. 80; *Stettner*, in: Dreier, GG, Bd. 2 Supplementum, Art. 73 Rn. 38.

99 *Stettner* (Fn. 98), Art. 73 Rn. 39.

100 BVerfGE 12, 205.

101 BVerfGE 12, 205 (226).

102 *Degenhart*, in: Sachs, GG, Art. 73 Rn. 33; *Sannwald* (Fn. 98), Art. 73 Rn. 80.

103 BVerfGE 46, 120 (143).

werde[104]. Ob die Informationen am Empfangsort vom Menschen unmittelbar sinnlich wahrgenommen würden, sei unbeachtlich[105]. Der Begriff der Fernmeldeanlage umfasse nicht nur die bekannten Arten der Informationsübertragung, sondern auch neuartige Übertragungstechniken, sofern es um körperlose Übertragung der Informationen in der Weise gehe, dass diese am Empfangsort „wiedergegeben" würden[106]. Insoweit gehöre die Übermittlung digitaler Informationen zum Begriff des Fernmeldewesens[107].

Nach der Klärung des Begriffs „Fernmeldewesen" lässt sich feststellen, dass der Begriff der Telekommunikation in Art. 73 Abs. 1 Nr. 7 und Art. 87 f n. F. GG die körperlose Übermittlung der Informationen mit technischen Mitteln umfasst[108]. Mithin wird die Gesetzgebungskompetenz des Bundes im Bereich der Telekommunikation auf die technische Seite des Übermittlungsvorgangs der Informationen beschränkt[109]. Dem entspricht die einfach-gesetzliche Definition der Telekommunikation im TKG.

2. E-Mail-Verkehr als Telekommunikation

Bei der Versendung einer E-Mail ist die E-Mail-Adresse des Empfängers einzugeben. Die E-Mail-Adresse besteht aus zwei Teilen: Benutzername und Name des Mailservers[110]. Beide Teile werden durch das Sonderzeichen „@" verbunden[111]. Beispielsweise lautet die E-Mail-Adresse der Universität Freiburg „info@pr.uni-freiburg.de"[112].

Neben den E-Mail-Textnachrichten können alle Dateiformen, wie etwa Texte, Töne, Bilder und Videos, als E-Mail-Anlagen verschickt werden[113]. Nachdem der Absender durch die Bestätigung des „Absendens" eine E-Mail abgeschickt hat, werden diese E-Mail und ihre Anlagen zuerst an den Mailserver des Providers, der dem Absender die E-Mail-Dienste anbie-

104 BVerfGE 46, 120 (143), vgl. auch *Degenhart* (Fn. 102), Art. 73 Rn. 33; *Heintzen* (Fn. 98), Art. 73 Rn. 69; *Masing* (Fn. 95), § 90 Rn. 23; *Stettner* (Fn. 98), Art. 73 Rn. 39.

105 BVerfGE 46, 120 (143).

106 BVerfGE 46, 120 (144).

107 BVerfGE 46, 120 (144).

108 *Degenhart* (Fn. 102), Art. 73 Rn. 33; *Gersdorf* (Fn. 98), Art. 87 f Rn. 12; *Masing* (Fn. 95), § 90 Rn. 23.

109 Vgl. *Degenhart* (Fn. 102), Art. 73 Rn. 34; *Haratsch*, in: Sodan, GG, Art. 73 Rn. 16; *Heintzen* (Fn. 98), Art. 73 Rn. 73; *Kunig* (Fn. 98), Art. 73 Rn. 31; *Masing* (Fn. 95), § 90 Rn. 23; *Pieroth*, in: Jarass/Pieroth, GG, Art. 73 Rn. 26; *Sannwald* (Fn. 98), Art. 73 Rn. 82; *Stettner* (Fn. 98), Art. 73 Rn. 40.

110 Vgl. *Damm/Irion*, in: Eberle/Rudolf/Wasserburg, Mainzer Rechtshandbuch, Kapitel VII Rn. 7; *Determann* (Fn. 7), S. 46; *Germann* (Fn. 7), S. 71; *Hoeren*, Grundzüge des Internetrechts, S. 14; *Kleine-Voßbeck* (Fn. 88), S. 11.

111 *Damm/Irion* (Fn. 110), Kapitel VII Rn. 7; *Hoeren* (Fn. 110), S. 14.

112 Insoweit ist „info" der Benutzername. Demgegenüber stellt „pr.uni-freiburg.de" den Namen des Mailservers dar.

113 *Determann* (Fn. 7), S. 48; *Greiner* (Fn. 31), S. 16; *Kleine-Voßbeck* (Fn. 88), S. 10; *Sieber*, Verantwortlichkeit, Rn. 72.

ten, gesandt und dort kurz zwischengespeichert[114]. Danach werden sie durch die Technik des SMTP (Simple Mail Transfer Protocol) an den Mailserver des Providers, der dem Empfänger seine E-Mail-Dienste anbietet, weitergesandt[115]. In der Regel werden sie im Mailserver der dem Empfänger die E-Mail-Dienste anbietenden Provider gespeichert, bis der Empfänger sie mit dem Computer abruft[116]. In diesem Punkt dient die Technik des POP (Post Office Protocol) zum Abruf der E-Mail, die im Mailserver der Provider „ruht"[117]. Da der Übermittlungsvorgang der E-Mail auf dem Internet basiert, wird die E-Mail in einzelne digitale „Datenpakete" zerlegt und versandt[118]. Falls ein Versand der einzelnen Datenpakete gestört ist, wählen die Vermittlungsstellen (Router), die die Datenpakete in Richtung Empfänger weiterleiten, automatisch eine andere Verbindung[119]. Deswegen können verschiedene Datenpakete einer einzigen Datenübermittlung über verschiedene Wege übertragen werden[120].

Die Einrichtungen wie etwa Server und Router, die beim Versand einer E-Mail genutzt werden, sind als Telekommunikationsanlagen im Sinne des § 3 Nr. 23 TKG zu qualifizieren[121]. Aufgrund des obigen körperlosen Übermittlungsvorgangs der digitalen Informationen mittels der Telekommunikationsanlagen entspricht der E-Mail-Verkehr in technischer Hinsicht der Legaldefinition der Telekommunikation (§ 3 Nr. 22 TKG). Folglich sind E-Mail-Dienste (z. B. Gmail, Hotmail) als Telekommunikationsdienste (§ 3 Nr. 24 TKG) zu betrachten[122]. Diese Zuordnung steht mit der Richtlinie 2002/21/EG des Europäischen Parlaments und des Rates vom 7. März 2002 über einen gemeinsamen Rechtsrahmen für elektronische Kommunikationsnetze und -dienste (Rahmenrichtlinie)[123] in Einklang.

114 *Greiner* (Fn. 31), S. 16; *Sieber* (Fn. 113), Rn. 72.

115 *Behling*, Zugang elektronischer Willenserklärungen, S. 70 f.; *Sievers* (Fn. 7), S. 59.

116 *Greiner* (Fn. 31), S. 16; *Sieber* (Fn. 113), Rn. 72.

117 *Sievers* (Fn. 7), S. 62.

118 Vgl. dazu *Axmann/Degen*, NJW 2006, S. 1457 f.; *Behling* (Fn. 115), S. 70 f.; *Determann* (Fn. 7), S. 46; *Eberle* (Fn. 9), Kapitel I Rn. 46; *Hoffmann*, MMR 2002, S. 284 (287); *Kleine-Voßbeck* (Fn. 88), S. 10; *Sieber*, in: Hoeren/Sieber, Multimedia-Recht, Teil 1 Rn. 70. Die Internettelefonie (VoIP) basiert auch auf der Technik der Übertragung von Datenpaketen (vgl. *Holznagel/Bonnekoh* (Fn. 35), S. 585).

119 *Behling* (Fn. 115), S. 71; *Kleine-Voßbeck* (Fn. 88), S. 10.

120 *Kleine-Voßbeck* (Fn. 88), S. 10; *Sieber* (Fn. 118), Teil 1 Rn. 70.

121 Vgl. *Säcker*, in: Säcker, TKG, § 3 Rn. 68.

122 *Fetzer*, in: Arndt/Fetzer/Scherer, TKG, § 3 Rn. 86; *Heun*, in: Heun, Handbuch Telekommunikationsrecht, A Rn. 43; *Säcker* (Fn. 121), § 3 Rn. 73.

123 Erwägungsgrund 10, ABl. EG Nr. L 108 vom 24. 4. 2002, S. 33 (34).

II. E-Mail und Telemedien

1. Konvergenz der Medien

Im Gegensatz zum Telekommunikationsrecht, das sich auf die technische Seite der Informationsübertragung erstreckt, bezieht sich das Medienrecht auf die inhaltlichen Fragen der Kommunikation[124]. Zu betonen ist jedoch, dass sich die technische Entwicklung der Telekommunikation im Bereich des Medienrechts auswirkt. In diesem Punkt ist die Konvergenz der Medien am bemerkenswertesten. Durch digitale Internet-Technik können unterschiedliche Medieninhalte über dieselben Transportwege verbreitet und durch dasselbe Endgerät empfangen werden (technische Konvergenz)[125]. Beispielsweise lassen sich die Inhalte der verschiedenen herkömmlichen Medien wie etwa Texte der Zeitung, Programme des Radios, Filme und Musik über das Internet übertragen und durch den PC abrufen[126].

Wegen der technischen Konvergenz wurde daher der Begriff „Multimedia" geprägt. Zwar ist der Inhalt des Begriffs Multimedia noch unklar[127], bezeichnet er doch jedenfalls „die Möglichkeit der Kombination von Texten und Grafiken, bewegten Bildern und Tönen in einem Medium"[128]. Aus diesem Grund wird Multimedia auch „Neue Medien" genannt[129]. Insofern lässt sich der Begriff der „Neuen Medien" als die Gegenüberstellung zu den „alten" herkömmlichen Medien ansehen[130]. Können verschiedene Arten der Informationen (z. B. Text, Bild, Musik, Film) auf der Basis der Digitalisierung[131] in gleicher Weise, also durch „Neue Medien", übertragen und empfangen werden, wird die herkömmliche Abgrenzung der Medien immer unschärfer[132].

2. Rechtliche Ordnung für Multimediadienste

a) Kompetenzstreit

Aus der Sicht der Rechtspolitik soll die Konvergenz der Medien – jedenfalls aufgrund der Anforderung des Gleichheitssatzes – zu einer Konvergenz des

124 *Dörr/Schwartmann* (Fn. 5), Rn. 300; *Fechner* (Fn. 3), 12. Kapitel Rn. 100.

125 Vgl. *Dörr/Schwartmann* (Fn. 5), Rn. 253; *Determann* (Fn. 7), S. 110; *Eberle* (Fn. 9), Kapitel I Rn. 76; *Hartmann*, in: Wandtke, Medienrecht Praxishandbuch, 5. Teil 1. Kapitel Rn. 2; *Hoffmann-Riem/Schulz/Held*, Konvergenz und Regulierung, S. 20; *Holznagel*, NJW 2002, S. 2351 (2352); *Masing* (Fn. 95), § 90 Rn. 24; *Petersen* (Fn. 2), § 1 Rn. 24; *Schoch*, JZ 2002, S. 798.

126 Vgl. *Holznagel* (Fn. 125), S. 2351 f.; *Kube* (Fn. 1), § 91 Rn. 3.

127 *Fechner* (Fn. 3), 12. Kapitel Rn. 1.

128 *Fechner* (Fn. 3), 12. Kapitel Rn. 2; vgl. auch *Kloepfer* (Fn. 7), § 1 Rn. 13.

129 Vgl. *Fechner* (Fn. 3), 12. Kapitel Rn. 1; *Kloepfer* (Fn. 7), § 3 Rn. 92.

130 *Fechner* (Fn. 3), 12. Kapitel Rn. 2.

131 Die Digitalisierung der Übertragungswege ist die Grundlage der Konvergenz der Medien (vgl. *Fechner* (Fn. 3), 12. Kapitel Rn. 3 f.; *Petersen* (Fn. 2), § 1 Rn. 24; *Schoch* (Fn. 125), S. 798 (800)).

132 Vgl. dazu *Dörr/Schwartmann* (Fn. 5), Rn. 253; *Fechner* (Fn. 3), 12. Kapitel Rn. 3.

Medienrechts führen[133]. Tatsächlich weicht die rechtliche Ordnung für die vom Gesetzgeber als „Informations- und Kommunikationsdienste" bezeichneten Multimediadienste[134] in Deutschland jedoch von der Konvergenz des Medienrechts ab.

Eine grundlegende Ursache für diese Abweichung dürfte die Unklarheit der Gesetzgebungskompetenz im Bereich der Multimediadienste sein. Im Gegensatz zur ausschließlichen Gesetzgebungskompetenz des Bundes für das Telekommunikationsrecht, die sich aus Art. 73 Abs. 1 Nr. 7 GG ergibt, gibt es im Grundgesetz keine deutliche Vorgabe für die Aufteilung der Kompetenz zur Multimediagesetzgebung. Diese Unklarheit hatte einen Kompetenzstreit zur Folge. Einerseits leitete der Bund seine Gesetzgebungskompetenz hierfür aus Art. 74 Abs. 1 Nr. 11 GG (konkurrierende Gesetzgebungskompetenz im Bereich des Wirtschaftsrechts) ab[135]. Andererseits verwiesen die Länder darauf, dass keine ausdrückliche Gesetzgebungskompetenz des Bundes für Multimediadienste im Grundgesetz bestehe und die Länder deswegen gemäß Art. 70 GG diese Kompetenz hätten[136].

b) Parallelgesetzgebung als Kompromiss

Zur Beilegung dieses Kompetenzstreits verständigten sich Bund und Länder miteinander im Jahre 1996 über die Verteilung der Gesetzgebungskompetenz für das Recht der Multimediadienste[137]. Nach dem Kompromiss zwischen Bund und Ländern wurden die Multimediadienste in Teledienste, die für eine individuelle Nutzung bestimmt sind, und Mediendienste, die an die Allgemeinheit gerichtet sind, aufgeteilt[138]. Ausgehend dieser begrifflichen Trennung trat einerseits das Informations- und Kommunikationsdienste-Gesetz des Bundes (IuKDG) mit dem Teledienstegesetz (TDG = Art. 1 IuKDG) am 22. 7. 1997 in Kraft[139]. Andererseits wurden die Mediendienste durch den Mediendienste-Staatsvertrag (MDStV) von den Ländern geregelt.

---

133 *Petersen* (Fn. 2), § 1 Rn. 25; *Schoch* (Fn. 125), S. 798 (800); a. A. *Eberle* (Fn. 9), Kapitel I Rn. 78.

134 Vgl. *Engel-Flechsig/Maennel/Tettenborn*, NJW 1997, S. 2981 (2982); *Kloepfer* (Fn. 7), § 13 Rn. 1.

135 Vgl. *Fechner* (Fn. 3), 12. Kapitel Rn. 16.

136 Vgl. *Fechner* (Fn. 3), 12. Kapitel Rn. 16.

137 Vgl. dazu *Fechner* (Fn. 3), 12. Kapitel Rn. 17; *Gersdorf* (Fn. 92), Kapitel III Rn. 224; *Roßnagel*, NVwZ 1998, S. 1 (2); *Sieber* (Fn. 31), S. 1 (3).

138 Zur Abgrenzung zwischen Telediensten und Mediendiensten *Beater* (Fn. 5), Rn. 285; *Engel-Flechsig/Maennel/Tettenborn* (Fn. 134), S. 2981 (2983 f.); *Fechner* (Fn. 3), 12. Kapitel Rn. 17; *Gersdorf* (Fn. 92), Kapitel III Rn. 225 ff.; *Kloepfer* (Fn. 7), § 13 Rn. 4; *Roßnagel* (Fn. 142), S. 1 (3).

139 BGBl. 1997 I, S. 1870.

Ob der verfassungsrechtliche Kompetenzstreit durch einen politischen Kompromiss gelöst werden darf, ist allerdings zweifelhaft[140]. Wegen der zwingenden Kompetenzvorgaben im Grundgesetz ist eine „vereinbarte Kompetenzaufteilung" verfassungsrechtlich unzulässig[141]. Weder Bund noch Länder dürfen auf eine eigene Kompetenz verzichten. Sie dürfen auch nicht ihre Kompetenzen überschreiten. Zudem ist das bundesverfassungsgerichtliche Verfahren (Art. 93 Abs. 1 Nr. 3 GG) bei der Beilegung des Kompetenzstreits nicht zu umgehen. Die Grundlage der Parallelgesetzgebung für Multimediadienste ist folglich verfassungsrechtlich sehr problematisch.

Davon abgesehen ist die begriffliche Trennung zwischen Telediensten und Mediendiensten, die den Ausgangspunkt der Parallelgesetzgebung darstellt, zweifelhaft[142]. Das Ziel der Schaffung von TDG und MDStV war die Schlichtung des Kompetenzstreits für Multimediadienste. Hier ist zu berücksichtigen, dass die Entstehung von Multimedia aufgrund der technischen Konvergenz den Unterschied zwischen Individualkommunikation und Massenkommunikation verwässert[143]. Die Frage, welches Ziel (Individualkommunikation oder Massenkommunikation) die Dienste verfolgen, ist für Multimediadienste schwer zu beantworten. Da die Abgrenzung zwischen Telediensten und Mediendiensten darin lag, dass Erstere für eine individuelle Nutzung bestimmt sind und Letztere an die Allgemeinheit gerichtet waren, war das Scheitern dieser begrifflichen Trennung vorbestimmt. Vor allem bestand eine große Schwierigkeit der Trennung zwischen Telediensten und Mediendiensten im Bereich von Internetdiensten[144]. Die Parallelgesetzgebung führte keine Konvergenz des Medienrechts herbei. Hingegen hatte sie Unsicherheiten in der Rechtsanwendung zur Folge.

c) Neue Regelung: Telemediengesetz

Die problematische Trennung zwischen Telediensten und Mediendiensten wird – im Bundesrecht – durch das Telemediengesetz (TMG), das Art. 1 des Gesetzes zur Vereinheitlichung von Vorschriften über bestimmte elektronische Informations- und Kommunikationsdienste (Elektronischer-Geschäftsverkehr-Vereinheitlichungsgesetz – ElGVG) vom 26. 2. 2007[145] darstellt, abgelöst. Gemäß Art. 5 ElGVG traten TDG und MDStV außer Kraft.

140 *Stettner* (Fn. 98), Art. 73 Rn. 42.
141 *Stettner* (Fn. 98), Art. 70 Rn. 39.
142 *Fechner* (Fn. 3), 12. Kapitel Rn. 17; *Hartmann* (Fn. 125), 5. Teil 1. Kapitel Rn. 21.
143 *Dörr/Schwartmann* (Fn. 5), Rn. 253; *Schoch* (Fn. 18), S. 158 (170).
144 Vgl. *Schoch* (Fn. 125), S. 798 (802).
145 BGBl. 2007 I, S. 179.

Zugleich trat der neue Staatsvertrag für Rundfunk und Telemedien (RStV) der Länder[146], der einige Regelungen vom MDStV übernimmt, in Kraft[147].

Im TMG wird der neue Begriff „Telemedien" verwendet[148]. Nach § 1 Abs. 1 TMG versteht man unter Telemedien alle Informations- und Kommunikationsdienste, die elektronisch Text-, Bild- oder Toninhalte anbieten[149]. Diese umfassende Zielrichtung des Begriffs hat zur Folge, dass sowohl Teledienste als auch Mediendienste vom einheitlichen Begriff der Telemedien ersetzt werden[150]. Damit ist die Konvergenz des Medienrechts im Bundesrecht in gewissem Maße realisiert.

d) E-Mail-Dienste als Telemedien

Zwar gibt es keine Legaldefinition des Begriffs der Telemedien im TMG, jedoch lässt sich die Begriffsbedeutung der Telemedien durch § 1 Abs. 1 TMG (Anwendungsbereich) in groben Umrissen beschreiben. Gemäß § 1 Abs. 1 TMG gilt dieses Gesetz für alle elektronischen Informations- und Kommunikationsdienste, soweit sie nicht Telekommunikationsdienste nach § 3 Nr. 24 des Telekommunikationsgesetzes, die ganz in der Übertragung von Signalen über Telekommunikationsnetze bestehen, telekommunikationsgestützte Dienste nach § 3 Nr. 25 des Telekommunikationsgesetzes oder Rundfunk nach § 2 des Rundfunkstaatsvertrages sind (Telemedien).

Zu beachten ist, dass nicht alle Telekommunikationsdienste aus dem Begriff der Telemedien ausgeschlossen werden[151]. Nach § 3 Nr. 24 TKG sind Telekommunikationsdienste die Dienste, die „ganz oder überwiegend" in der Übertragung von Signalen über Telekommunikationsnetze bestehen. In diesem Zusammenhang können die Telekommunikationsdienste, die nur „überwiegend" in der Übertragung von Signalen über Telekommunikationsnetze bestehen, auch Telemedien sein[152]. Dazu gehören auch E-Mail-Dienste, weil sie neben der Übertragungsdienstleistung noch eine inhaltliche Dienstleistung anbieten[153].

146 GBl. BW 2007, S. 111.

147 Zum Gesetzgebungsverfahren des GlGVG *Hoeren*, NJW 2007, S. 801 f.; *Roßnagel*, NVwZ 2007, S. 743 f.

148 Eigentlich ist diese Terminologie nicht neu. Der Begriff der Telemedien wurde in § 3 Abs. 2 Nr. 1 Jugendmedienschutz-Staatsvertrag (JMStV) als Oberbegriff für Tele- und Mediendienste verwendet (vgl. *Dörr*, in: Dörr/Kreile/Cole, Medienrecht, S. 183).

149 *Degenhart* (Fn. 102), Art. 73 Rn. 37; *Roßnagel* (Fn. 147), S. 743 (744).

150 Vgl. BT-Drs. 16/3078, S. 11; *Hoeren* (Fn. 147), S. 801 (802); *Roßnagel* (Fn. 147), S. 743.

151 Die Auffassung, dass § 1 Abs. 1 TMG eine Abgrenzung der Dienste im Sinne eines „Entweder-Oder" fordere (so *Korehnke*, in: Schwartmann, Praxishandbuch, 8. Abschnitt Rn. 85), ist unzutreffend. § 1 Abs. 1 TMG grenzt nur die reinen Telekommunikationsdienste aus (*Eckhardt*, in: Heun, Handbuch, L Rn. 137). Ein Dienst, der dem Begriff der Telemedien entspricht, könnte deswegen zugleich auch einen Telekommunikationsdienst darstellen.

152 BT-Drs. 16/3078, S. 13; *Hoeren* (Fn. 147), S. 801 (802); *Roßnagel* (Fn. 147), S. 743 (745).

153 BT-Drs. 16/3078, S. 13; *Cole*, in Dörr/Kreile/Cole, Medienrecht, S. 103; *Eckhardt* (Fn. 151), L Rn. 142; *Hartmann* (Fn. 125), 5. Teil 1. Kapitel Rn. 40; *Roßnagel* (Fn. 147), S. 743 (745).

Aus der obigen telekommunikationsrechtlichen und medienrechtlichen Diskussion ergibt sich die Konsequenz, dass die E-Mail-Kommunikation eine Telekommunikation darstellt und die E-Mail-Dienste dem Begriff der Telemedien entsprechen. Deswegen kann die Polizeibehörde zur Gefahrenabwehr im Internet einen E-Mail-Verkehr beobachten, soweit der Gesetzgeber den präventiv-polizeilichen Zugriff auf die Telekommunikation erlaubt. Die Frage, ob die präventiv-polizeiliche E-Mail-Überwachung auch im Bereich des Medienrechts eine Ermächtigungsgrundlage finden kann, wird im Folgenden untersucht.

C. Präventiv-polizeiliche E-Mail-Überwachung als eine der Möglichkeiten zur Gefahrenabwehr im Internet

Heutzutage entwickelt sich die Gefahrenabwehr im Internet zu einem aktuellen Thema des Polizeirechts. Die Gefährdungslagen im Internet bestehen nicht nur in verbotenen Internetinhalten, sondern auch in der Online-Telekommunikation. Hinsichtlich der möglichen Maßnahmen zur Gefahrenabwehr im Internet kommen zunächst die Verhinderung und Beseitigung der verbotenen Internetinhalte in Betracht. Darüber hinaus ist auch die Überwachung der Internet-basierten Telekommunikation in Betracht zu ziehen. Ferner kommt die Maßnahme der sogenannten Online-Durchsuchung infrage.

Rechtlich eröffnet das TKG – wie sich bereits aus dem 1. Kapitel dieser Arbeit ergibt – die technische Möglichkeit zur Vorkehrung für die Umsetzung der präventiven-polizeilichen Telekommunikationsüberwachung. Da der E-Mail-Verkehr eine Telekommunikation im Sinne des TKG ist, gelten die im TKG zur Vorkehrung für die Umsetzung der präventiv-polizeilichen Telekommunikationsüberwachung vorgesehenen Regelungen auch für die Anbieter von E-Mail-Diensten. Allerdings enthält das TKG keine Ermächtigungsvorschrift zur Telekommunikationsüberwachung. Ob die Polizei selbst oder durch die Mitwirkung der Anbieter, deren technische Vorkehrung im TKG geregelt wird, den E-Mail-Verkehr präventiv zur Gefahrenabwehr überwachen darf, hängt davon ab, ob der Gesetzgeber entsprechende Ermächtigungsgrundlagen schafft. Damit sind zunächst die Regelungen zur präventiven Telekommunikationsüberwachung in Polizei- und Ordnungsgesetzen zu berücksichtigen. Da die E-Mail-Dienste dem Begriff der Telemedien entsprechen, ist ferner zu überlegen, ob es eine medienrechtliche Ermächtigungsgrundlage zur präventiv-polizeilichen E-Mail-Überwachung gibt.

I. Mögliche polizeiliche Maßnahmen zur Gefahrenabwehr im Internet

1. Verhinderung und Beseitigung der verbotenen Internetinhalte

Verbotene Internetinhalte (z. B. Gewaltverherrlichung oder Kinderpornografie) stellen polizeirechtliche Gefährdungslagen dar. Um die staatliche Schutzpflicht im Internet zu erfüllen, hat die Polizei diese Internetinhalte zu verhindern und zu beseitigen. Denkbares Vorgehen können die Beseitigung der gefährlichen Internetinhalte, die Sperrung des Zugangs zu auf anderen Servern gespeicherten fremden Internetinhalten oder der Einsatz von Filterprogrammen sein[154].

Die Beseitigung und Sperrung der verbotenen Internetinhalte sowie der Einsatz eines Filterprogramms bedürfen in aller Regel der technischen Hilfe der Inhalts- bzw. Serviceanbieter, die die Nutzung des Internets anbieten und damit dem bis 2007 geltenden Begriff der Teledienste (§ 2 TDG) entsprechen[155]. Da es – anders als § 18 MDStV – keine Zuständigkeitsvorschriften im TDG gab, hatte die Polizei früher die Zuständigkeit für die Überwachung von Verstößen einzelner Diensteanbieter gegen gesetzliche Bestimmungen[156]. Gemäß § 59 Abs. 2 und Abs. 3 RStV ist jedoch nun nur die nach Landesrecht bestimmte Aufsichtsbehörde[157] zuständig für die Überwachung telemedienrechtlicher Vorschriften und die Durchführung der erforderlichen Maßnahmen gegenüber dem Anbieter. Aufgrund dieser positiv-rechtlichen Regelung hat die Polizeibehörde keine Zuständigkeit mehr für die Überwachung der telemedienrechtlichen Normen und die Durchführung erforderlicher Maßnahmen gegenüber dem Internetanbieter[158].

2. Überwachung der Internet-basierten Telekommunikation

Die Gefährdungslage im Internet beschränkt sich nicht auf verbotene Internetinhalte. Sie besteht auch in Internet-basierter Telekommunikation. Wegen der Heimlichkeit der virtuellen Welt erleichtern die Mittel der Online-Telekommunikation wie etwa E-Mail oder Nachrichtensofortversand-Programm (z. B. MSN, SKYPE, Yahoo! Messenger, ICQ) die Übertragung der „gefährlichen Informationen". Das hat zur Folge, dass die Überwachung der Internet-basierten Telekommunikation zu einer neuen Möglichkeit der

154 Vgl. *Germann* (Fn. 7), S. 305 ff.; *Greiner* (Fn. 31), S. 44 ff.; *Würtenberger/Heckmann* (Fn. 31), Rn. 552; *Zimmermann*, NJW 1999, S. 3145.

155 *Cole* (Fn. 153), S. 101; *Eberle* (Fn. 9), Kapitel I Rn. 43; *Zimmermann* (Fn. 154), S. 3145 (3149).

156 *Schenke* (Fn. 36), Rn. 387 mit Fn. 106; *Würtenberger/Heckmann* (Fn. 31), Rn. 551; *Zimmermann* (Fn. 154), S. 3145 (3147).

157 Übersicht über die zuständigen Aufsichtsbehörden der Länder *Holznagel/Ricke*, MMR 2008, S. 18 (20).

158 *Schenke* (Fn. 36), Rn. 387.

Gefahrenabwehr im Digitalzeitalter wird. Diese neue Möglichkeit der (verdeckten) Gefahrenabwehr im Internet trifft jedoch den sensiblen Nerv der Grundrechte, weil die Daten der Online-Telekommunikation (z. B. IP-Adresse oder E-Mail-Adresse), die als personenbezogene Daten gelten[159], heimlich gespeichert, übermittelt und verarbeitet werden. Ferner kann eine solche staatliche verdeckte Informationserhebung im Internet – nach der Auffassung des Bundesverfassungsgerichts – in den unantastbaren Kernbereich privater Lebensgestaltung, dessen Schutz sich aus der Menschwürde (Art. 1 Abs. 1 GG) ergibt, eingreifen[160].

Da der E-Mail-Verkehr die wichtigste und häufigste Online-Telekommunikation darstellt[161], erhofft man sich durch den präventiven Zugriff auf die laufende E-Mail-Kommunikation (präventiv-polizeiliche E-Mail-Überwachung), die gefahrenabwehrrechtlich relevanten Sachverhalte aufzuklären und damit die Gefahr beseitigen zu können. Eine solche Erwartung kommt deutlich darin zum Ausdruck, dass immer mehr Bundesländer gesetzliche Ermächtigungsgrundlagen zur präventiv-polizeilichen Telekommunikationsüberwachung schaffen. Zwar steht dieser Entwicklungstrend nicht mit der Tradition[162] in Einklang, er entspricht jedoch einem oben genannten Grundsatz für die Erfüllung der staatlichen Schutzpflicht: Präventive Schutzmaßnahme ist vorrangig gegenüber repressiver Schutzmaßnahme[163]. Da die repressive Telekommunikationsüberwachung ihre gesetzlichen Grundlagen in §§ 100a, 100b StPO findet, könnten im Hinblick auf die Erfüllung der staatliche Schutzpflicht Bedenken bestehen, falls der Gesetzgeber der Polizei keine Befugnis zur präventiven Telekommunikationsüberwachung einräumt[164]. Nicht zu verkennen ist jedoch, dass die Ausweitung der polizeilichen Überwachungstätigkeit teilweise als ein vermeintlich weiterer Schritt in einen Orwell'schen Überwachungsstaat[165] angesehen wird[166]. Ob Deutschland aufgrund der Einführung präventiv-po-

159 IP-Adresse und E-Mail-Adresse sind als personenbezogene Daten zu betrachten (vgl. OLG Bamberg, MMR 2006, S. 481 (483); LG Berlin, MMR 2007, S. 799 (800); *Dammann*, in: Simitis, BDSG, § 3 Rn. 10; *Jandt*, MMR 2006, S. 652 (654); *Roßnagel*, NZV 2006, S. 281 (282); *Warg*, MMR 2006, S. 77 (80 f.)).

160 BVerfGE 113, 348 (390 ff.).

161 Dazu siehe oben Fn. 88.

162 Gemäß Art. 117 der Weimarer Reichsverfassung vom 11. 8. 1919 kann das „Fernsprechgeheimnis" nur durch Reichsgesetz, nicht aber durch Landesgesetz beschränkt werden (vgl. *Petri* (Fn. 86), H Rn. 305).

163 *Greiner* (Fn. 31), S. 39 f.

164 Vgl. *Schenke* (Fn. 36), Rn. 197b.

165 Der Begriff des Orwell'schen Überwachungsstaats beschreibt einen Zustand totaler Überwachung, wie ihn der britische Schriftsteller *George Orwell* in seinem Roman „1984" schilderte.

166 *R. P. Schenke*, AöR 125 (2000), S. 1 (6 f.).

lizeilicher Telekommunikationsüberwachung auf dem Weg zum Orwell'schen Überwachungsstaat ist, bleibt abzuwarten. Jedenfalls lässt sich feststellen, dass die präventiv-polizeiliche Überwachung der Internet-basierten Telekommunikation jetzt ihre gesetzlichen Ermächtigungsgrundlagen in den meisten Bundesländern findet[167].

3. Online-Durchsuchung

Schließlich gehört auch die sogenannte Online-Durchsuchung zum Aufgabenbereich der Gefahrenabwehr im Internet. Diese Maßnahme besagt eine Durchsuchung eines Computers nach in ihm gespeicherten Daten mittels der staatlichen Schadensoftware (Staatstrojaner)[168]. Technisch können die „Trojaner-Programme" durch Dateidownload aus manipulierten Webseiten, das Versenden einer E-Mail mit der getarnten Schadensoftware als Dateianhang, die Ausnutzung von Sicherheitslücken des Zielcomputers (aktives Hacking) und „Verstecken" der Software im Datenstrom unter Mithilfe eines Zugangsproviders im Zielcomputer installiert werden[169]. Eine manuelle Installation der „Trojaner-Programme" ist ebenfalls möglich[170]. Beispielsweise können die „Trojaner-Programme" dem Adressaten über eine CD mit vorgeblich interessanten Inhalten zugespielt werden[171]. Soweit eine Internetverbindung besteht, kann der Computer, in dem die staatlichen Trojaner-Programme heimlich installiert wurden, von der Polizei überwacht werden.

Zu beachten ist die Abgrenzung zwischen der Online-Durchsuchung und der Telekommunikationsüberwachung. Bei der Telekommunikationsüberwachung handelt es sich um die im Laufe des Telekommunikationsvorgangs stattfindende Erhebung der durch die Telekommunikation übertragenen Daten. Der Gegenstand der Überwachung ist die Telekommunikation selbst. Deswegen ist eine Telekommunikationsüberwachung unmöglich, soweit ein Telekommunikationsvorgang noch nicht beginnt oder schon abgeschlossen ist. Im Vergleich dazu betrifft die Online-Durchsuchung den Zugriff auf Daten, die noch nicht oder nicht mehr Gegenstand einer laufenden Telekommunikation sind[172]. Insoweit ist Online-Durchsuchung keine Überwachung der Telekommunikation, sondern eine Überwachung durch

167 Siehe unten II 2.

168 Zur Definition und technischen Möglichkeit der Online-Durchsuchung *Eifert*, NVwZ 2008, S. 521; *Gercke*, CR 2007, S. 245 (248); *Hofmann*, NStZ 2005, S. 121; *Huber*, NVwZ 2007, S. 880 (881); *Kutscha*, NJW 2007, S. 1169; *Leipold*, NJW-Spezial 2007, S. 135; *Schenke* (Fn. 36), Rn. 197 f.

169 *Buermeyer*, HRRS 2007, S. 154, http://www.hrr-strafrecht.de; *Gercke* (Fn. 168), S. 245 (248); *Huber* (Fn. 168), S. 880 (881).

170 *Gercke* (Fn. 168), S. 245 (248); *Huber* (Fn. 168), S. 880 (881).

171 *Hornung*, DuD 2007, S. 575.

172 BT-Dr. 16/9588, S. 70 (Begründung zur Befugnis des Bundeskriminalamtes für die Online-Durchsuchung im Entwurf des neuen BKA-Gesetzes).

Telekommunikation[173]. Beispielsweise entspricht die heimliche Erhebung der durch eine laufende E-Mail-Kommunikation übertragenen Daten dem Begriff der Telekommunikationsüberwachung (E-Mail-Überwachung). Wurde die E-Mail noch nicht vom Absender abgeschickt oder bereits vom Empfänger abgerufen und in seinem Computer gespeichert, stellt der verdeckte Zugriff auf diese E-Mail hingegen keine Telekommunikationsüberwachung (E-Mail-Überwachung), sondern eine Online-Durchsuchung dar.

Fraglos ist, dass eine Informationserhebung mittels einer Telekommunikationsüberwachung nach Abschluss des Telekommunikationsvorgangs unmöglich ist. Jedoch stellt sich die Frage, warum der Staat eine Online-Durchsuchung statt einer Telekommunikationsüberwachung durchführt, wenn er technisch im Laufe des Telekommunikationsvorgangs die Telekommunikation überwachen kann. Die Antwort ist nicht schwer zu geben: Die Telekommunikationsüberwachung hat eine technische Grenze[174]. Diese liegt vor, wenn die Teilnehmer der Telekommunikation eine verschlüsselte Verbindung nutzen. Beispielsweise wird ein starkes Verschlüsselungsverfahren für den Online-Banking-Service der Bank eingesetzt, um die Sicherheit der übertragenen Daten zu schützen. Bei der Überwachung einer solchen verschlüsselten Datenübertragung kann der Staat lediglich feststellen, dass eine Telekommunikation zwischen der Bank und dem Kunden stattfindet. Welche Daten übermittelt werden, kann der Staat technisch nicht durch Telekommunikationsüberwachung aufklären[175]. Die Daten, die in dieser Situation erhoben werden, sind wertlos. In diesem Zusammenhang hat die Online-Durchsuchung eine Ergänzungsfunktion gegenüber der Telekommunikationsüberwachung. Nach Abschluss der Telekommunikation kann der Staat – wenn eine gesetzliche Ermächtigungsgrundlage besteht – eine Online-Durchsuchung zur heimlichen Erhebung der detaillierten Daten durchführen.

Da die Online-Durchsuchung keine Telekommunikationsüberwachung ist, können die Regelungen über die Telekommunikationsüberwachung nicht als Ermächtigungsgrundlagen angesehen werden[176]. Außerdem lassen sich die polizei- und ordnungsgesetzlichen Ermächtigungsvorschriften zur (klassischen) Durchsuchung[177] und Beschlagnahme[178] auch nicht als

173 Vgl. BGHSt. 51, 211 (217 f.); *Hornung* (Fn. 171), S. 575 (576); *Klesczewski*, in: Säcker, TKG, § 110 Rn. 4; *Schenke* (Fn. 36), Rn. 197d; ähnlich *Hofmann* (Fn. 168), S. 121 (123); *Rux*, JZ 2007, S. 285 (292).

174 Vgl. *Buermeyer* (Fn. 169), S. 154 (159 f.).

175 *Buermeyer* (Fn. 169), S. 154 (160).

176 Vgl. BGH, NJW 2007, S. 930 (931 f.); *Hofmann* (Fn. 168), S. 121 (123); *Hornung* (Fn. 171), S. 575 (576); *Schenke* (Fn. 36), Rn. 197d.

177 Nachweise bei *Schenke* (Fn. 36), Rn. 151 mit Fn. 356.

178 Nachweise bei *Schenke* (Fn. 36), Rn. 158 mit Fn. 382.

Rechtsgrundlagen der Online-Durchsuchung betrachten[179]. Der Grund besteht darin, dass diese Regelungen (polizei- und ordnungsgesetzlichen Ermächtigungsvorschriften zur Durchsuchung und Beschlagnahme) der offenen Gefahrenaufklärung dienen. Im Gegensatz dazu stellt die Online-Durchsuchung eine heimliche Informationserhebung dar. Daher bedarf sie einer (eigenen) speziellen Ermächtigungsgrundlage. Bisher gibt es – mit Ausnahme des Art. 34d bayPAG – noch keine polizei- und ordnungsgesetzlichen Vorschriften zur Online-Durchsuchung[180]. Seiner Verfassungsschutzbehörde hat der nordrhein-westfälische Gesetzgeber durch § 5 Abs. 2 Nr. 11 des Gesetzes über den Verfassungsschutz in Nordrhein-Westfalen (NWVerfSchG)[181] die Befugnis zur Online-Durchsuchung eingeräumt. Jedoch erklärte das Bundesverfassungsgericht durch sein Urteil vom 27. 2. 2008[182] diese nordrhein-westfälische Vorschrift für grundgesetzwidrig und damit nichtig[183]. Obwohl § 5 Abs. 2 Nr. 11 NWVerfSchG für nichtig erklärt wurde, sah das Bundesverfassungsgericht die Online-Durchsuchung nicht als eine verfassungsrechtlich absolut unzulässige Eingriffsmaßnahme an, soweit sie weitergehenden verfassungsrechtlichen Anforderungen entspricht. In diesem Zusammenhang ist eine (zukünftige) Schaffung weiterer Rechtsgrundlagen für die Online-Durchsuchung denkbar. Auf Bundesebene wurde die Neufassung des BKA-Gesetzes[184], die durch seinen § 20k dem Bundeskriminalamt (BKA) die Befugnis für die präventive Online-Durchsuchung zur Bekämpfung des internationalen Terrorismus einräumt, bereits beschlossen. Auf Landesebene enthält der neue Art. 34d bayPAG, der am 01. 8. 2008 in Kraft trat, die Befugnis für die präventiv-polizeiliche Online-Durchsuchung[185]. Ob die präventiv-polizeiliche Online-Durchsuchung in Zukunft auch in anderen Bundesländern geregelt wird, bleibt abzuwarten.

4. Exkurs: Problematik der Quellen-Telekommunikationsüberwachung

Wie oben bereits ausgeführt wurde, ist die (traditionelle) Überwachung der Internet-basierten Telekommunikation schwierig, wenn die zu überwa-

179 *Schenke* (Fn. 36), Rn. 151, 159.
180 *Rux* (Fn. 173), S. 285 (289).
181 GVBl. NW 2006, S. 620.
182 BVerfGE 120, 274 ff.
183 Zu dieser Entscheidung des Bundesverfassungsgerichts vgl. *Bär*, MMR 2008, S. 325 ff.; *Britz*, DÖV 2008, S. 411 ff.; *Eifert* (Fn. 168), S. 521 ff.; *Hirsch*, NJOZ 2008, S. 1907 ff.; *Hornung*, CR 2008, S. 299 ff.; *Kutscha*, NJW 2008, S. 1042 ff.; *Sachs/Kring*, JuS 2008, S. 481 ff.
184 Gesetz über das Bundeskriminalamt und die Zusammenarbeit des Bundes und der Länder in kriminalpolizeilichen Angelegenheiten (letzte Änderung durch Art. 1 Terrorismusabwehr-G vom 25. 12. 2008, BGBl. I, S. 3083).
185 GVBl. BAY 2008, S. 365.

chende Telekommunikation verschlüsselt wird[186]. Zur Bewältigung dieser Überwachungsschwierigkeit kommt eine sogenannte Quellen-Telekommunikationsüberwachung in Betracht. Bei der Durchführung einer Quellen-Telekommunikationsüberwachung wird eine Spionagesoftware auf dem Zielcomputer installiert. Vor der Verschlüsselung der Telekommunikation werden die Daten der laufenden verschlüsselten Telekommunikation durch die auf dem Zielcomputer installierte Spionagesoftware erhoben und an die überwachende Behörde übermittelt. Obwohl die Quellen-Telekommunikationsüberwachung auch als heimlicher Zugriff auf informationstechnische Systeme über das Internet anzusehen ist, ist sie von der Online-Durchsuchung zu unterscheiden. Während die Online-Durchsuchung, deren Technik der Vorgehensweise auch die Installation eines Trojaner-Programms ist, der Gewinnung der im Zielcomputer gespeicherten Daten dient, werden – nach der Mitteilung der Bundesregierung[187] – durch die zur Quellen-Telekommunikationsüberwachung installierte Spionagesoftware nur die Daten der zu überwachenden Telekommunikation aufgezeichnet.

Es stellt sich die Frage, ob die Installation des Trojaner-Programms, das der Quellen-Telekommunikationsüberwachung dient, eine eigenständige Maßnahme gegenüber der dadurch ermöglichten Überwachung der verschlüsselten Telekommunikation ist. Berücksichtigt man, dass die überwachende Behörde zur Überwachung einer laufenden verschlüsselten Telekommunikation das Trojaner-Programm auf dem Zielcomputer installiert, ist diese Installation der Spionagesoftware als ein Teil der Maßnahme der Telekommunikationsüberwachung anzusehen[188]. Demzufolge kann die Installation des Trojaner-Programms, das der präventiv-polizeilichen Quellen-Telekommunikationsüberwachung dient, in den polizei- und ordnungsgesetzlichen Ermächtigungsvorschriften zur Telekommunikationsüberwachung ihre Rechtsgrundlage finden.

186 Ein Musterbeispiel der verschlüsselten Internet-basierten Telekommunikation ist das durch die VoIP-Software Skype geführte Telefongespräch.

187 BT-Drs. 16/6885, S. 4.

188 Dementsprechend greift die Installation des einer Quellen-Telekommunikationsüberwachung dienenden Trojaner-Programms nicht in das „Computergrundrecht", das durch das Urteil des Bundesverfassungsgerichts vom 27. 2. 2008 neu entwickelt wurde, sondern in das Fernmeldegeheimnis (Art. 10 Abs. 1 GG) ein. Zur dogmatischen Problematik des „Computergrundrechts" siehe 4. Kapitel A III.

II. Technische Art und Weise und rechtliche Rahmenbedingungen für präventiv-polizeiliche E-Mail-Überwachung

1. Technische Art und Weise der E-Mail-Überwachung

a) Häufigste technische Art und Weise: Abfangen der E-Mail

Wie bereits ausgeführt, wird die E-Mail in einzelne digitale „Datenpakete" zerlegt und versandt. Dies führt zu dem Risiko, dass die E-Mail an einem Übertragungsknoten abgefangen und damit kontrolliert werden kann[189]. Insoweit ist nachvollziehbar, dass das Abfangen der Datenpakete die häufigste technische Art und Weise der E-Mail-Überwachung darstellt. Um die E-Mails der Zielpersonen abzufangen und zu kontrollieren, setzt die überwachende Polizeibehörde mit Hilfe des Diensteanbieter im Knoten, über den die Datenpakete der E-Mails der Zielpersonen übertragen werden können, ein Überwachungsprogramm (E-Mail-Filter)[190] ein. Mit der Suche nach einschlägigen Stichworten (z. B. bestimmte Namen oder E-Mail-Adressen) kann der E-Mail-Filter die über den kontrollierten Internet-Knoten übermittelten E-Mail-Datenpakete analysieren und damit die „gefährliche E-Mail" finden. Die Kopie der gefundenen „gefährlichen E-Mail" wird durch eine spezielle Hardware (sogenannte Sina-Box), die nach § 110 TKG in Verbindung mit § 3 TKÜV bei Anbietern der E-Mail-Dienste installiert werden muss, auf den Server der überwachenden Polizeibehörde übertragen[191]. Festzustellen ist, dass die Sina-Box keine Überwachungsfunktion hat[192]. Da die Sina-Box durch ein VPN (Virtual Private Network) die Verbindung zwischen dem E-Mail-Filter und dem Server der überwachenden Polizeibehörde verschlüsselt[193], kann nur die überwachende Polizeibehörde auf der Sina-Box einloggen. Im Unterschied zum Überwachungsprogramm (E-Mail-Filter) stellt die Sina-Box deswegen sicher, dass kein Unbefugter die gefundene und auf den Server der überwachenden Polizeibehörde übertragene „gefährliche E-Mail" mitlesen kann[194].

b) Technische Folge: Erhebung der Telekommunikationsverkehrsdaten und Telekommunikationsinhaltsdaten

Mit der geschilderten technischen Überwachungsweise können sowohl Telekommunikationsverkehrsdaten als auch Telekommunikationsinhalte ermittelt werden. Nach § 3 Nr. 30 TKG sind Verkehrsdaten der Telekom-

189 Vgl. *Sieber* (Fn. 118), Teil 1 Rn. 70.
190 Z. B. das amerikanische System „Carnivore" (dazu *Sievers* (Fn. 7), S. 83 ff.).
191 *Ermert*, c't 1/2006, S. 44; *Krempl*, c't 26/2004, S. 100 (101 f.).
192 Zur Funktion der Sina-Box siehe die Website des Bundesamtes für Sicherheit in der Informationstechnik (http://www.bsi.de/fachthem/sina/sysbesch/sysbesch.htm).
193 *Ermert* (Fn. 191), S. 44; *Krempl* (Fn. 191), S. 100 (101 f.).
194 *Ermert* (Fn. 191), S. 44.

munikation die Daten, die bei der Erbringung eines Telekommunikationsdienstes erhoben, verarbeitet oder genutzt werden[195]. Ihr Katalog wird in § 96 Abs. 1 TKG aufgeführt. Gemäß § 96 Abs. 1 Nr. 1 oder 5 TKG[196] gehört die E-Mail-Adresse, die einerseits als „Nummer" oder „Kennung" im Sinne des § 96 Abs. 1 Nr. 1 TKG betrachtet werden kann und andererseits zum Aufbau einer E-Mail-Kommunikation technisch notwendig ist, zu Verkehrsdaten der Telekommunikation[197]. Auch der Zeitpunkt des Absendens der E-Mail, der mit der E-Mail-Adresse des Absenders und des Empfängers zusammen im Header (Kopfzeile der E-Mail) eingetragen ist, entspricht dem Begriff der Verkehrsdaten (§ 96 Abs. 1 Nr. 2 TKG). Da die (wichtigen) Verkehrsdaten der E-Mail-Kommunikation (E-Mail-Adresse des Absenders und Empfängers, Zeitpunkt des Absendens der E-Mail etc.) bereits in der Kopfzeile der E-Mail eingetragen werden, ergibt sich folgende Konsequenz: Sobald die Inhaltsdaten der E-Mail-Kommunikation mitgelesen werden, werden die Verkehrsdaten der E-Mail-Kommunikation zugleich erhoben. Obwohl die telekommunikationsrechtlichen Regelungen zur Vorratsdatenspeicherung (§§ 113a und 113b TKG) vom Bundesverfassungsgericht für nichtig erklärt wurden, kann die Behörde, die nach einschlägigen gesetzlichen Ermächtigungsvorschriften eine E-Mail-Kommunikation überwacht, durch die Erhebung der Inhaltsdaten der E-Mail-Kommunikation auch die Verkehrsdaten der E-Mail-Kommunikation gewinnen.

2. Präventiv-polizeiliche E-Mail-Überwachung nach polizei- und ordnungsgesetzlichen Regelungen zum präventiven Zugriff auf die Telekommunikation

Früher verzichtete der Landesgesetzgeber darauf, der Polizei die Befugnis zur Telekommunikationsüberwachung einzuräumen. Heutzutage gibt es in den meisten Bundesländern eine ausdrückliche polizei- und ordnungsgesetzliche Ermächtigungsvorschrift zur präventiven Telekommunikationsüberwachung, nach der die Polizei den E-Mail-Verkehr überwachen darf.

---

195 Von Verkehrsdaten zu unterscheiden sind die Bestandsdaten. Bestandsdaten sind die Daten eines Telekommunikationsteilnehmers, die für die Begründung, inhaltliche Ausgestaltung, Änderung oder Beendigung eines Vertragsverhältnisses über Telekommunikationsdienste erhoben werden (§ 3 Nr. 3 TKG). Zu Bestandsdaten zählen z. B. Name und Anschrift des Kunden (*Fetzer* (Fn. 122), § 3 Rn. 16; *Janik/Büttgen*, in: Geppert/Piepenbrock/Schütz/Schuster, TKG, § 3 Rn. 13; *Lünenbürger*, in: Scheurle/Mayen, TKG, § 3 Rn. 9; *Säcker* (Fn. 121), § 3 Rn. 9). Im Gegensatz zu Bestandsdaten, bei denen es um das Vertragverhältnis zwischen dem Diensteanbieter und seinen Kunden geht, betreffen Verkehrsdaten die technischen Umstände des Telekommunikationsvorgangs (*Graulich*, in: Arndt/Fetzer/Scherer, TKG, § 113 Rn. 3; *Säcker* (Fn. 121), § 3 Rn. 9).

196 § 96 Abs. 1 Nr. 5 TKG stellt einen Auffangtatbestand dar (*Klesczewski* (Fn. 173), § 96 Rn. 11; *Robert*, in: Geppert/Piepenbrock/Schütz/Schuster, TKG, § 96 Rn. 7).

197 *Graulich* (Fn. 195), § 113 Rn. 3.

Gemäß § 23a Abs. 1 Satz 1 Nr. 1 bwPolG ist eine präventiv-polizeiliche Erhebung der Telekommunikationsverkehrsdaten zulässig, soweit dies zur Abwehr einer unmittelbar bevorstehenden Gefahr für den Bestand oder die Sicherheit des Bundes oder eines Landes oder für Leben, Gesundheit oder Freiheit einer Person erforderlich ist. Da sich die nach § 23a Abs. 1 bwPolG zu erhebenden Informationen auf die Verkehrdaten der Telekommunikation beschränken, bezieht sich die präventiv-polizeiliche Telekommunikationsüberwachung in Baden-Württemberg nicht auf die Überwachung der Telekommunikationsinhalte[198]. Die präventiv-polizeiliche Telekommunikationsüberwachung kann auch durchgeführt werden, wenn konkrete Planungen oder Vorbereitungshandlungen für sich oder zusammen mit weiteren Tatsachen die Annahme rechtfertigen, dass Personen schwerwiegende Straftaten begehen werden (§ 23a Abs. 1 Satz 1 Nr. 2 Buchstabe a bwPolG) oder wenn Personen in die Planung oder Vorbereitung von schwerwiegenden Straftaten eines potenziellen Straftäters ganz oder teilweise eingeweiht sind oder deren Pläne aktiv unterstützen (§ 23a Abs. 1 Satz 1 Nr. 2 Buchstabe b bwPolG). Ferner kann sich die präventiv-polizeiliche Telekommunikationsüberwachung gegen die Personen richten, bei denen Tatsachen die Annahme rechtfertigen, dass sie Mitteilungen entgegennehmen, die für eine oben genannte Person bestimmt sind oder von ihr herrühren oder dass ihre Kommunikationseinrichtung von einer solchen Person benutzt wird (§ 23a Abs. 1 Satz 1 Nr. 2 Buchstabe c bwPolG). Die präventiv-polizeiliche Telekommunikationsüberwachung bedarf der Anordnung durch das Amtsgericht (§ 23a Abs. 3 Satz 1 bwPolG). Bei Gefahr im Verzug darf eine präventiv-polizeiliche Telekommunikationsüberwachung durch den Behördenleiter angeordnet werden (§ 23a Abs. 3 Satz 7 in Verbindung mit § 23 Abs. 3 Satz 8 bwPolG). Die Anbieter der Telekommunikationsdienste sind verpflichtet, bei der Durchführung einer präventiv-polizeilichen Telekommunikationsüberwachung mitzuhelfen (§ 23a Abs. 5 bwPolG).

Nach Art. 34a Abs. 1 Satz 1 Nr. 1 bayPAG kann die Polizei durch die Überwachung und Aufzeichnung der Telekommunikation personenbezogene Daten erheben, soweit dies zur Abwehr einer dringenden Gefahr für den Bestand oder die Sicherheit des Bundes oder eines Landes oder für Leib, Leben oder Freiheit einer Person oder für Sachen, soweit eine gemeine Gefahr besteht, erforderlich ist. Außerdem kann die präventiv-po-

198 BW-LT-Drs. 14/3165, S. 57. Die Beschränkung der polizeilichen Befugnis zur Telekommunikationsüberwachung auf die Verkehrsdaten stellt einen politischen Kompromiss dar (vgl. *Stephan*, in: Wolf/Stephan/Deger, PolG BW, § 23a Rn. 1). Da sich die in § 23a bwPolG vorgeschriebene präventiv-polizeiliche Telekommunikationsüberwachung nur auf die Erhebung der Telekommunikationsverkehrsdaten erstreckt, kommt das Abfangen der E-Mail, das auch zum Mitlesen der Inhaltsdaten der E-Mail-Kommunikation führt, technisch nicht in Betracht.

lizeiliche Telekommunikationsüberwachung durchgeführt werden, wenn konkret bestimmte Tatsachen die begründete Annahme rechtfertigen, dass Personen eine schwerwiegende Straftat begehen werden (Art. 34a Abs. 1 Satz 1 Nr. 2 bayPAG). Ferner kann sich die präventiv-polizeiliche Telekommunikationsüberwachung gegen die Kontakt- und Begleitpersonen richten (Art. 34a Abs. 1 Satz 1 Nr. 3 bayPAG). Die präventiv-polizeiliche Telekommunikationsüberwachung darf nur durch den Richter angeordnet werden (Art. 34c Abs. 1 in Verbindung mit Art. 34 Abs. 4 Satz 1 bayPAG). Bei Gefahr im Verzug kann die präventiv-polizeiliche Telekommunikationsüberwachung auch durch den Leiter eines Präsidiums der Landespolizei oder des Landeskriminalamts angeordnet werden (Art. 34c Abs. 1 in Verbindung mit Art. 34 Abs. 4 Satz 1 bayPAG). Gemäß Art. 35a bayPAG haben Diensteanbieter eine Mitwirkungspflicht für die präventiv-polizeiliche Telekommunikationsüberwachung.

In Brandenburg kann die Polizei personenbezogene Daten durch den verdeckten Einsatz technischer Mittel zur Überwachung und Aufzeichnung der Telekommunikation erheben, wenn bestimmte Tatsachen die Annahme rechtfertigen, dass dadurch Erkenntnisse erlangt werden, die für die Gefahrenabwehr von Bedeutung sind und dies zur Abwehr einer dringenden Gefahr für Leib, Leben oder Freiheit einer Person unerlässlich ist (§ 33b Abs. 1 in Verbindung mit § 33a Abs. 1 Nr. 1 bbgPOlG) oder aufgrund tatsächlicher Anhaltspunkte, insbesondere aufgrund konkreter Informationen über Planungs- und Vorbereitungshandlungen, anzunehmen ist, dass die in § 33a Abs. 1 Nr. 2 bbgPolG genannten Verbrechen organisiert begangen werden sollen, die drohende Rechtsgutsverletzung auch im Einzelfall schwer wiegt und die Datenerhebung zur Abwehr der mit diesen Straftaten verbundenen dringenden Gefahr erforderlich ist (§ 33b Abs. 1 in Verbindung mit § 33a Abs. 1 Nr. 2 bbgPOlG). Grundsätzlich darf die präventiv-polizeiliche Telekommunikationsüberwachung nur durch den Richter, bei Gefahr im Verzug auch durch den Behördenleiter, angeordnet werden (§ 33b Abs. 5 bbgPOlG). Nach § 33b Abs. 6 bbgPOlG haben Diensteanbieter Mitwirkungspflichten für die präventiv-polizeiliche Telekommunikationsüberwachung.

Die Polizei in Hamburg darf durch die Überwachung und Aufzeichnung von Telekommunikation einschließlich der innerhalb des Telekommunikationsnetzes in Datenspeichern abgelegten Inhalte Daten über die für eine Gefahr Verantwortlichen und unter den Voraussetzungen des § 10 hambSOG über die dort genannten Personen erheben, wenn dies zur Abwehr einer unmittelbar bevorstehenden Gefahr für Leib, Leben oder Freiheit einer Person erforderlich ist (§ 10a Abs. 1 hambGDatPol). Die Maßnahmen der Telekommunikationsüberwachung bedürfen einer Anordnung durch einen Richter. Ausnahmsweise können sie bei Gefahr im Verzug durch den Polizeipräsidenten angeordnet werden (§ 10c Abs. 1 hambGDatPol). Die Anbieter der Telekommunikationsdienste sind verpflichtet, bei der Durch-

führung einer präventiv-polizeilichen Telekommunikationsüberwachung mitzuwirken (§ 10a Abs. 3 hambGDatPol).

Das hessSOG ermächtigt die Polizei dazu, eine Telekommunikation zu überwachen. Die Polizeibehörden können gemäß § 15a Abs. 1 hessSOG von einem Diensteanbieter, der geschäftsmäßig Telekommunikationsdienste erbringt oder daran mitwirkt, verlangen, dass er die Kenntnisnahme des Inhalts der Telekommunikation ermöglicht und die näheren Umstände der Telekommunikation einschließlich des Standorts aktiv geschalteter nicht ortsfester Telekommunikationsanlagen übermittelt, wenn dies zur Abwehr einer gegenwärtigen Gefahr für Leib, Leben oder Freiheit einer Person unerlässlich ist. Die präventiv-polizeiliche Telekommunikationsüberwachung bedarf außer bei Gefahr im Verzug der richterlichen Anordnung (§ 15a Abs. 4 hessSOG).

In Mecklenburg-Vorpommern kann die Polizei personenbezogene Daten durch den Einsatz technischer Mittel zur Überwachung und Aufzeichnung der Telekommunikation erheben, wenn dies zur Abwehr einer im einzelnen Falle bevorstehenden Gefahr für Leib, Leben, Freiheit einer Person oder den Bestand oder die Sicherheit des Bundes oder eines Landes erforderlich ist (§ 34a Abs. 1 Satz 1 Nr. 1 mvSOG). Darüber hinaus kann die Polizei durch eine Telekommunikationsüberwachung personenbezogene Daten erheben über Personen, wenn deren Leben oder Gesundheit gefährdet ist (34a Abs. 1 Satz 1 Nr. 2 mvSOG). Der präventiv-polizeiliche Zugriff auf die Telekommunikation bedarf der richterlichen Anordnung (§ 34a Abs. 4 Satz 1 in Verbindung mit § 34 Abs. 3 Satz 1 mvSOG). Bei Gefahr im Verzug für Leib, Leben oder Freiheit einer Person kann der Behördenleiter die präventiv-polizeiliche Telekommunikationsüberwachung anordnen (§ 34a Abs. 4 Satz 1 in Verbindung mit § 34 Abs. 3 Satz 2 mvSOG). Der Diensteanbieter hat Mitwirkungspflichten für die präventiv-polizeiliche Überwachung der Telekommunikation (§ 34a Abs. 6 mvSOG).

Nach § 33a Abs. 1 ndsSOG[199] kann die Polizei zur Abwehr einer gegenwärtigen Gefahr für Leib, Leben oder Freiheit einer Person personenbezogene Daten über polizeirechtliche Störer und Nichtstörer durch Überwachung und Aufzeichnung der Telekommunikation erheben. Die präventiv-polizeiliche Telekommunikationsüberwachung bedarf einer Anordnung durch das Amtsgericht (§ 33a Abs. 4 ndsSOG). Bei Gefahr im Verzuge kann die Polizei die Anordnung treffen (§ 33a Abs. 5 ndsSOG). Die Mitwirkungspflichten der Diensteanbieter werden in § 33a Abs. 7 ndsSOG geregelt.

199 Da die Regelungen des § 33a Abs. 1 ndsSOG a. F. die Telekommunikationsüberwachung zur Strafverfolgungsvorsorge zuließen, wurden sie vom Bundesverfassungsgericht durch Entscheidung vom 27. 7. 2005 für nichtig erklärt (BVerfGE 113, 348 ff.). § 33a ndsSOG n. F. wurde am 25. 11. 2007 eingefügt (Nds. GVBl. S. 654).

Die präventiv-polizeiliche Telekommunikationsüberwachung ist auch in Rheinland-Pfalz zulässig. Gemäß § 31 Abs. 1 rpPOG kann die Polizei personenbezogene Daten über polizeirechtliche Störer und Nichtstörer durch den Einsatz technischer Mittel zur Überwachung und Aufzeichnung der Telekommunikation sowie durch Auskünfte über die Telekommunikation erheben, soweit die Datenerhebung zur Abwehr einer gegenwärtigen Gefahr für Leib oder Leben einer Person zwingend erforderlich ist. Die präventiv-polizeiliche Telekommunikation bedarf einer richterlichen Entscheidung (§ 31 Abs. 5 Satz 1 rpPOG). Bei Gefahr im Verzug kann die präventiv-polizeiliche Telekommunikationsüberwachung vorläufig durch die Behördenleitung oder einen von ihr besonders beauftragten Beamten des höheren Dienstes angeordnet werden (§ 31 Abs. 5 Satz 6 rpPOG). Diensteanbieter haben Mitwirkungspflichten für die Ermöglichung präventiv-polizeilicher Telekommunikationsüberwachung (§ 31 Abs. 6 rpPOG).

Durch die Änderung des Polizeigesetzes vom 12. 09. 2007 hat der saarländische Gesetzgeber eine Regelung zur präventiv-polizeilichen Telekommunikationsüberwachung eingefügt. Nach § 28b Abs. 1 saarlPolG kann die Vollzugspolizei durch die Telekommunikationsüberwachung personenbezogene Informationen erheben, um eine gegenwärtige Gefahr für Leib, Leben oder Freiheit einer Person abzuwehren oder die in § 100c StPO genannten Straftaten vorbeugend zu kämpfen. Eine Anordnung des Richters ist für diese heimliche polizeiliche Informationserhebung erforderlich (§ 28b Abs. 5 Satz 1 saarlPolG). Bei Gefahr im Verzug erfolgt die Anordnung durch die Behördenleitung oder eine von ihr beauftragte Beamtin oder einen von ihr beauftragten Beamten des höheren Polizeivollzugsdienstes; eine richterliche Entscheidung ist unverzüglich nachzuholen (§ 28b Abs. 5 Satz 4 saarlPolG). Anbieter der Telekommunikationsdienste haben eine Mitwirkungspflicht für die Ermöglichung der präventiv-polizeilichen Telekommunikationsüberwachung (§ 28b Abs. 2 saarlPolG).

In Schleswig-Holstein stellt der präventiv-polizeiliche Zugriff auf die Telekommunikation eine zulässige Maßnahme zur Gefahrenabwehr dar. Gemäß § 185a Abs. 1 Satz 1 shLVwG kann die Polizei personenbezogene Daten durch Überwachung und Aufzeichnung der Telekommunikation zur Abwehr einer gegenwärtigen Gefahr für Leib, Leben oder Freiheit einer Person erheben, wenn dies zur Aufklärung des Sachverhalts unerlässlich ist. Die präventiv-polizeiliche Überwachung der Telekommunikation darf nur richterlich angeordnet werden (§ 186 Abs. 1 Satz 1 shLVwG). Bei Gefahr im Verzuge kann der präventiv-polizeiliche Zugriff auf die Telekommunikation durch die Leiterin oder den Leiter des Landespolizeiamtes, des Landeskriminalamtes oder einer Polizeidirektion angeordnet werden (§ 186 Abs. 1 Satz 2 und 3 shLVwG). Die Mitwirkungspflichten der Diensteanbieter werden in § 185 Abs. 4 shLVwG geregelt.

Auch in Thüringen besteht eine gesetzliche Ermächtigungsgrundlage für die präventiv-polizeiliche Telekommunikationsüberwachung. Nach § 34a Abs. 1 und 2 thürPAG kann die Polizei unter Mitwirkung eines Dienstanbieters oder mit Hilfe von eigenen technischen Erfassungsanlagen eine Telekommunikation überwachen. Die präventiv-polizeiliche Telekommunikationsüberwachung kann sich gegen den für eine Gefahr Verantwortlichen richten, soweit dies zur Abwehr einer dringenden Gefahr für den Bestand oder die Sicherheit des Bundes oder eines Landes oder für Leib, Leben oder Freiheit einer Person oder für Sachen, soweit eine gemeine Gefahr besteht, zwingend erforderlich ist (§ 34a Abs. 3 Satz 1 Nr. 1 thürPAG). Zudem kann die präventiv-polizeiliche Telekommunikationsüberwachung auch zur Verhütung einer Straftat durchgeführt werden, wenn konkrete Planungs- und Vorbereitungshandlungen für sich oder zusammen mit weiteren bestimmten Tatsachen die begründete Annahme rechtfertigen, dass eine Straftat im Sinne des § 31 Abs. 5 thürPAG begangen werden soll (§ 34a Abs. 3 Satz 1 Nr. 2 thürPAG). Ferner kann sich die präventiv-polizeiliche Telekommunikationsüberwachung gegen Kontakt- oder Begleitpersonen richten (§ 34a Abs. 3 Satz 1 Nr. 3 thürPAG). Die präventiv-polizeiliche Telekommunikationsüberwachung bedarf einer Anordnung eines Richters (§ 34a Abs. 5 Satz 1 thürPAG). Soweit die Maßnahme der Telekommunikationsüberwachung erforderlich ist, kann die Anordnung bei Gefahr im Verzug der Leiter der Polizeibehörde oder bei dessen Verhinderung sein Stellvertreter treffen (§ 34a Abs. 5 Satz 2 thürPAG).

Aufgrund der genannten polizei- und ordnungsgesetzlichen Vorschriften hat der präventiv-polizeiliche Zugriff auf die E-Mail-Kommunikation in den meisten Bundesländern eine ausdrückliche Rechtsgrundlage. Die Polizei kann durch eigene moderne Technik den E-Mail-Verkehr überwachen[200]. Sie kann aber auch durch die technische Mithilfe der E-Mail-Provider diese verdeckte Maßnahme der Informationserhebung durchführen.

3. § 59 RStV als Ermächtigungsgrundlage für die präventiv-polizeiliche E-Mail-Überwachung?

Wenn man berücksichtigt, dass die E-Mail-Dienste dem Begriff der Telemedien entsprechen, wird die Frage aufgeworfen: Kann § 59 RStV eine Rechtsgrundlage für präventiv-polizeiliche E-Mail-Überwachung darstellen? Die Frage ist zu verneinen. Wie bereits dargelegt wurde, hat die Polizeibehörde gemäß § 59 Abs. 2 und Abs. 3 RStV keine Zuständigkeit mehr für die Durchführung erforderlicher Maßnahmen gegenüber den Anbietern der Telemedien. Darüber hinaus ist die E-Mail-Überwachung begrifflich keine Unter-

200 In Hessen kann die Polizei nicht selbst Maßnahmen zur E-Mail-Überwachung ergreifen (§ 15a Abs. 1 hessSOG).

brechung der E-Mail-Kommunikationsverbindung[201]. Deswegen gilt die Befugnis nach § 59 RStV, deren Rechtsfolge die Beseitigung (Untersagung oder Sperrung) der gefährlichen Internetinhalte ist, auch sachlich nicht für die E-Mail-Überwachung. Die Polizei in den Bundesländern, deren Polizei- und Ordnungsgesetze noch keine ausdrücklichen Vorschriften zur Telekommunikationsüberwachung enthalten, kann § 59 RStV nicht als Ermächtigungsgrundlage für die präventiv-polizeiliche E-Mail-Überwachung heranziehen.

D. Zusammenfassung des 2. Kapitels

Die Digitalisierung der Daten führt zur Beschleunigung des Informationsaustauschs. Angesichts dieser Entwicklung stellt das Internet, in dem Daten durch digitale Technik übermittelt werden, eine Informationsquelle in der Informationsgesellschaft dar. Allerdings ist zu berücksichtigen, dass die Kriminalität in der virtuellen Welt auf dem Vormarsch ist. Insoweit wird das Internet auch zu einem Gefahrenträger. Aufgrund seiner Schutzpflicht muss der Staat die Gefahren im Internet abwehren. Dies hat zur Folge, dass das Internet als ein neuer Zuständigkeitsraum der Polizei zu betrachten ist. Wegen dieser Entwicklung kommen drei denkbare Maßnahmen zur Abwehr der im Internet bestehenden Gefahren in Betracht: erstens die Verhinderung oder Beseitigung der verbotenen Internetinhalte; zweitens die Überwachung der Online-Telekommunikation; drittens die Online-Durchsuchung.

Der E-Mail-Verkehr lässt sich als wichtigste und häufigste Internet-basierte Telekommunikation ansehen. Aus diesem Grund gelten die in TKG und TKÜV vorgeschriebenen technischen Vorkehrungen für die Umsetzung der Telekommunikationsüberwachung auch für präventiv-polizeiliche E-Mail-Überwachung. Zurzeit haben elf Bundesländer eine polizei- und ordnungsgesetzliche Ermächtigungsgrundlage für den Zugriff auf die Telekommunikation. Dies bedeutet, dass die präventiv-polizeiliche E-Mail-Überwachung bereits in den meisten Bundesländern eine ausdrückliche Rechtsgrundlage hat.

Zwar entsprechen die E-Mail-Dienste dem neuen medienrechtlichen Begriff der Telemedien, aus § 59 RStV ergibt sich jedoch keine Befugnis für eine präventiv-polizeiliche E-Mail-Überwachung. Ob die Polizei in den

201 *Pieroth/Schlink/Kniesel* (Fn. 36), § 14 Rn. 128a. Gemäß § 23a Abs. 7 bwPolG; Art. 34a Abs. 4 S. 1 bayPAG, § 33b Abs. 3 Nr. 3 bbgPolG, § 10a Abs. 2 S. 1 hambGDatPol, § 34a Abs. 3 S. 2 mvSOG, § 33b Abs. 2 ndsSOG und § 34a Abs. 4 S. 1 thürPAG kann die Polizei unter den Voraussetzungen der Telekommunikationsüberwachung die Kommunikationsverbindungen durch den Einsatz technischer Mittel unterbrechen oder verhindern. Hieraus ergibt sich, dass es einen begrifflichen Unterschied zwischen der Telekommunikationsüberwachung und der Unterbrechung der Telekommunikationsverbindungen gibt.

Bundesländern, deren Polizei- und Ordnungsgesetze keine ausdrücklichen Ermächtigungsvorschriften zur präventiven E-Mail-Überwachung enthalten, nach der polizeirechtlichen Generalklausel oder der Generalklausel zur Informationserhebung[202] den E-Mail-Verkehr überwachen darf, wird im 5. Kapitel behandelt.

202 Nachweise bei *Schenke* (Fn. 36), Rn. 181 mit Fn. 444.

3. Kapitel: Klassische Gefahrenabwehr und vorbeugende Straftatenbekämpfung als Zwecke der geltenden Ermächtigungsvorschriften zur präventiv-polizeilichen Telekommunikationsüberwachung

Wie bereits im 2. Kapitel dargelegt wurde, gibt es in den meisten Bundesländern eine polizei- und ordnungsgesetzliche Ermächtigungsgrundlage für die präventiv-polizeiliche Überwachung eines E-Mail-Verkehrs. Die Zielsetzung dieser Vorschriften ist jedoch eingehender zu klären. Theoretisch herrscht in Deutschland ein Dualismus polizeilicher Aufgaben. Anders gesagt: Die Aufgaben der Polizei sollen nach ihrer Zielsetzung in präventive Gefahrenabwehr und repressive Strafverfolgung aufgeteilt werden[1]. Allerdings wird die Trennlinie immer dünner[2]. Das Graugebiet kommt vor allem in polizei- und ordnungsgesetzlichen Ermächtigungsvorschriften zur präventiven Telekommunikationsüberwachung zum Ausdruck. Alle polizei- und ordnungsgesetzlichen Ermächtigungsvorschriften zur Telekommunikationsüberwachung verfolgen den Zweck der Gefahrenabwehr. Nach § 23a Abs. 1 Satz 1 Nr. 2 bwPolG, Art. 34a Abs. 1 Nr. 2 bayPAG, § 33b Abs. 2 Satz 2 bbgPolG, § 28b saarlPolG und § 34a Abs. 3 Satz 1 Nr. 2 thürPAG kann die Polizei über die (klassische) Gefahrenabwehr hinaus zum Zweck der vorbeugenden Straftatenbekämpfung eine Telekommunikation überwachen. Es fragt sich, ob die vorbeugende Bekämpfung von Straftaten, die sich auf die zukünftig mögliche Begehung von Straftaten bezieht, noch in den Bereich der Gefahrenabwehr fällt oder bereits die Grenze zur Strafverfolgung überschreitet.

A. (Klassische) Gefahrenabwehr als Zweck der Ermächtigungsvorschriften zur präventiv-polizeilichen Telekommunikationsüberwachung

I. Dualismus polizeilicher Aufgaben

In Deutschland gilt der Dualismus polizeilicher Aufgaben. Einerseits weist § 163 StPO der Polizei die Aufgabe der Strafverfolgung zu. Andererseits gehört die Gefahrenabwehr nach den Polizei- und Ordnungsgesetzen auch

1 Vgl. dazu *Pieroth/Schlink/Kniesel*, PolR, § 2 Rn. 7 f.; *Schoch*, in: Schmidt-Aßmann/Schoch, BesVerwR, 2. Kapitel, Rn. 9.

2 *Gusy*, Die Polizei 2004, S. 61.

zur Aufgabe der Polizei. Zwar besteht eine Überschneidung[3], doch sind die beiden polizeilichen Aufgaben deutlich zu trennen.

1. Strafverfolgung als repressive Aufgabe der Polizei

Gemäß § 163 Abs. 1 StPO hat die Polizei Straftaten zu erforschen. Daraus lässt sich die polizeiliche Aufgabe der Strafverfolgung herleiten. Bei der Strafverfolgung geht es um die Aufklärung begangener Straftaten[4]. Da das Ziel der Strafverfolgung die Ahndung von Straftaten ist, setzt die Strafverfolgung eine bereits geschehene Straftat voraus[5]. Insoweit ist die Strafverfolgung die repressive Aufgabe der Polizei[6].

a) Gesetzgebungskompetenz

Gemäß Art. 72 Abs. 1 GG haben die Länder im Bereich der konkurrierenden Gesetzgebung die Befugnis zur Gesetzgebung, solange und soweit der Bund von seiner Gesetzgebungszuständigkeit nicht durch Gesetz Gebrauch gemacht hat. In diesem Zusammenhang hängt der Kompetenzumfang des Landesgesetzgebers im Bereich der konkurrierenden Gesetzgebung in der Regel davon ab, ob der Bund von seiner Gesetzgebungszuständigkeit Gebrauch gemacht hat[7]. Insofern hat das Bundesgesetz eine Sperrwirkung für die Gesetzgebungszuständigkeit der Länder im Bereich der konkurrierenden Gesetzgebung[8].

Die einzelnen Kompetenztitel im Bereich der konkurrierenden Gesetzgebung werden in Art. 74 Abs. 1 GG bestimmt[9]. Nach Art. 74 Abs. 1 Nr. 1 GG stellt das gerichtliche Verfahren einen Gegenstand der konkurrierenden Gesetzgebung dar. Unter dem Begriff des gerichtlichen Verfahrens im Sinne des Art. 74 Abs. 1 Nr. 1 GG wird die verfahrensmäßige Behandlung der Angelegenheiten durch die Gerichte verstanden[10]. Dazu gehört auch das unmittelbare „Vorfeld" des gerichtlichen Verfahrensrechts[11]. Deswegen fällt

3 Vgl. *Pieroth/Schlink/Kniesel* (Fn. 1), § 2 Rn. 9; *Schoch* (Fn. 1), Rn. 10.

4 *Gusy* (Fn. 2), S. 61 (63).

5 *Kugelmann*, PolR, 1. Kapitel Rn. 40.

6 *Denninger*, in: Lisken/Denninger, HPolR, E Rn. 169 f.; *Gusy* (Fn. 2), S. 61 (63); *Kugelmann* (Fn. 5), 1. Kapitel Rn. 40; *Pieroth/Schlink/Kniesel* (Fn. 1), § 2 Rn. 8; *Schoch* (Fn. 1), Rn. 9; *Tettinger/Erbguth/Mann*, BesVerwR, Rn. 621.

7 *Stettner*, in: Dreier, GG, Bd. 2 Supplementum, Art. 72 Rn. 14.

8 *Haratsch*, in: Sodan, GG, Art. 72 Rn. 6 ff.; *Kunig*, in: von Münch/Kunig, GG, Bd. 3, Art. 72 Rn. 7 f.; *Oeter*, in: von Mangoldt/Klein/Starck, GG, Bd. 2, Art. 72 Rn. 53, 59 ff.; *Pieroth*, in: Jarass/Pieroth, GG, Art. 72 Rn. 11 ff.; *Rengeling*, in: Isensee/Kirchhof, HStR, Bd. 6, 3. Aufl., § 135 Rn. 155 ff.; *Sannwald*, in: Schmidt-Bleibtreu/Hofmann/Hopfauf, GG, Art. 72 Rn. 14 ff.

9 Vgl. *Degenhart*, in: Sachs, GG, Art. 74 Rn. 1.

10 *Degenhart* (Fn. 9), Art. 74 Rn. 25; *Pieroth* (Fn. 8), Art. 74 Rn. 9; *Rengeling* (Fn. 8), § 135 Rn. 203; vgl. auch *Kunig* (Fn. 8), Art. 74 Rn. 19; *Seiler*, in: Epping/Hillgruber, GG, Art. 74 Rn. 10.

11 *Degenhart* (Fn. 9), Art. 74 Rn. 26; *Haratsch* (Fn. 8), Art. 74 Rn. 5; *Pieroth* (Fn. 8), Art. 74 Rn. 9; *Rengeling* (Fn. 8), § 135 Rn. 203; *Stettner* (Fn. 7), Art. 74 Rn. 28.

das strafprozessuale Ermittlungsverfahren in diesem Bereich, in dem das Bundesgesetz eine Sperrwirkung gegenüber der Gesetzgebungszuständigkeit von Ländern hat[12]. Der Gesetzgebungskompetenz für die Strafverfolgung, die als repressive Aufgabe der Polizei angesehen wird, liegt gemäß Art. 74 Abs. 1 Nr. 1 GG beim Bund[13].

b) Legalitätsprinzip

Nach § 163 Abs. 1 Satz 1 StPO ist die Polizei verpflichtet, Straftaten zu erforschen. Bei der Strafverfolgung besteht kein Ermessen der Polizei; es gilt das Legalitätsprinzip[14]. Das Legalitätsprinzip kann sich auch aus der Einheit des Ermittlungsverfahrens ergeben[15]. Die Staatsanwaltschaft als „Herrin des Ermittlungsverfahrens“[16] ist, soweit nicht gesetzlich ein anderes bestimmt ist, verpflichtet, wegen aller verfolgbaren Straftaten einzuschreiten, sofern zureichende tatsächliche Anhaltspunkte vorliegen (§ 152 Abs. 2 StPO). Da die Polizei gemäß § 161 StPO der Weisungsbefugnis der Staatsanwaltschaft unterliegt[17], fehlt das Ermessen der Polizei im Bereich der Strafverfolgung.

Im Schrifttum wird teilweise vertreten, dass das Legalitätsprinzip für die Strafverfolgung nur eingeschränkt gelte[18]. Ob die Polizei die Straftaten erforsche und verfolge, unterliege dem Legalitätsprinzip. Wie die Polizei die Straftaten erforsche und verfolge, unterliege hingegen dem Opportunitätsprinzip[19]. Dieser Auffassung ist nicht zuzustimmen. Jedenfalls steht diese Auffassung nicht mit § 161 Abs. 1 Satz 2 StPO in Einklang[20]. Aus § 161 Abs. 1 Satz 2 StPO lässt sich nur das Ergebnis herleiten, dass sich die Weisungsbefugnis der Staatsanwaltschaft auch auf das „Wie“ des polizeilichen Handelns erstreckt.

c) Rechtsschutz

Der Rechtsschutz gegen Strafverfolgungsmaßnahmen der Polizei kommt vor ordentlichen Gerichten in Betracht[21]. Es geht um die Sonderzuweisungen

12 *Degenhart* (Fn. 9), Art. 74 Rn. 26; *Haratsch* (Fn. 8), Art. 74 Rn. 5; *Oeter* (Fn. 8), Art. 74 Rn. 25; *Pieroth* (Fn. 8), Art. 74 Rn. 9; *Sannwald* (Fn. 8), Art. 74 Rn. 40; *Stettner* (Fn. 7), Art. 74 Rn. 28.

13 *Denninger* (Fn. 6), E Rn. 171 f.; *Kugelmann* (Fn. 5), 1. Kapitel Rn. 44; *Pieroth/Schlink/Kniesel* (Fn. 1), § 2 Rn. 8; *W.-R. Schenke*, PolR, Rn. 29; *Schoch* (Fn. 1), Rn. 9.

14 *Gusy*, PolR, Rn. 391; *Kugelmann* (Fn. 5), 8. Kapitel Rn. 2; *Pieroth/Schlink/Kniesel* (Fn. 1), § 2 Rn. 8; *Schenke* (Fn. 13), Rn. 413; *W.-R. Schenke/R. P. Schenke*, in: Steiner, BesVerwR, Rn. 222; *Schoch* (Fn. 1), Rn. 9; *Würtenberger/Heckmann*, PolR BW, Rn. 494.

15 Vgl. *Denninger* (Fn. 6), E Rn. 180.

16 *Denninger* (Fn. 6), E Rn. 180; *Götz*, PolR, § 18 Rn. 1.

17 *Denninger* (Fn. 6), E Rn. 180; *Schenke* (Fn. 13), Rn. 413; *Schoch* (Fn. 1), Rn. 9.

18 So *Knemeyer*, PolR, Rn. 403.

19 *Knemeyer* (Fn. 18), Rn. 403.

20 *Schenke* (Fn. 13), Rn. 413.

21 *Schoch*, JURA 2001, S. 628 (630 f.).

nach der StPO[22]. Zudem handelt es sich auch um den Rechtsweg nach §§ 23 ff. EGGVG, falls die Polizei durch sogenannte Justizverwaltungsakte handelt[23].

2. Gefahrenabwehr als präventive Aufgabe der Polizei

Neben der Aufgabe der Strafverfolgung, die durch die StPO zugewiesen ist, hat die Polizei die Aufgabe der Gefahrenabwehr. Die Rechtsgrundlage dafür liegt in den Polizei- und Ordnungsgesetzen. Die Aufgabe der Gefahrenabwehr bezieht sich auf das präventive Handeln der Polizei[24]. Denn für die Gefahrenabwehr „steht die Gefahr, d. h. der potenzielle Schaden, im Vordergrund“[25]. Die Polizei muss den potenziellen Schaden (= Gefahr) zum Schutz des Rechtsguts abwenden. Aufgrund des potenziellen Schadens und der möglichen Verhinderung stellt die zukunftsgerichtete Prognose den Ausgangspunkt der Gefahrenabwehr dar[26]. Insoweit unterscheidet sich die Gefahrenabwehr in der Zielsetzung von der Strafverfolgung[27].

Verfassungsrechtlich ergibt sich die präventive Aufgabe der Polizei, also die Gefahrenabwehr, aus der Schutzpflicht des Staats[28]. Der Staat mit seinem Gewaltmonopol hat die Aufgabe, die Grundrechte der Bürger vor Übergriffen Dritter zu schützen. Wenn das Individuum und die Allgemeinheit durch „Gefahren“ bedroht werden, muss der Staat präventiv die Gefahren beseitigen, um Grundrechte des Einzelnen und kollektive Rechtsgüter zu gewährleisten. Ausgehend davon ist die Gefahrenabwehr eine notwendige Aufgabe des Staats[29]. Die aus der Schutzpflicht hergeleitete Idee des „Präventionsstaats“[30] wird durch die Aufgabenzuweisung der Gefahrenabwehr in Polizei- und Ordnungsgesetzen erfüllt.

---

22 Vgl. dazu *Gusy* (Fn. 14), Rn. 482 f.; *Knemeyer* (Fn. 18), Rn. 413; *Pieroth/Schlink/Kniesel* (Fn. 1), § 2 Rn. 14.

23 *Gusy* (Fn. 14), Rn. 483; *Knemeyer* (Fn. 18), Rn. 412; *Pieroth/Schlink/Kniesel* (Fn. 1), § 2 Rn. 14; *Schoch* (Fn. 21), S. 628 (630).

24 *Götz* (Fn. 16), § 1 Rn. 1; *Gusy* (Fn. 14), Rn. 19; *Knemeyer* (Fn. 18), Rn. 71; *Kugelmann* (Fn. 5), 1. Kapitel Rn. 41; *Pieroth/Schlink/Kniesel* (Fn. 1), § 2 Rn. 8; *Schoch* (Fn. 1), Rn. 9.

25 *Gusy* (Fn. 2), S. 61 (63).

26 Vgl. *Gusy* (Fn. 2), S. 61 (63); *Kugelmann* (Fn. 5), 4. Kapitel Rn. 93 ff.; *Würtenberger/Heckmann* (Fn. 14), Rn. 416.

27 *Schoch* (Fn. 1), Rn. 9.

28 Vgl. *Gusy* (Fn. 14), Rn. 73; *Götz*, in: Isensee/Kirchhof, HStR, Bd. 4, § 85 Rn. 24; *Schoch* (Fn. 1), Rn. 20 f.; *Waechter*, NVwZ 1997, S. 729 (733); *Würtenberger/Heckmann* (Fn. 14), Rn. 23.

29 *Schoch* (Fn. 1), Rn. 20.

30 Zur Begriffsbildung des Präventionsstaats *Denninger* (Fn. 6), E Rn. 5; *Götz* (Fn. 28), § 85 Rn. 16; *Lisken*, NVwZ 2002, S. 513 (516); *Roggan/Bergemann*, NJW 2007, S. 876 (881); *Volkmann*, NVwZ 2000, S. 361 (366); *Wahl/Appel*, in: Wahl, Prävention und Vorsorge, S. 1 (14 f.); *Würtenberger/Heckmann* (Fn. 14), Rn. 23.

a) Gesetzgebungskompetenz

Gemäß Art. 70 Abs. 1 GG haben die Länder das Recht der Gesetzgebung, soweit das Grundgesetz nicht dem Bund Gesetzgebungsbefugnisse verleiht. Dadurch wird die Grundregel für die Verteilung der Gesetzgebungskompetenz zwischen Bund und Ländern aufgestellt[31]. Der Bund besitzt nur die Gesetzgebungskompetenz, die das Grundgesetz ihm zuweist. Seine Gesetzgebungszuständigkeit beschränkt sich nach Art. 70 Abs. 2 GG auf ausschließliche Bundesgesetzgebung (Art. 71 und 73 GG) und konkurrierende Gesetzgebung (Art. 72 und 74 GG). Hingegen fällt der unbenannte Rest in den Bereich der Gesetzgebungskompetenz der Länder[32].

Die Gefahrenabwehr stellt weder einen Gegenstand ausschließlicher Bundesgesetzgebung (Art. 73 GG) noch den Gegenstand konkurrierender Gesetzgebung (Art. 74 GG) dar. Demzufolge haben Länder die Gesetzgebungskompetenz für die Gefahrenabwehr[33]. Da die durch Art. 30 GG geregelte Kompetenzverteilung zwischen Bund und Ländern zwingend ist[34], dürfen Länder dem Bund ihre Gesetzgebungskompetenz für die Gefahrenabwehr, die sich aus Art. 70 GG ergibt, nicht überlassen[35]. Zwar begründet Art. 70 GG keine Gesetzgebungspflicht der Länder[36], jedoch dürfte das völlige Unterlassen des Gesetzgebers für die Gefahrenabwehr verfassungsrechtlich unzulässig sein.

b) Opportunitätsprinzip

Im Gegensatz zur polizeilichen Aufgabe der Strafverfolgung, die vom Legalitätsprinzip beherrscht wird, gilt im Bereich der Gefahrenabwehr das Opportunitätsprinzip[37]. Zwar lauten die Aufgabenzuweisungsnormen in Polizei- und Ordnungsgesetzen: „Die Polizei hat die Aufgabe, … Gefahren

31 *Degenhart* (Fn. 9), Art. 70 Rn. 7; *Pieroth* (Fn. 8), Art. 70 Rn. 1; *Rozek*, in: von Mangoldt/Klein/Starck, GG, Bd. 2, Art. 70 Rn. 11; *Stettner* (Fn. 7), Art. 70 Rn. 46.

32 *Degenhart* (Fn. 9), Art. 70 Rn. 7; *Haratsch* (Fn. 8), Art. 70 Rn. 10; *Kunig* (Fn. 8), Art. 70 Rn. 5; *Pieroth* (Fn. 8), Art. 70 Rn. 1; *Rozek* (Fn. 31), Art. 70 Rn. 2; *Stettner* (Fn. 7), Art. 74 Rn. 46.

33 BVerfGE 8, 143 (150); 110, 141 (173); *Gusy* (Fn. 14), Rn. 29; *Kugelmann* (Fn. 5), 1. Kapitel Rn. 148; *Kunig* (Fn. 8), Art. 70 Rn. 8; *Pieroth/Schlink/Kniesel* (Fn. 1), § 2 Rn. 8; *Pieroth* (Fn. 8), Art. 70 Rn. 17; *Schenke* (Fn. 13), Rn. 23; *Schoch* (Fn. 1), Rn. 9; *Tettinger/Erbguth/Mann* (Fn. 6), Rn. 387; *Würtenberger/Heckmann* (Fn. 14), Rn. 73.

34 *Erbguth*, in: Sachs, GG, Art. 30 Rn. 11; *Leisner*, in: Sodan, GG, Art. 30 Rn. 4; *Pieroth* (Fn. 8), Art. 30 Rn. 8; *Rengeling* (Fn. 8), § 135 Rn. 16; *Rozek* (Fn. 31), Art. 70 Rn. 15; *Sannwald* (Fn. 8), Art. 30 Rn. 8; *Stettner* (Fn. 7), Art. 74 Rn. 39.

35 Vgl. BVerfGE 32, 145 (156); 63, 1 (39).

36 *Degenhart* (Fn. 9), Art. 70 Rn. 63; *Haratsch* (Fn. 8), Art. 70 Rn. 8; *Kunig* (Fn. 8), Art. 70 Rn. 14; *Pieroth* (Fn. 8), Art. 70 Rn. 32; *Rozek* (Fn. 31), Art. 70 Rn. 18; *Sannwald* (Fn. 8), Art. 70 Rn. 10; *Stettner* (Fn. 7), Art. 70 Rn. 26; a. A. *Bleckmann*, DÖV 1983, S. 129 (131).

37 *Götz* (Fn. 16), § 11 Rn. 1; *Haurand/Vahle*, NVwZ 2003, S. 513; *Gusy* (Fn. 14), Rn. 391; *Kugelmann* (Fn. 5), 8. Kapitel Rn. 3; *Pieroth/Schlink/Kniesel* (Fn. 1), § 2 Rn. 8; *Schenke* (Fn. 13), Rn. 93; *Schoch* (Fn. 1), Rn. 9; *Tettinger/Erbguth/Mann* (Fn. 6), Rn. 531; *Würtenberger/Heckmann* (Fn. 14), Rn. 494; kritisch *Knemeyer* (Fn. 18), Rn. 129 f.

... abzuwehren“[38], jedoch bedeutet dies nicht, dass die Polizei in jedem Einzelfall eine Maßnahme zur Gefahrenabwehr durchführen muss. Vielmehr erfolgt hierdurch nur eine Aufgabenzuweisung zur Gefahrenabwehr[39]. Da dementsprechend i. d. R. keine Pflicht der Polizei, einzuschreiten, besteht[40], genießt die Polizei im Bereich der Aufgabe der Gefahrenabwehr einen Ermessensspielraum. Dieser bezieht sich sowohl auf die Frage, *ob* Maßnahmen zur Gefahrenabwehr ergriffen werden sollen (Entschließungsermessen), als auch auf die Frage, *wie* die Polizei die Gefahren abzuwehren gedenkt (Auswahlermessen)[41].

Die maßgebende Leitlinie des polizeilichen Ermessens besteht in einer möglichst optimalen Gefahrenabwehr[42], damit die polizeilichen Schutzgüter, also die öffentliche Sicherheit und Ordnung, effektiv gewährleistet werden[43]. Hier stellt sich die Frage: Was bedeutet eine effektive Gefahrenabwehr? Unstreitig ist, dass sich die Optimierung des Grundrechtschutzes als ein Hinweis für eine effektive Gefahrenabwehr betrachten lässt. Zweifelhaft ist jedoch, ob eine effektive Gefahrenabwehr vom ökonomischen Gesichtspunkt aus beurteilt werden darf. Es wird vertreten, dass die Wirtschaftlichkeit oder das fiskalische Interesse bei der Ausübung polizeilichen Ermessens zu berücksichtigen sei, da die Ressourcen für die Aufrechterhaltung der inneren Sicherheit begrenzt seien[44]. Außerdem müsse das finanzielle Interesse auch im Bereich der Gefahrenabwehr beachtet werden, wenn die Aufwendungen nach Einschätzung des Gesetzgebers „unzumutbar“ aufwendig seien[45]. Diese Auffassung ist allerdings unzutreffend. Nach § 40 VwVfG muss die Polizei das Ermessen entsprechend dem Zweck der Ermächtigung ausüben. Die Polizei- und Ordnungsgesetze, die der Gefahrenabwehr dienen, verfolgen keinen finanziellen Zweck. Deshalb ist die Berücksichtigung fiskalischer Gesichtspunkte bei der Ausübung des Ermessens im Bereich der Gefahrenabwehr unzulässig, da sie zu einem Ermessensmissbrauch führt[46]. Bei der polizeilichen „pflichtgemäßen“ Ermessensausübung ist das fiskalische Interesse nicht zu berücksichtigen, weil es keine Pflicht der Wirtschaftlichkeitserwägung gibt.

38 Z. B. § 1 Abs. 1 S. 1 bwPolG.

39 Vgl. *Schoch*, JuS 1994, S. 754.

40 *Pieroth/Schlink/Kniesel* (Fn. 1), § 10 Rn. 32.

41 *Götz* (Fn. 16), § 11 Rn. 2; *Gusy* (Fn. 14), Rn. 392; *Kugelmann* (Fn. 5), 8. Kapitel Rn. 7 ff.; *Pieroth/Schlink/Kniesel* (Fn. 1), § 10 Rn. 33; *Rachor*, in: Lisken/Denninger, HPolR, F Rn. 115; *Schenke* (Fn. 13), Rn. 94; *Schoch* (Fn. 39), S. 754 (755); *Tettinger/Erbguth/Mann* (Fn. 6), Rn. 532 ff.; *Waechter*, VerwArch 88 (1997), S. 298 (313); *Würtenberger/Heckmann* (Fn. 14), Rn. 494.

42 *Götz* (Fn. 16), § 11 Rn. 4.

43 *Waechter* (Fn. 41), S. 298 (327); *Würtenberger/Heckmann* (Fn. 14), Rn. 494.

44 *Würtenberger/Heckmann* (Fn. 14), Rn. 497.

45 *Peters*, DÖV 2001, S. 749 (761).

46 *Maurer*, AllgVerwR, § 7 Rn. 22; *Sachs*, in: Stelkens/Bonk/Sachs, VwVfG, § 40 Rn. 65.

Ermessensfehler im Gefahrenabwehrrecht sind gegeben, wenn eine Ermessensüberschreitung, ein Ermessensnichtgebrauch oder ein Ermessensmissbrauch vorliegt[47]. Aufgrund des Opportunitätsprinzips kann der Bürger einen Anspruch auf polizeiliches Einschreiten nur besitzen, wenn eine Ermessensreduzierung auf null besteht[48]. Ob die Voraussetzung der Ermessensreduzierung auf null erfüllt ist, hängt von der Wertigkeit der zu schützenden Rechtsgüter, der Intensität der Gefahr[49] sowie der Dringlichkeit[50] ab.

c) Rechtsschutz

Die Maßnahme, die die Polizei im Bereich der Gefahrenabwehr durchführt, stellt öffentlich-rechtliches Handeln nichtverfassungsrechtlicher Art dar. Gegen polizeiliche Maßnahmen der Gefahrenabwehr kann man mithin gemäß § 40 Abs. 1 VwGO das Verwaltungsgericht anrufen[51]. Insoweit steht der Verwaltungsrechtsweg für eine gefahrenabwehrrechtliche Streitigkeit offen.

II. Zugriff auf die Telekommunikation zur Gefahrenabwehr nach Polizei- und Ordnungsgesetzen

Nach der Differenzierung zwischen beiden Aufgaben der Polizei werden polizeiliche Befugnisse zur Telekommunikationsüberwachung in zwei Typen aufgeteilt. Der Bundesgesetzgeber lässt durch § 100a StPO die repressive Überwachung einer Telekommunikation zu. Die strafprozessrechtliche Telekommunikationsüberwachung dient repressiver Aufklärung einer begangenen Straftat. Ihre Voraussetzung ist der Verdacht einer verübten Straftat[52]. Hingegen wird die polizeirechtliche Telekommunikationsüber-

47 *Kugelmann* (Fn. 5), 8. Kapitel Rn. 13; *Pieroth/Schlink/Kniesel* (Fn. 1), § 10 Rn. 36; *Rachor* (Fn. 41), F Rn. 117; *Schenke* (Fn. 13), Rn. 95; *Schoch* (Fn. 1), Rn. 104; *Waechter* (Fn. 41), S. 298 (313 f.); *Würtenberger/Heckmann* (Fn. 14), Rn. 497. Zu drei unterschiedlichen Ermessensfehlergruppen *Detterbeck*, AllgVerwR, Rn. 328 ff.; *Hoffmann-Riem*, in: Hoffmann-Riem/Schmidt-Aßmann/Voßkuhle, GVwR, Bd. 1, § 10 Rn. 88; *J. Ipsen*, AllgVerwR, Rn. 536 ff.; *Kopp/Ramsauer*, VwVfG, § 40 Rn. 58 ff.; *Jestaedt*, in: Erichsen/Ehlers, AllgVerwR, § 10 Rn. 61; *Maurer* (Fn. 46), § 7 Rn. 19 ff.; *Peine*, AllgVerwR, Rn. 216 ff.; *Ziekow*, VwVfG, § 40 Rn. 39 ff.

48 *Gusy* (Fn. 14), Rn. 394; *Kugelmann* (Fn. 5), 8. Kapitel Rn. 22; *Pieroth/Schlink/Kniesel* (Fn. 1), § 10 Rn. 45; *Schenke* (Fn. 13), Rn. 104; *Schoch* (Fn. 1), Rn. 115; *Tettinger/Erbguth/Mann* (Fn. 6), Rn. 532; *Würtenberger/Heckmann* (Fn. 14), Rn. 499.

49 *Götz* (Fn. 16), § 11 Rn. 6; *Gusy* (Fn. 14), Rn. 393; *Kugelmann* (Fn. 5), 8. Kapitel Rn. 13; *Maurer* (Fn. 46), § 7 Rn. 24; *Peine* (Fn. 47), Rn. 224; *Rachor* (Fn. 41), F Rn. 134; *Schenke* (Fn. 13), Rn. 100; *Schoch* (Fn. 1), Rn. 110; *Waechter* (Fn. 41), S. 298 (313); *Ziekow* (Fn. 47), § 40 Rn. 35.

50 *Pieroth/Schlink/Kniesel* (Fn. 1), § 10 Rn. 41.

51 *Götz* (Fn. 16), § 19 Rn. 2; *Gusy* (Fn. 14), Rn. 483; *Pieroth/Schlink/Kniesel* (Fn. 1), § 2 Rn. 14; *Schoch* (Fn. 21), S. 628 (629); *Würtenberger/Heckmann* (Fn. 14), Rn. 178.

52 Zur repressiven Telekommunikationsüberwachung *Bär*, MMR 2000, S. 472 ff.; *Dorsch*, Effizienz der Überwachung der Telekommunikation; *Günther*, NStZ 2005, S. 485 ff.; *Krüpe-Gescher*, Überwachung der Telekommunikation; *Meininghaus*, Zugriff auf E-Mails, S. 59 ff.;

wachung, die als eine neue polizeiliche informationelle Standardmaßnahme[53] eingefügt wurde, zur präventiven Aufklärung potenziell gefährlicher Sachverhalte durchgeführt. In allen polizei- und ordnungsgesetzlichen Ermächtigungsvorschriften zur Telekommunikationsüberwachung wird ausdrücklich gefordert, dass diese verdeckte Maßnahme der Gefahrenabwehr dienen muss. Deswegen geht die polizeirechtliche Telekommunikationsüberwachung, die eine neue heimliche polizeiliche Standardmaßnahme der Informationserhebung[54] darstellt, von einer zukunftsgerichteten Prognose aus[55]. Die Telekommunikationsüberwachung nach den Polizei- und Ordnungsgesetzen setzt keinen Verdacht einer begangenen Straftat, sondern eine Gefahr im Sinne des Polizeirechts voraus.

B. Vorbeugende Straftatenbekämpfung als Zweck der Ermächtigungsvorschriften zur präventiv-polizeilichen Telekommunikationsüberwachung

Über die Gefahrenabwehr hinaus verfolgen einige polizei- und ordnungsgesetzliche Ermächtigungsvorschriften zur Telekommunikationsüberwachung auch dem Zweck der vorbeugenden Straftatenbekämpfung[56]. Diese Zielsetzung bezieht sich auf zukünftig mögliche Straftaten. Falls sie realisiert werden, geht es um die Strafverfolgung. Davon ausgehend stellt sich eine Frage: Überschreitet die in Polizei- und Ordnungsgesetzen vorgeschriebene Telekommunikationsüberwachung, die der vorbeugenden Straftatenbekämpfung dient, die Grenze zum Bereich der Strafverfolgung? Da man unter der vorbeugenden Straftatenbekämpfung – nach der Zuwei-

Puschke/Singelnstein, NJW 2008, S. 113 ff.; *Störing*, Strafprozessuale Zugriffsmöglichkeiten; zum Vergleich der repressiven mit der präventiv-polizeilichen Telekommunikationsüberwachung *C. Sievers*, Telekommunikationsüberwachung, S. 105 ff.

53 Die informationellen Standardmaßnahmen wurden – als eine Reaktion auf das Volkszählungsurteil des Bundesverfassungsgerichts vom 15. 12. 1983 (BVerfGE 65, 1 ff.) – seit Ende der 1980er Jahre in allen Bundesländern geschaffen (vgl. *Koch*, Datenerhebung, S. 39 f.; weitere Nachweise bei *Tettinger/Erbguth/Mann* (Fn. 6), Rn. 430).

54 Unter den informationellen Standardmaßnahmen werden sowohl Standardmaßnahmen der Informationserhebung als auch Standardmaßnahmen der Informationsverarbeitung verstanden (*Schoch* (Fn. 3), Rn. 194). Die Standardmaßnahmen der Informationserhebung können weiter zwischen Maßnahmen der offenen Informationserhebung und Maßnahmen der verdeckten Informationserhebung untergliedert werden (*Erichsen*, JURA 1993, S. 45). In einigen Polizei- und Ordnungsgesetzen ist der Terminus „Informationsverarbeitung" der Oberbegriff für Informationserhebung, Informationsspeicherung, Informationsveränderung, Informationsnutzung und Informationsübermittlung (vgl. z. B. §§ 27–36k bremPolG; §§ 25–40 saarlPolG).

55 Vgl. *Gusy* (Fn. 2), S. 61 (63).

56 § 23a Abs. 1 S. 1 Nr. 2 bwPolG; Art. 34a Abs. 1 S. 1 Nr. 2 bayPAG; § 33b Abs. 2 S. 2 bbgPolG; § 28b Abs. 1 S. 1 Nr. 2 saarlPolG; § 34a Abs. 3 S. 1 Nr. 2 thürPAG.

sungsnorm der polizeilichen Aufgaben im positiven Recht[57] – sowohl die Verhütung von Straftaten als auch die Vorsorge für die Verhütung und Verfolgung künftiger Straftaten versteht[58], unterscheidet folgende Erörterung diese beiden Konstellationen.

I. Verhütung von Straftaten

Heutzutage erschöpft sich die Gefahrenabwehr nicht in der Verhinderung der bereits vorliegenden konkreten Gefahren (klassische Gefahrenabwehr)[59]. Vielmehr besteht die Polizeiaufgabe der Gefahrenabwehr auch im Vorfeld konkreter Gefahren, andernfalls kommt die gefahrenabwehrrechtliche Maßnahme zur Gefahrenabwehr bei heimlicher und vorsätzlicher Gefahrenverursachung stets zu spät[60]. Daraus lässt sich der Schluss ziehen, dass die Gefahrenvorsorge (= die Beseitigung der Gefahrenursachen bzw. die Verhinderung der zukünftigen konkreten Gefahren)[61] in den Bereich der Gefahrenabwehr fällt[62].

Nicht zu leugnen ist, dass sich Gefahren, die sich aus menschlichem Verhalten ergeben, immer wieder zu Straftaten entwickeln. Die Einschätzung, dass sich die Straftatenverhütung als Teil der Gefahrenabwehr ansehen lässt, entspricht insoweit dem Charakter des Gefahrenabwehrrechts. Denn die Straftatenverhütung verhindert die Verletzung des Strafrechts[63], die die

57 Vgl. dazu *Rachor* (Fn. 41), F Rn. 163.

58 *Albers*, Determination polizeilicher Tätigkeit, S. 116 ff.; *Götz* (Fn. 16), § 17 Rn. 21; *Pieroth/Schlink/Kniesel* (Fn. 1), § 5 Rn. 1; *Rachor* (Fn. 41), F Rn. 163; *Schoch* (Fn. 1), Rn. 12. In einigen Polizei- und Ordnungsgesetzen beschränkt sich die vorbeugende Bekämpfung von Straftaten auf die Verhütung von Straftaten (Nachweise bei *Pieroth/Schlink/Kniesel* (Fn. 1), § 5 Rn. 1 mit Fn. 4). Das Bundesverfassungsgericht trennt die Strafverfolgungsvorsorge von der vorbeugenden Straftatenbekämpfung (BVerfGE 113, 348 (369)).

59 *Schoch*, Der Staat 43 (2004), S. 347 (352).

60 *Waechter*, JZ 2002, S. 854 (855).

61 Im Schrifttum wird vertreten, dass die Gefahrenvorsorge mit dem Begriff der abstrakten Gefahren gleichzusetzen sei (vgl. *Germann*, Gefahrenabwehr und Strafverfolgung, S. 244, 251; *Pieroth/Schlink/Kniesel* (Fn. 1), § 15 Rn. 19). Dem ist nicht zuzustimmen. Der Begriff der abstrakten Gefahr bezieht sich auf eine hinreichende Wahrscheinlichkeit des Schadenseintritts. Demgegenüber betrifft die Gefahrenvorsorge nur eine geringere hinreichende Wahrscheinlichkeit des Schadenseintritts (vgl. *Knemeyer* (Fn. 18), Rn. 72; *Möstl*, JURA 2005, S. 48 (51); *Schenke* (Fn. 13), Rn. 71 mit Fn. 114). Dabei geht es nur um Gefahrenursachen, nicht aber um Gefahren. Aus diesem Grund ist die – sich wohl an Art. 2 Abs. 1 bayPAG anlehnende – Auffassung, dass sich die Gefahrenvorsorge auf eine „allgemeine Gefahr" bzw. „allgemein bestehende Gefahr" erstreckt (vgl. *Denninger* (Fn. 6), E Rn. 45; *Knemeyer* (Fn. 18), Rn. 72; *Schenke* (Fn. 13), Rn. 71), abzulehnen.

62 *Kugelmann* (Fn. 5), 4. Kapitel Rn. 148 f.; *Schenke* (Fn. 13), Rn. 71; *Trute*, in: Erbguth/Müller/Neumann, GS Jeand'Heur, S. 403; *Waechter* (Fn. 60), S. 854 (855); a. A. *Knemeyer*, in: Arndt/Knemeyer/Kugelmann/Meng/Schweitzer, FS Rudolf, S. 483 (490): Die Gefahrenvorsorge kann nur als eigenständige neuformulierte dritte polizeiliche Aufgabe angesehen werden.

63 *Kugelmann* (Fn. 5), 4. Kapitel Rn. 156.

Unverletzlichkeit der Rechtsordnung, also öffentliche Sicherheit (= Schutzgut der Polizei), betrifft. Insoweit stellt die Verhütung der sich später möglicherweise realisierenden, aber derzeitig noch nicht vorliegenden Straftaten eine Gefahrenvorsorge dar[64]. Unter dem Aspekt des Gefahrenabwehrrechts dient die Straftatenverhütung auch dem Zweck, die Gefahrenursachen zu beseitigen oder noch nicht vorliegende Gefahr zu verhindern. Folglich wird die Straftatenverhütung der Gefahrenabwehr zugerechnet[65].

II. Vorsorge für die Verfolgung künftiger Straftaten

Im Gegensatz zur Straftatenverhütung ist die Zuordnung der Vorsorge für die Verfolgung künftiger Straftaten äußerst umstritten. Die Vorsorge für die Verfolgung künftiger Straftaten betrifft die polizeilichen Maßnahmen, die der zukünftigen Durchführung der Strafverfolgung in Bezug auf mögliche spätere bzw. später bekannt werdende Straftaten dienen[66]. Dadurch lassen sich die künftigen strafprozessualen Ermittlungen oder Aufklärungen ermöglichen oder erleichtern[67]. Insoweit erfolgt die Verfolgungsvorsorge in zeitlicher Hinsicht präventiv, betrifft aber gegenständlich das repressiv ausgerichtete Strafverfahren[68].

Durch seine Entscheidung vom 27. 7. 2005 erklärte das Bundesverfassungsgericht, dass die Vorsorge für die Verfolgung noch nicht begangener, sondern in ungewisser Zukunft bevorstehender Straftaten zum gerichtlichen Verfahren gehöre. Von der in Art. 74 Abs. 1 Nr. 1 GG normierten konkurrierenden Gesetzgebung zur Strafverfolgung habe der Bundesgesetzgeber im Bereich der Telekommunikationsüberwachung abschließend Gebrauch gemacht, sodass die Länder gemäß Art. 72 Abs. 1 GG von der Gesetzgebung ausgeschlossen seien[69].

Demgegenüber vertrat das Bundesverwaltungsgericht früher die Ansicht, dass die Maßnahme der Strafverfolgungsvorsorge keine Maßnahme auf dem Gebiet des Strafprozesses darstelle[70], sondern dem Bereich der Gefahren-

64 *Schenke* (Fn. 13), Rn. 10; a. A. *Knemeyer* (Fn. 62), S. 483 (490): Die Gefahrenvorsorge und die Straftatenverhütung sind unterschiedliche Kategorien polizeilicher Aufgaben.

65 BVerfGE 113, 348 (368); *Degenhart* (Fn. 9), Art. 74 Rn. 27; *Denninger* (Fn. 6), E Rn. 199; *Götz* (Fn. 16), § 17 Rn. 21 f.; *Knemeyer* (Fn. 62), S. 483 (490); *Kugelmann* (Fn. 5), 4. Kapitel Rn. 156; *Kutscha*, NVwZ 2005, S. 1231 (1233); *Paeffgen*, JZ 1991, S. 437 (443); *Pieroth* (Fn. 8), Art. 74 Rn. 9; *Pieroth/Schlink/Kniesel* (Fn. 1), § 5 Rn. 2; *Schenke* (Fn. 13), Rn. 10; *Schoch* (Fn. 1), Rn. 14; *Son*, Heimliche polizeiliche Eingriffe, S. 105; *Würtenberger/Heckmann* (Fn. 14), Rn. 178.

66 *Schenke* (Fn. 13), Rn. 11.

67 Vgl. BVerwGE 26, 169 (170); *Gusy* (Fn. 14), Rn. 199; *Rachor* (Fn. 41), F Rn. 165; *Tischer*, System der informationellen Befugnisse, S. 60; *Würtenberger/Heckmann* (Fn. 14), Rn. 181.

68 BVerfGE 113, 348 (370).

69 BVerfGE 113, 348 (369 f.).

70 BVerwGE 26, 169 (170).

abwehr zuzuordnen sei[71]. Diese Ansicht wurde in einem jüngeren Urteil[72] aufgegeben. In seiner Entscheidung vom 23. 11. 2005 unterschied es zunächst – wie in seinem älteren Urteil – die Strafverfolgungsvorsorge von der Strafverfolgung[73]. Sodann erklärte es, dass die Gesetzgebungskompetenz des Bundes zur Vorsorge für die Verfolgung der Straftaten unmittelbar der Befugnis für die konkurrierende Gesetzgebung in Art. 74 Abs. 1 Nr. 1 GG zu entnehmen sei, weil die dortige Zuständigkeitsbeschreibung für „das Strafrecht und den Strafvollzug" sowie das „gerichtliche Verfahren" keine Einschränkung dahingehend enthalte, dass Maßnahmen, die sich auf zukünftige Strafverfahren bezögen, von der Zuweisung der konkurrierenden Gesetzgebungskompetenz nicht erfasst sein sollten[74]. Falls die StPO jedoch keine Regelung über die Zuständigkeit der Polizei für Maßnahmen der Strafverfolgungsvorsorge enthalte, beurteile sich die Zuständigkeit für polizeiliche Maßnahmen der Strafverfolgungsvorsorge nach den Polizei- und Ordnungsgesetzen der Länder[75].

Bundesverwaltungsgericht und Bundesverfassungsgericht sind sich in der Frage, aus welcher grundgesetzlichen Vorschrift die Gesetzgebungskompetenz zur Strafverfolgungsvorsorge hergeleitet wird, einig. Nach der Auffassung der beiden Bundesgerichte entspreche die Strafverfolgungsvorsorge dem Begriff des gerichtlichen Verfahrens im Sinne des Art. 74 Abs. 1 Nr. 1 GG. Folglich falle die Strafverfolgungsvorsorge nicht in den Bereich der Gefahrenabwehr, die keinen Gegenstand konkurrierender Gesetzgebung (Art. 74 GG) darstelle. Ob die Länder die Gesetzgebungskompetenz für bestimmte polizeiliche Maßnahmen (z. B. Telekommunikationsüberwachung) im Bereich der Strafverfolgungsvorsorge besitzen könnten, hänge davon ab, ob der Bundesgesetzgeber von dieser Kompetenz bereits abschließend Gebrach gemacht habe[76]. Zur Frage, ob die Strafverfolgungsvorsorge der Strafverfolgung zugeordnet wird, vertreten die beiden Bundesgerichte allerdings unterschiedliche Meinungen[77]. Das Bundesverfassungsgericht vertritt, dass die Gesetzgebungskompetenz der Länder im Bereich der Telekommunikationsüberwachung zur Verfolgungsvorsorge ausgeschlossen sei, weil der Bundesgesetzgeber von der in Art. 74 Abs. 1 Nr. 1 GG normierten konkurrierenden Gesetzgebung zur „Strafverfolgung" im Bereich der Telekommunikationsüberwachung abschließend Gebrauch gemacht habe[78]. Die Strafverfolgungsvorsorge falle deswegen in den Bereich der Strafverfol-

71 BVerwG NJW 1990, S. 2765 (2766 f.).
72 BVerwG NJW 2006, S. 1225 ff.
73 BVerwG NJW 2006, S. 1225 (1226).
74 BVerwG NJW 2006, S. 1225 (1226).
75 BVerwG NJW 2006, S. 1225 (1226).
76 BVerfGE 113, 348 (369 ff.); BVerwG NJW 2006, S. 1225 (1226).
77 A. A. *W.-R. Schenke*, JZ 2006, S. 707 (708).
78 BVerfGE 113, 348 (369 f.).

gung. Anders als das Bundesverfassungsgericht trennt das Bundesverwaltungsgericht die Strafverfolgungsvorsorge von der Strafverfolgung[79]. Nach dem Urteil des Bundesverwaltungsgerichts bestimmt die StPO eine Zuständigkeit der Behörden und Beamten des Polizeidienstes lediglich für die Strafverfolgung. Sie enthalte aber keine Regelung über die Zuständigkeit für Maßnahmen der Strafverfolgungsvorsorge[80]. Zwar entspreche die Strafverfolgungsvorsorge dem Begriff des gerichtlichen Verfahrens im Sinne des Art. 74 Abs. 1 Nr. 1 GG, sie lasse sich jedoch als eine „Verwaltungsaufgabe" der Polizei ansehen, falls sie nach Art. 72 Abs. 1 GG in Polizei- und Ordnungsgesetzen der Länder geregelt werde[81]. Insoweit betrachtet das Bundesverwaltungsgericht die Strafverfolgungsvorsorge als eine neue dritte Kategorie der Polizeiaufgaben. Sie gehöre weder zur Strafverfolgung noch zur Gefahrenabwehr.

Die Frage nach der Zuordnung der Strafverfolgungsvorsorge wird im Schrifttum uneinheitlich beantwortet. Es wird vertreten, dass die Strafverfolgungsvorsorge wegen ihrer Zielrichtung der Strafverfolgung zuzurechnen sei[82]. Mithin stelle die Strafverfolgungsvorsorge einen Gegenstand konkurrierender Gesetzgebung des Art. 74 Abs. 1 Nr. 1 GG (gerichtliches Verfahren) dar[83]. Nach Art. 72 Abs. 1 GG sei die Landesgesetzgebungskompetenz zur Strafverfolgungsvorsorge eröffnet, soweit es bundesrechtliche Lücken in diesem Bereich gebe[84]. Die Gegner dieser Ansicht stehen jedoch auf dem Standpunkt, dass die Strafverfolgungsvorsorge nicht der Strafverfolgung zuzuordnen sei, weil der Strafprozess die Straftat voraussetze und nach der Straftat einsetze[85]. Die Strafverfolgungsvorsorge entspreche dem Begriff des gerichtlichen Verfahrens in Art. 74 Abs. 1 Nr. 1 GG nicht[86]. Ausgehend von der Ansicht, dass die Strafverfolgungsvorsorge nicht der Strafverfolgung zuzurechnen sei, sind zwei Untermeinungen zu unterscheiden. Nach der ersten Untermeinung soll die Strafverfolgungsvorsorge der Gefah-

79 BVerwG NJW 2006, S. 1225 (1226).

80 BVerwG NJW 2006, S. 1225 (1226).

81 BVerwG NJW 2006, S. 1225 (1226).

82 So *Eisenberg/Puschke*, JZ 2006, S. 729 (730); *Germann* (Fn. 61), S. 256 f.; *Kugelmann* (Fn. 5), 4. Kapitel Rn. 162; *Kutscha* (Fn. 65), S. 1231 (1233); *Rachor* (Fn. 41), F Rn. 167; *Schenke* (Fn. 13), Rn. 11; *Siebrecht*, JZ 1996, S. 711 (713); *Son* (Fn. 65), S. 108; *Stephan*, VBlBW 2005, S. 410 f.; *Tischer* (Fn. 67), S. 60 f.; *Waechter*, DÖV 1999, S. 138 (140).

83 *Degenhart* (Fn. 9), Art. 74 Rn. 27; *Eisenberg/Puschke* (Fn. 82), S. 729 (730); *Kutscha* (Fn. 65), S. 1231 (1233); *Pieroth* (Fn. 8), Art. 74 Rn. 9; *Schenke* (Fn. 13), Rn. 30; *Siebrecht* (Fn. 82), S. 711 (713); *Son* (Fn. 65), S. 109; *Stephan* (Fn. 82), S. 410 (411); *Tischer* (Fn. 67), S. 62 f.

84 *Einsenberg/Puschke* (Fn. 82), S. 729 (730); *Schenke* (Fn. 13), Rn. 12; *Son* (Fn. 65), S. 109.

85 So *Kastner*, VerwArch 92 (2001), S. 216 (236); *Paeffgen* (Fn. 65), S. 437 (442); *Pieroth/Schlink/Kniesel* (Fn. 1), § 5 Rn. 6; *Schoch* (Fn. 1), Rn. 17.

86 *Schoch* (Fn. 1), Rn. 17.

renabwehr zuzuordnen sein[87]. Der Landesgesetzgeber besitze gemäß Art. 70 Abs. 1 GG die Gesetzgebungskompetenz zur Strafverfolgungsvorsorge[88]. Gemäß der zweiten Untermeinung wird die Strafverfolgung als eigenständige dritte Aufgabenkategorie der Polizei angesehen[89]. Die Frage, wie die Gesetzgebungskompetenz für diese eigenständige dritte Kategorie der Polizeiaufgaben verteilt wird, ist jedoch unklar[90].

Welche Meinung ist nun richtig? Berücksichtigt man, dass jede in die Grundrechte eingreifende polizeiliche Maßnahme die Prüfung des Verhältnismäßigkeitsgrundsatzes bestehen muss, ist die Auffassung, dass die Strafverfolgungsvorsorge der Strafverfolgung zuzuordnen ist, zutreffend. Wie bereits dargelegt wurde, liegt der Ausgangspunkt der Strafverfolgungsvorsorge darin, die künftigen strafprozessualen Ermittlungen oder Aufklärungen zu ermöglichen oder zu erleichtern. Da die Strafverfolgungsvorsorge der späteren Identifizierung des Straftäters dient, geht es bei der Strafverfolgungsvorsorge um die Situation, in der die Verletzung des Strafrechts (in Zukunft) realisiert und nicht mehr präventiv verhindert wird. Deswegen lässt sich die Strafverfolgungsvorsorge nicht als Gefahrenabwehr kategorisieren.

III. Vorbeugende Straftatenbekämpfung als Teil der Gefahrenabwehr

Es wird erwartet, dass die Gefahrenursache im Vorfeld der Gefahr durch die polizeilichen informationellen Standardmaßnahmen aufgeklärt werden kann. In diesem Zusammenhang ist polizeiliche Informationserhebung von bemerkenswerter Bedeutung für die Gefahrenvorsorge[91]. Vor allem liegt in der präventiv-polizeilichen Telekommunikationsüberwachung, die in Baden-Württemberg, Bayern, Brandenburg, Saarland und Thüringen zur vorbeugenden Straftatenbekämpfung im Vorfeld der Gefahr durchgeführt werden darf, eine Vorverlagerung polizeilicher Tätigkeiten. Die in den Polizei- und Ordnungsgesetzen ermöglichte Vorverlagerung von polizeilichen Tätigkeiten, die in der polizeilichen Informationsvorsorge zum Ausdruck kommt[92], ist Bestandteil der Gefahrenvorsorge (= Verhütung von Strafta-

87 So *Deutsch*, Erhebung von Informationen, S. 190 f.; *Kastner* (Fn. 85), S. 216 (236); *Knemeyer* (Fn. 18), Rn. 71; *Pieroth/Schlink/Kniesel* (Fn. 1), § 5 Rn. 6; *Schoch* (Fn. 1), Rn. 17.

88 *Deutsch* (Fn. 87), S. 190 f.; *Pieroth/Schlink/Kniesel* (Fn. 1), § 5 Rn. 6; *Schoch* (Fn. 1), Rn. 17.

89 So *Albers* (Fn. 58), S. 359 ff.

90 *West*, Fingerabdruck, S. 132.

91 Vgl. *Knemeyer* (Fn. 18), Rn. 72; *Kugelmann* (Fn. 5), 4. Kapitel Rn. 153; *Tettinger/Erbguth/Mann* (Fn. 6), Rn. 425; *Würtenberger/Heckmann* (Fn. 14), Rn. 179.

92 Die polizeiliche Informationsvorsorge stellt eine Konsequenz der Vorverlagerung polizeilicher Tätigkeiten dar (vgl. dazu *Schoch* (Fn. 59), S. 347 (353 f.)).

ten)[93]. Die vorbeugende Straftatenbekämpfung, die in Baden-Württemberg, Bayern, Brandenburg, Saarland und Thüringen als ein Ziel der in den Polizei- und Ordnungsgesetzen vorgeschriebenen Telekommunikationsüberwachung angesehen wird, bezieht sich nicht auf die Strafverfolgungsvorsorge, sondern nur auf die Straftatenverhütung, weil die Strafverfolgungsvorsorge der Strafverfolgung zuzuordnen ist. Daraus ergibt sich die Konsequenz: Die vorbeugende Straftatenbekämpfung ist Teil der Gefahrenabwehr. Eine präventiv-polizeiliche Telekommunikationsüberwachung, die durch Informationsvorsorge der vorbeugenden Straftatenbekämpfung dient, überschreitet die Grenze zur Strafverfolgung nicht.

C. Zusammenfassung des 3. Kapitels

Alle polizei- und ordnungsgesetzlichen Ermächtigungsvorschriften zur Telekommunikationsüberwachung regeln, dass diese verdeckte polizeiliche Maßnahme der Informationserhebung zum Zweck der (klassischen) Gefahrenabwehr durchgeführt werden kann. In Baden-Württemberg, Bayern, Brandenburg, Saarland und Thüringen darf die Polizei auch zur vorbeugenden Straftatenbekämpfung im Vorfeld der Gefahr eine Telekommunikation überwachen. Der in den Polizei- und Ordnungsgesetzen verwendete Begriff der vorbeugenden Straftatenbekämpfung bezieht sich nicht auf die Strafverfolgungsvorsorge, weil die Strafverfolgungsvorsorge der Strafverfolgung zuzuordnen ist. Da die vorbeugende Straftatenbekämpfung nur die Gefahrenvorsorge (= Verhütung von Straftaten) betrifft, ist die präventiv-polizeiliche Telekommunikationsüberwachung, die zur vorbeugenden Straftatenbekämpfung im Vorfeld der Gefahr durchgeführt wird, auch eine Maßnahme, die in den Bereich der Gefahrenabwehr fällt.

93 Zum Verhältnis zwischen der Gefahrenvorsorge und polizeilicher Informationsvorsorge *Aulehner*, Informationsvorsorge, S. 48: Die polizeiliche Informationsvorsorge ist Teil der polizeilichen Gefahrenvorsorge.

4. Kapitel: Grundrechtliche Relevanz der präventiv-polizeilichen E-Mail-Überwachung

Die präventiv-polizeiliche E-Mail-Überwachung, die in den meisten Bundesländern eine ausdrückliche Rechtsgrundlage findet, wirft Grundrechtsfragen auf.

Die Grundrechte der Telekommunikationsteilnehmer, in die durch präventiv-polizeiliche E-Mail-Überwachung eingegriffen werden, lassen sich unter drei Gesichtspunkten untersuchen. Zuerst beeinträchtigt die präventiv-polizeiliche Überwachung eines E-Mail-Verkehrs die Vertraulichkeit der Telekommunikation. Dabei geht es um den Schutzbereich des Art. 10 Abs. 1 GG. Zweitens kann die Polizei durch präventive E-Mail-Überwachung personenbezogene Daten erheben. Dabei handelt es sich um das Grundrecht auf informationelle Selbstbestimmung. Drittens stellt die präventiv-polizeiliche E-Mail-Überwachung eine heimliche Infiltration des informationstechnischen Systems (Internets) dar. Hierbei ist das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme, also das sogenannte „Computergrundrecht“[1], das das Bundesverfassungsgericht in seinem Urteil vom 27. 2. 2008[2] entwickelt hat, in Betracht zu ziehen.

Zu beachten ist, dass die präventiv-polizeiliche E-Mail-Überwachung nicht nur in Grundrechte der Telekommunikationsteilnehmer eingreift. Der Eingriff in Grundrechte der Diensteanbieter, der sich aus der Durchführung präventiv-polizeilicher E-Mail-Überwachung herleitet, muss ebenfalls berücksichtigt werden[3]. Bei der Durchführung einer präventiv-polizeilichen E-Mail-Überwachung haben E-Mail-Provider nach den Polizei- und Ordnungsgesetzen eine Mitwirkungspflicht. In dieser Hinsicht wird die Berufsfreiheit (Art. 12 Abs. 1 GG) der E-Mail-Provider betroffen. Denn gemäß den polizei- und ordnungsgesetzlichen Regelungen über die Mitwirkungspflicht der Diensteanbieter müssen sich die E-Mail-Provider an einer Durchführung der präventiv-polizeilichen E-Mail-Überwachung beteiligen. Diese Vorschriften beziehen sich auf das Wie der Berufstätigkeit der Dienstanbieter.

---

1 So wörtlich *Hufen*, Grundrechte, § 12 Rn. 5; *J. Ipsen*, Grundrechte, Rn. 325a; *Künast*, NJW 2009, S. 1723 (1724); *Kutscha*, LKV 2008, S. 481 (484); *Manssen*, Grundrechte, Rn. 225.

2 BVerfGE 120, 274 ff.

3 *R. P. Schenke*, AöR 125 (2000), S. 1 (37).

A. Eingriff in Grundrechte der Telekommunikationsteilnehmer

I. Schutz der E-Mail-Übertragung durch Art. 10 Abs. 1 GG

1. Schutzbereich des Art. 10 Abs. 1 GG

Art. 10 Abs. 1 GG schützt die Vertraulichkeit individueller Kommunikationen, „die wegen der räumlichen Distanz zwischen den Beteiligten auf Übermittlung durch Dritte angewiesen sind“[4]. Dabei handelt es sich um drei Garantien: Brief-, Post- und Fernmeldegeheimnis. Die Schutzbereiche dieser drei Garantien stehen selbstständig nebeneinander[5]. Aus diesem Grund bezieht sich die Gewährleistung des Art. 10 Abs. 1 GG auf drei unterschiedliche Grundrechte[6]. Die Auffassung, dass Art. 10 Abs. 1 GG wegen der Abgrenzungsschwierigkeit ein einheitliches Grundrecht darstelle[7], ist unhaltbar. Denn wenn man Abgrenzungsschwierigkeiten anerkennt, setzt dies logisch die Möglichkeit einer Abgrenzung voraus. Aus der Abgrenzungsschwierigkeit kann man nur die Folgerung ableiten, dass Art. 10 Abs. 1 GG kein einheitliches Grundrecht, sondern drei unterschiedliche Grundrechte enthält.

a) Briefgeheimnis

Art. 10 Abs. 1 GG schützt zunächst das Briefgeheimnis. Unter dem Begriff des Briefs in Art. 10 Abs. 1 GG wird die individuelle[8] schriftliche Mitteilung verstanden[9]. Ob eine solche Mitteilung verschlossen ist, spielt für den grundrechtlichen Schutz des Briefgeheimnisses keine Rolle[10]. Deswe-

4 BVerfGE 85, 386 (396).

5 *Gusy*, in: von Mangoldt/Klein/Starck, GG, Bd. 1, Art. 10 Rn. 25; *Sachs*, Grundrechte, B10 Rn. 3.

6 *Hermes*, in: Dreier, GG, Bd. 1, Art. 10 Rn. 25; *Löwer*, in: von Münch/Kunig, GG, Bd. 1, Art. 10 Rn. 11; *Manssen* (Fn. 1), Rn. 524; *Stern*, in: Stern, Staatsrecht, Bd. IV/1, S. 220; a. A. *Hufen* (Fn. 1), § 17 Rn. 4; *Jarass*, in: Jarass/Pieroth, GG, Art. 10 Rn. 1: ein einheitliches Grundrecht.

7 So *Jarass* (Fn. 6), Art. 10 Rn. 1.

8 A. A. *Michael/Morlok*, Grundrechte, Rn. 322.

9 Vgl. *Epping*, Grundrechte, Rn. 680; *Hermes* (Fn. 6), Art. 10 Rn. 30; *Ipsen* (Fn. 1), Rn. 302; *Manssen* (Fn. 1), Rn. 526; *Pagenkopf*, in: Sachs, GG, Art. 10 Rn. 12; *Pieroth/Schlink*, Grundrechte, Rn. 829.

10 Vgl. *Baldus*, in: Epping/Hillgruber, GG, Art. 10 Rn. 3; *Gusy* (Fn. 5), Art. 10 Rn. 27; *Hermes* (Fn. 6), Art. 10 Rn. 31; *Ipsen* (Fn. 1), Rn. 302; *Jarass* (Fn. 6), Art. 10 Rn. 3; *Löwer* (Fn. 6), Art. 10 Rn. 16; *Schmitt Glaeser*, in: Isensee/Kirchhof, HStR, Bd. 6, 2. Aufl., § 129 Rn. 62; *Sodan*, in: Sodan, GG, Art. 10 Rn. 3; *Stern* (Fn. 6), S. 220; a. A. *Groß*, JZ 1999, S. 326 (332); *Hömig*, in: Hömig, GG, Art. 10 Rn. 4; *Hufen* (Fn. 1), § 17 Rn. 5; *Manssen* (Fn. 1), Rn. 526; *Pagenkopf* (Fn. 9), Art. 10 Rn. 12.

gen können offene Sendungen, wie etwa Postkarten, dem Begriff des Briefs im Sinne des Art. 10 Abs. 1 GG entsprechen[11].

Bei der Gewährleistung des Briefgeheimnisses geht es um den Schutz vor der Kenntnisnahme des Briefsinhalts[12]. Darüber hinaus erstreckt sich die Garantie des Briefgeheimnisses auch auf „die mit der Briefsendung notwendigerweise anfallenden Daten“[13] wie etwa Absender, Empfänger und die Umstände der Beförderung[14]. Zeitlich wirkt die Garantie des Briefgeheimnisses, „sobald der Absender den Brief aus der Hand gegeben hat, bis der Empfänger den Brief erhalten hat“[15].

b) Postgeheimnis

Die Abgrenzung des Postgeheimnisses vom Briefgeheimnis besteht darin, dass sich die Garantie des Postgeheimnisses auf alle von der Post körperlich übermittelten Sendungen bezieht[16]. Ob die Sendung inhaltlich eine individuelle Mitteilung darstellt, ist für die Gewährleistung des Postgeheimnisses irrelevant[17]. Insoweit können Zeitungen, Warenproben, Werbemitteilungen in den Schutzbereich des Postgeheimnisses fallen[18]. In zeitlicher Hinsicht wirkt die Garantie des Postgeheimnisses von der Einlieferung bei der Post bis zur Ablieferung beim Empfänger[19].

Früher war der Grundrechtsadressat des Postgeheimnisses die staatliche Postverwaltung und sonstige postfremde Exekutive[20]. Nach der Privatisierung der Deutschen Post ist an deren Stelle die Deutsche Post AG, eine

11 *Gusy* (Fn. 5), Art. 10 Rn. 27; *Hermes* (Fn. 6), Art. 10 Rn. 31; *Hofmann*, in: Schmidt-Bleibtreu/Hofmann/Hopfauf, GG, Art. 10 Rn. 7; *Jarass* (Fn. 6), Art. 10 Rn. 3; *Löwer* (Fn. 6), Art. 10 Rn. 16; *Pieroth/Schlink* (Fn. 9), Rn. 830; *Stern* (Fn. 6), S. 220; *Sodan* (Fn. 10), Art. 10 Rn. 3.

12 BVerfGE 33, 1 (11); 67, 157 (171); *Epping* (Fn. 9), Rn. 680; *Gusy* (Fn. 5), Art. 10 Rn. 30; *Hermes* (Fn. 6), Art. 10 Rn. 31; *Hömig* (Fn. 10), Art. 10 Rn. 4; *Pagenkopf* (Fn. 9), Art. 10 Rn. 12; *Pieroth/Schlink* (Fn. 9), Rn. 829; *Schmitt Glaeser* (Fn. 10), § 129 Rn. 62; *Sodan* (Fn. 10), Art. 10 Rn. 3.

13 *Epping* (Fn. 9), Rn. 680.

14 *Epping* (Fn. 9), Rn. 680; *Gusy* (Fn. 5), Art. 10 Rn. 30; *Hermes* (Fn. 6), Art. 10 Rn. 31; *Pagenkopf* (Fn. 9), Art. 10 Rn. 12; *Pieroth/Schlink* (Fn. 9), Rn. 831; *Stern* (Fn. 6), S. 221.

15 *Jarass* (Fn. 6), Art. 10 Rn. 3; vgl. auch *Gusy* (Fn. 5), Art. 10 Rn. 28.

16 Vgl. BVerfGE 67, 157 (171); 85, 386 (396); 100, 313 (358); *Epping* (Fn. 9), Rn. 681; *Gusy* (Fn. 5), Art. 10 Rn. 33; *Hermes* (Fn. 6), Art. 10 Rn. 44; *Hofmann* (Fn. 11), Art. 10 Rn. 8; *Ipsen* (Fn. 1), Rn. 304; *Jarass* (Fn. 6), Art. 10 Rn. 4; *Löwer* (Fn. 6), Art. 10 Rn. 17; *Pieroth/Schlink* (Fn. 9), Rn. 833; *Schmitt Glaeser* (Fn. 10), § 129 Rn. 63; *Sodan* (Fn. 10), Art. 10 Rn. 4; *Stern* (Fn. 6), S. 222; *Zippelius/Würtenberger*, Staatsrecht, § 28 Rn. 3.

17 *Epping* (Fn. 9), Rn. 681.

18 *Epping* (Fn. 9), Rn. 681; *Gusy* (Fn. 5), Art. 10 Rn. 33; *Jarass* (Fn. 6), Art. 10 Rn. 4; *Löwer* (Fn. 6), Art. 10 Rn. 17; *Manssen* (Fn. 1), Rn. 527; *Pieroth/Schlink* (Fn. 9), Rn. 833; *Schmitt Glaeser* (Fn. 10), § 129 Rn. 63 *Stern* (Fn. 6), S. 222.

19 *Gusy* (Fn. 5), Art. 10 Rn. 33; *Ipsen* (Fn. 1), Rn. 304; *Jarass* (Fn. 6), Art. 10 Rn. 4; *Löwer* (Fn. 6), Art. 10 Rn. 17; *Manssen* (Fn. 1), Rn. 527; *Pieroth/Schlink* (Fn. 9), Rn. 833; *Stern* (Fn. 6), S. 222; *Zippelius/Würtenberger* (Fn. 16), § 28 Rn. 6.

20 BVerfGE 67, 157 (171 f.); *Gusy* (Fn. 5), Art. 10 Rn. 34; *Stern* (Fn. 6), S. 222.

juristische Person des Privatrechts, getreten. Angesichts dieser Entwicklung hatte die Garantie des Postgeheimnisses ihren Adressaten verloren[21]. Das Postgeheimnis ist obsolet geworden[22].

Im Schrifttum wird die Gegenauffassung vertreten, dass das Postgeheimnis nach der Privatisierung der Deutschen Post noch den durch „Postdienstleister" vermittelten Postverkehr gegenüber der postfremden Exekutive gewährleisten könne[23], sonst bestehe eine Rechtsschutzlücke[24]. Auch die Unternehmen postalischer Dienste einschließlich der Deutschen Post AG könnten das Postgeheimnis des Art. 10 Abs. 1 GG geltend machen[25]. Zudem behalte das Postgeheimnis seine Bedeutung jedenfalls in der Übergangszeit, da die Deutsche Post AG für eine Übergangsfrist auch im Eigentum des Bundes stehe[26]. Ferner besitze die Deutsche Post AG heute faktisch noch die Stellung des Beförderungsmonopols, das die staatliche Post ehemals genossen habe[27]. Aufgrund der Monopolstellung und des staatlichen Einflusses sei die Bedeutung des Postgeheimnisses nicht fortgefallen, anderenfalls könne der Staat aus dem Anwendungsbereich des Art. 10 GG in das Privatrecht flüchten[28].

Diese Gegenansicht klingt zunächst einleuchtend. Bei näherer Betrachtung erweist sie sich jedoch als unzutreffend. Nach der Privatisierung der Deutschen Post wurde ihre Nachfolgerin, die Deutsche Post AG, in ein Unternehmen privater Rechtsform umgewandelt (Art. 143b Abs. 1 Satz 1 GG). Zwar steht die Deutsche Post AG gemäß Art. 143b Abs. 2 Satz 2 GG für eine Übergangsfrist auch im Eigentum des Bundes, diese Frist ist jedoch bereits abgelaufen[29]. Denn gemäß Art. 15 Gesetz zur Neuordnung des Postwesens und der Telekommunikation vom 14. 9. 1994 (Postneuordnungsgesetz – PTNeuOG)[30] in Verbindung mit Art. 143b Abs. 2 Satz 2 GG darf der Bund frühestens 5 Jahre nach dem Inkrafttreten des PTNeuOG, also zum 1. 1. 2000, die Kapitalmehrheit an der Deutschen Post AG aufgeben[31].

---

21 *Hermes* (Fn. 6), Art. 10 Rn. 46; a. A. *Hofmann* (Fn. 11), Art. 10 Rn. 8; *Hömig* (Fn. 10), Art. 10 Rn. 5; *Ipsen* (Fn. 1), Rn. 304; *Jarass* (Fn. 6), Art. 10 Rn. 6; *Michael/Morlok* (Fn. 8), Rn. 323; *Stern* (Fn. 6), S. 221.

22 *Hermes* (Fn. 6), Art. 10 Rn. 24; a. A. *Sodan* (Fn. 10), Art. 10 Rn. 4; *Stern* (Fn. 6), S. 221 f.

23 So *Hofmann* (Fn. 11), Art. 10 Rn. 8; *Hömig* (Fn. 10), Art. 10 Rn. 5; *Ipsen* (Fn. 1), Rn. 304; *Pagenkopf* (Fn. 9), Art. 10 Rn. 13.

24 So *Ipsen* (Fn. 1), Rn. 304; *Löwer* (Fn. 6), Art. 10 Rn. 13.

25 *Stern* (Fn. 6), S. 224.

26 *Epping* (Fn. 9), Rn. 682; *Zippelius/Würtenberger* (Fn. 16), § 28 Rn. 4.

27 *Pagenkopf* (Fn. 9), Art. 10 Rn. 13.

28 *Gusy* (Fn. 5), Art. 10 Rn. 37; *Michael/Morlok* (Fn. 8), Rn. 323.

29 *Gusy* (Fn. 5), Art. 10 Rn. 36; *Uerpmann*, in: von Münch/Kunig, GG, Bd. 3, Art. 143b Rn. 5; *Wieland*, in: Dreier, GG, Bd. 3, Art. 143b Rn. 11.

30 BGBl. 1994 I, S. 2325.

31 *Battis*, in: Sachs, GG, Art. 143b Rn. 6; *Jarass*, in: Jarass/Pieroth, GG, Art. 143b Rn. 3; *Uerpmann* (Fn. 29), Art. 143b Rn. 5; *Wieland* (Fn. 29), Art. 143b Rn. 11.

Aufgrund der verfassungsrechtlichen Ermächtigung des Art. 143b Abs. 2 Satz 2 GG hält der Bund zurzeit nur noch mehr als 30 % der Aktien an der Deutschen AG mittelbar über die Kreditanstalt für Wiederaufbau[32].

Art. 143b Abs. 2 Satz 2 GG bezieht sich nicht nur auf die formelle Privatisierung, sondern auch auf die materielle Privatisierung[33]. Da die materielle Privatisierung (= Aufgabenprivatisierung) besagt, dass der Staat eine Aufgabe nicht länger wahrnimmt und sein Aufgabenbestand reduziert wird[34], ist die Postdienstleistung nunmehr aus dem Bereich staatlicher Aufgaben ausgeschieden[35]. Daher ist schwer einzusehen, warum die Deutsche Post AG, die keine staatliche Aufgabe wahrnimmt und nur privatwirtschaftliche Tätigkeiten ausübt[36], als Grundrechtsadressat des Postgeheimnisses angesehen werden kann[37]. Die Frage, ob das Postgeheimnis in seiner Bedeutung fortgefallen ist, hängt nicht davon ab, ob die Deutsche Post AG eine Monopolstellung besitzt und ob der Staat einen Einfluss auf die Deutsche Post AG ausübt. Vielmehr ist entscheidend, dass die Deutsche Post AG unter dem Aspekt der formellen sowie materiellen Privatisierung ein (echtes) Privatunternehmen, das keine öffentliche Verwaltungsaufgabe wahrnimmt, darstellt[38]. Gemäß Art. 1 Abs. 3 GG binden Grundrechte keine private Person, sondern die staatliche Gewalt als unmittelbar geltendes Recht. Deswegen lässt sich die Deutsche Post AG nicht als Adressat des Postgeheimnisses betrachten[39], es sei denn, dass die Deutsche Post AG als Beliehene handelt[40] oder die unmittelbare Drittwirkung der Grundrechte

32 *Battis* (Fn. 31), Art. 143b Rn. 6; *Wieland* (Fn. 29), Art. 143b Rn. 11.

33 *Battis* (Fn. 31), Art. 143b Rn. 6; *Wieland* (Fn. 29), Art. 143b Rn. 11; a. A. *Gersdorf*, in: von Mangoldt/Klein/Starck, GG, Bd. 3, Art. 143b Rn. 14.

34 Vgl. dazu *Burgi*, in: Erichsen/Ehlers, AllgVerwR, § 9 Rn. 35; *Maurer*, AllgVerwR, § 23 Rn. 63; *Schoch*, DVBl. 1994, S. 962 f.; *Schulze-Fielitz*, in: Hoffmann-Riem/Schmidt-Aßmann/Voßkuhle, GVwR, Bd. 1, § 12 Rn. 112.

35 *Wieland* (Fn. 29), Art. 87 f Rn. 23.

36 Die Deutsche Post AG übt gemäß Art. 87 f Abs. 2 S. 1 GG privatwirtschaftliche Tätigkeiten aus (vgl. *Gersdorf* (Fn. 33), Art. 87 f Rn. 51 ff.; *Hermes* (Fn. 6), Art. 10 Rn. 46; *Manssen* (Fn. 1), Rn. 528; *Pagenkopf* (Fn. 9), Art. 10 Rn. 20; *Stern* (Fn. 6), S. 224; *Wieland* (Fn. 29), Art. 87 f Rn. 23).

37 Hierbei ist zu betonen, dass sich die in Art. 87 f Abs. 2 S. 2 GG geregelten „Hoheitsaufgaben im Bereich des Postwesens" nicht auf die Aufgabe der Deutschen Post AG erstrecken. Da der Staat trotz der materiellen Privatisierung regulierend eingreifen kann und muss (vgl. *Maurer* (Fn. 34), § 23 Rn. 63), betreffen die Hoheitsaufgaben im Sinne des Art. 87 f Abs. 2 S. 2 GG nach der Privatisierung der Deutschen Post vielmehr die staatliche Regulierung im Bereich des Postwesens.

38 A. A. *Masing*, in: Isensee/Kirchhof, HStR, Bd. 4, § 90 Rn. 34: Die Deutsche Post AG stellt ein öffentliches Unternehmen dar, das durch Grundrechte gebunden ist.

39 *Herdegen*, in: Badura/von Danwitz/Herdegen/Sedemund/Stern, PostG, VerfGrdl. Rn. 73; *Hermes* (Fn. 6), Art. 10 Rn. 46; *Lang*, NJW 2004, S. 3601 (3604 f.).

40 *Herdegen* (Fn. 39), VerfGrdl Rn. 75; *Lang* (Fn. 39), S. 3601 (3605).

anerkannt würde[41]. Außerdem geht die Behauptung, dass die Deutsche Post AG das Postgeheimnis des Art. 10 Abs. 1 GG genießen könne und damit das Postgeheimnis des Art. 10 Abs. 1 GG nach der Privatisierung der Deutschen Post seine Bedeutung nicht verliere[42], zu weit. Denn nur Kommunikationsteilnehmer können Art. 10 Abs. 1 GG geltend machen. Da die Deutsche Post AG nicht Kommunikationsteilnehmer, sondern Anbieter von Postdiensten darstellt, kann sie sich nicht auf das Postgeheimnis des Art. 10 Abs. 1 GG berufen. Auch nicht zu folgen ist der Meinung, dass das Postgeheimnis des Art. 10 Abs. 1 GG nach der Privatisierung der Deutschen Post nicht gegenstandslos sei, weil der Schutz des Postgeheimnisses auch als staatliche Schutzpflicht wirke[43]. Da die staatliche Schutzpflicht zu den objektivrechtlichen Grundrechtsgehalten gehört, ist es schwer zu verstehen, dass sich eine staatliche Schutzpflicht aus dem Postgeheimnis, dessen Bedeutung nach der Privatisierung der Deutschen Post entfallen ist, ergeben soll. Die Befürchtung einer Rechtsschutzlücke[44] ist gegenstandslos. Denn die Sendungen, die früher in den Schutzbereich des Postgeheimnisses fielen, können nach der Privatisierung der Deutschen Post durch Art. 2 Abs. 1 GG geschützt werden.

c) Fernmeldegeheimnis

Im Gegensatz zum Brief- und Postgeheimnis, das die körperlich übermittelten Sendungen betrifft, schützt das Fernmeldegeheimnis die Vertraulichkeit der Individualkommunikation, die unkörperlich durch die Fernmeldetechnik übertragen wird[45]. Dabei geht es um die Entwicklung der modernen Telekommunikationstechnik[46]. Das Bundesverfassungsgericht hat in einem jüngeren Urteil diese Grundrechtsgewährleistung „Telekommunikationsgeheimnis" genannt[47]. Geschützt ist mithin nicht nur das traditionelle Telefon, sondern auch die Kommunikation mittels neuer Medien wie etwa

41 Nach der herrschenden Meinung gibt es nur eine mittelbare Drittwirkung von Grundrechten (vgl. *Dreier*, in: Dreier, GG, Bd. 1, Vorb. Rn. 98; *Hufen* (Fn. 1), § 7 Rn. 8 ff.; *Jarass* (Fn. 6), Vorb. vor Art. 1 Rn. 58 ff.; *Michael/Morlok* (Fn. 8), Rn. 478; *Papier*, in: Merten/Papier, HGR, Bd. 2, § 55 Rn. 22; *Pieroth/Schlink* (Fn. 9), Rn. 189 ff.; *Sachs*, in: Sachs, GG, vor Art. 1 Rn. 32; *Sodan* (Fn. 10), Art. 1 Vorb. Rn. 23; *Zippelius/Würtenberger* (Fn. 16), § 18 Rn. 21). Die herrschende Meinung ist zutreffend, weil sie dem Art. 1 Abs. 3 GG entspricht.

42 *Stern* (Fn. 6), S. 224.

43 *Michael/Morlok* (Fn. 8), Rn. 323.

44 Beispielsweise können Warensendungen, die nicht dem Begriff „Brief" entsprechen, nicht mehr durch das Postgeheimnis geschützt werden.

45 Vgl. BVerfGE 67, 157 (172); 85, 386 (396); *Baldus* (Fn. 10), Art. 10 Rn. 7; *Gusy* (Fn. 5), Art. 10 Rn. 39; *Hermes* (Fn. 6), Art. 10 Rn. 36; *Jarass* (Fn. 6), Art. 10 Rn. 5; *Michael/Morlok* (Fn. 8), Rn. 324; *Pagenkopf* (Fn. 9), Art. 10 Rn. 14 f.; *Pieroth/Schlink* (Fn. 9), Rn. 837; *Sodan* (Fn. 10), Art. 10 Rn. 5; *Stern* (Fn. 6), S. 226.

46 Vgl. *Hömig* (Fn. 10), Art. 10 Rn. 7; *Hufen* (Fn. 1), § 17 Rn. 7; *Jarass* (Fn. 6), Art. 10 Rn. 5; *Pagenkopf* (Fn. 9), Art. 10 Rn. 14.

47 BVerfGE 120, 274 (306 f.); vgl. auch *Sodan* (Fn. 10), Art. 10 Rn. 5.

Internet[48]. Zu beachten ist, dass das Fernmeldegeheimnis zwar nur die „Individualkommunikation" gewährleistet, eine „individuelle Kommunikation mittels der Massenmedien" jedoch auch in den Schutzbereich des Fernmeldegeheimnisses fallen kann[49]. Wie bereits im 2. Kapitel dargelegt wurde, führt die Entstehung des Internets teilweise zur Konvergenz zwischen Individualkommunikationen und Massenkommunikationen[50]. Ihre Abgrenzung wird heute immer schwieriger. Angesichts dieser Entwicklung muss für den Schutz des Fernmeldegeheimnisses genügen, dass der Kommunikationsvorgang eine individuelle Kommunikation befördern könnte[51].

Das Fernmeldegeheimnis schützt sowohl die Vertraulichkeit des Kommunikationsinhalts als auch die Vertraulichkeit des Kommunikationsvorgangs[52]. Dazu gehören die Kommunikationsverbindungsdaten bzw. Kommunikationsumstände[53]. Mit anderen Worten: Der Schutzbereich umfasst nicht nur Inhaltsdaten, sondern auch Verkehrsdaten im Sinne des § 3 Nr. 30 und § 96 TKG, die sich auf einen konkreten Telekommunikationsvorgang beziehen[54]. Zeitlich endet der Schutz des Fernmeldegeheimnisses erst in dem Moment, in dem die übermittelten Informationen beim Empfänger angekommen sind[55]. Folglich können die zwischengespeicherten Informationen durch das Fernmeldegeheimnis geschützt werden[56]. Falls die Inhalte und Verkehrsdaten der Telekommunikation nach Abschluss des Übertragungsvorgangs bereits bei einem Kommunikationsteilnehmer gespeichert werden, fallen sie nicht in den Schutzbereich des Fernmeldegeheimnisses[57]. Räumlich kann die Garantie des Fernmeldegeheimnisses im Ausland

48 BVerfGE 120, 274 (307); *Gusy* (Fn. 5), Art. 10 Rn. 40; *Hufen* (Fn. 1), § 17 Rn. 7; *Jarass* (Fn. 6), Art. 10 Rn. 5; *Pieroth/Schlink* (Fn. 9), Rn. 837; *Sodan* (Fn. 10), Art. 10 Rn. 5; *Zippelius/Würtenberger* (Fn. 16), § 28 Rn. 8.

49 *Gusy* (Fn. 5), Art. 10 Rn. 43 f.; *Hermes* (Fn. 6), Art. 10 Rn. 39; *Pieroth/Schlink* (Fn. 9), Rn. 837.

50 Vgl. *Schoch*, VVDStRL 57 (1998), S. 158 (170).

51 *Gusy* (Fn. 5), Art. 10 Rn. 44; *Hermes* (Fn. 6), Art. 10 Rn. 39; *Pieroth/Schlink* (Fn. 9), Rn. 837.

52 Vgl. BVerfGE 67, 157 (172); 85, 386 (396); *Gusy* (Fn. 5), Art. 10 Rn. 45; *Hermes* (Fn. 6), Art. 10 Rn. 41; *Horn*, in: Isensee/Kirchhof, HStR, Bd. 7, § 149 Rn. 101; *Hufen* (Fn. 1), § 17 Rn. 7; *Löwer* (Fn. 6), Art. 10 Rn. 22; *Manssen* (Fn. 1), Rn. 529; *Sodan* (Fn. 10), Art. 10 Rn. 6; *Stern* (Fn. 6), S. 226 f.

53 Vgl. BVerfGE 120, 274 (307); *Hermes* (Fn. 6), Art. 10 Rn. 41; *Hömig* (Fn. 10), Art. 10 Rn. 6; *Hofmann* (Fn. 11), Art. 10 Rn. 10; *Hufen* (Fn. 1), § 17 Rn. 7; *Pagenkopf* (Fn. 9), Art. 10 Rn. 14; *Sodan* (Fn. 10), Art. 10 Rn. 7; *Zippelius/Würtenberger* (Fn. 16), § 28 Rn. 5.

54 *Büttgen*, in: Scheurle/Mayen, TKG, § 96 Rn. 3; *Fetzer*, in: Arndt/Fetzer/Scherer, TKG, § 96 Rn. 3; *Schütz/Robert*, in: Geppert/Piepenbrock/Schütz/Schuster, TKG, § 3 Rn. 66.

55 BVerfGE 115, 166 (184); *Hermes* (Fn. 6), Art. 10 Rn. 42; *Hömig* (Fn. 10), Art. 10 Rn. 6; *Horn* (Fn. 52), § 149 Rn. 101; *Jarass* (Fn. 6), Art. 10 Rn. 5; *Sodan* (Fn. 10), Art. 10 Rn. 7.

56 *Hermes* (Fn. 6), Art. 10 Rn. 42.

57 BVerfGE 115, 166 (183); *Hömig* (Fn. 10), Art. 10 Rn. 6; *Sodan* (Fn. 10), Art. 10 Rn. 7.

jedenfalls dann wirken, wenn die Erfassung oder die Auswertung des im Ausland geführten Fernmeldeverkehrs in Deutschland stattfindet[58].

2. Rechtfertigung des Eingriffs durch den einfachen Gesetzesvorbehalt

Gemäß Art. 10 Abs. 2 S. 1 GG dürfen die drei Garantien des Art. 10 Abs. 1 GG beschränkt werden, wenn die Beschränkung auf Grund eines Gesetzes erfolgt. Insoweit lässt sich der Eingriff in das Brief-, Post- und Fernmeldegeheimnis zunächst durch formelle Gesetze rechtfertigen[59]. Er kann aber auch auf Grund gesetzlicher Ermächtigung durch Rechtsverordnungen, Satzungen oder Verwaltungsakte erfolgen[60]. Um mit Art. 80 Abs. 1 GG in Einklang zu stehen, muss die gesetzliche Ermächtigung ausreichend bestimmt sein[61]. Das Bestimmtheitsgebot für die gesetzliche Ermächtigung führt dazu, dass die materiellen Eingriffsvoraussetzungen und wesentlichen Modalitäten durch das Parlament zu entscheiden sind[62].

3. E-Mail-Kommunikation als Schutzgegenstand des Fernmeldegeheimnisses

a) Grundrechtsschutz des Fernmeldegeheimnisses für Internet-basierte Telekommunikation

Zwar ersetzt die E-Mail-Kommunikation Teile der traditionellen Briefkommunikation, jedoch kann die Vertraulichkeit des E-Mail-Verkehrs nicht durch das Briefgeheimnis geschützt werden. Denn die E-Mail-Kommunikation, die durch das Internet unkörperlich eine Nachricht überträgt, entspricht nicht dem Briefgeheimnis, das die körperliche Nachrichtenübermittlung betrifft[63]. Wie bereits im 2. Kapitel dargelegt wurde, ist die E-Mail das wichtigste und populärste moderne Internet-basierte Informations- und Kommunikationsmittel. Sie wird unkörperlich durch die Internet-Technik übertragen. Der E-Mail-Verkehr gehört zur Telekommunikation, bei der es um die grundrechtliche Gewährleistung des Fernmeldegeheimnisses des Art. 10 Abs. 1 GG geht. Folglich fällt die E-Mail-Übermittlung in den

58 BVerfGE 100, 313 (363 f.); *Hermes* (Fn. 6), Art. 10 Rn. 43; *Hömig* (Fn. 10), Art. 10 Rn. 8; *Jarass* (Fn. 6), Art. 10 Rn. 5; *Manssen* (Fn. 1), Rn. 525; *Pagenkopf* (Fn. 9), Art. 10 Rn. 15.

59 *Jarass* (Fn. 6), Art. 10 Rn. 16; *Pagenkopf* (Fn. 9), Art. 10 Rn. 31.

60 *Gusy* (Fn. 5), Art. 10 Rn. 65; *Hermes* (Fn. 6), Art. 10 Rn. 58; *Hömig* (Fn. 10), Art. 10 Rn. 11; *Hofmann* (Fn. 11), Art. 10 Rn. 22; *Jarass* (Fn. 6), Art. 10 Rn. 16; *Löwer* (Fn. 6), Art. 10 Rn. 28; *Pagenkopf* (Fn. 9), Art. 10 Rn. 31.

61 Vgl. *Gusy* (Fn. 5), Art. 10 Rn. 71; *Hömig* (Fn. 10), Art. 10 Rn. 9; *Jarass* (Fn. 6), Art. 10 Rn. 17.

62 *Gusy* (Fn. 5), Art. 10 Rn. 71; *Hermes* (Fn. 6), Art. 10 Rn. 58.

63 Aus diesem Grund kann die Vertraulichkeit der E-Mail-Kommunikation auch nicht durch das Postgeheimnis geschützt werden, auch wenn das Postgeheimnis seine Bedeutung nicht wegen der Privatisierung von Postdiensten verloren hätte und die Deutsche Post AG den E-Mail-Dienst anbieten würde.

Schutzbereich des Fernmeldegeheimnisses[64]. Dieses schützt nur die Individualkommunikation. Demzufolge wird eine E-Mail-Übertragung nicht durch das Fernmeldegeheimnis gewährleistet, falls es um die Mitteilung an die Allgemeinheit geht (z. B. unverlangte Massen-E-Mail)[65].

Wenn der Staat den Inhalt und die Umstände (= Verkehrsdaten im Sinne des TKG = in einigen polizei- und ordnungsgesetzlichen Ermächtigungsvorschriften zur Telekommunikationsüberwachung Verbindungsdaten genannt[66]) einer Telekommunikation erhebt, speichert, verwertet oder weitergibt, liegt ein Eingriff in das Fernmeldgeheimnis vor[67]. Wie im 2. Kapitel ausgeführt wurde[68], bezieht sich die präventiv-polizeiliche E-Mail-Überwachung sowohl auf die Erhebung der E-Mail-Inhalte als auch auf die Erhebung der Verkehrsdaten einer E-Mail-Kommunikation[69]. Diese beiden Daten sind Schutzgegenstände des Fernmeldegeheimnisses. Demzufolge greift ein präventiv-polizeilicher Zugriff auf den E-Mail-Verkehr in die grundrechtliche Gewährleistung des Fernmeldgeheimnisses des Art. 10 Abs. 1 GG ein.

b) Kein Grundrechtsschutz des E-Mail-Verkehrs durch das Fernmeldegeheimnis?

In der Literatur wird vertreten, dass die E-Mail-Übertragung nicht durch das Fernmeldegeheimnis geschützt werde[70]. Das Fernmeldegeheimnis gewährleiste nur die Telekommunikationsverbindung, die objektiv schutzgeeignet und schutzfähig sei. Wenn die Telekommunikation in technischer Hinsicht gar nicht oder nur unvollkommen vertraulich sei, sei sie nicht schutzfähig. Da die digitalen Datenpakete über eine Vielzahl von Stationen weitergeleitet würden, auf denen sie prinzipiell von jedermann einsehbar und auch manipulierbar seien[71], komme der E-Mail-Übertragung, die auf der Datenpaket-Technik basiere, keine Schutzfähigkeit zu. Insoweit werde

64 BVerfGE 113, 348 (383); 120, 274 (307); *Epping* (Fn. 9), Rn. 684; *Hofmann* (Fn. 11), Art. 10 Rn. 9; *Hufen* (Fn. 1), § 17 Rn. 7; *Jarass* (Fn. 6), Art. 10 Rn. 5; *Kube*, in: Isensee/Kirchhof, HStR, Bd. 4, § 91 Rn. 44; *Löwer* (Fn. 6), Art. 10 Rn. 18; *Michael/Morlok* (Fn. 8), Rn. 324; *M. Sievers*, Schutz der Kommunikation, S. 131; *Stern* (Fn. 6), S. 226; *Zippelius/Würtenberger* (Fn. 16), § 28 Rn. 8.

65 Vgl. *Stern* (Fn. 6), S. 226; wohl anders *Sievers* (Fn. 64), S. 129 f.

66 § 34a Abs. 2 Nr. 2 mvSOG; § 33a Abs. 2 S. 1 Nr. 2 ndsSOG; § 185a Abs. 2 Nr. 2 shLVwG.

67 BVerfGE 100, 313 (366 f.); 107, 299 (313 f.); 110, 33 (53); *Hermes* (Fn. 6), Art. 10 Rn. 53; *Hufen* (Fn. 1), § 17 Rn. 11; *Jarass* (Fn. 6), Art. 10 Rn. 11; *Pieroth/Schlink* (Fn. 9), Rn. 840; *Sodan* (Fn. 10), Art. 10 Rn. 10; *Zippelius/Würtenberger* (Fn. 16), § 28 Rn. 10.

68 Siehe 2. Kapitel C II 1 b) und 2.

69 Ausnahme: Nach 23a Abs. 1 S. 1 bwPolG dürfen nur die Verkehrsdaten erhoben werden.

70 *Pagenkopf* (Fn. 9), Art. 10 Rn. 14a.

71 *Brüning/Helios*, JURA 2001, S. 155 f.; *Groß* (Fn. 10), S. 326 (327); *Pagenkopf* (Fn. 9), Art. 10 Rn. 14a.

die E-Mail in Fachkreisen mit einer lesbaren Postkarte verglichen[72]. Sie gehöre mithin nicht zum Schutzbereich des Fernmeldegeheimnisses.

Dieser Auffassung ist jedoch nicht zuzustimmen. Da die unverschlossene Sendung auch durch das Brief- und Postgeheimnis geschützt wird, ist schwerlich einzusehen, warum das Fernmeldegeheimnis die Telekommunikation, deren Vorgang technisch in Internet-Knoten beobachtet werden kann, nicht schützt und damit die E-Mail-Kommunikation keinen Schutzgegenstand des Fernmeldegeheimnisses darstellt. Zudem können grundsätzlich nur die Kommunikationsteilnehmer, die das Passwort für den Zugang zur Mailbox haben, den Inhalt der E-Mail lesen. Obwohl die digitalen Datenpakete während des Übertragungsvorgangs einsehbar sein könnten, können sie nicht, wie eine Postkarte, durch Augen unmittelbar dechiffriert werden, es sei denn, dass man sie durch technische Mittel abfängt und dekodiert. In diesem Zusammenhang ist der Inhalt der E-Mail, der technisch aus digitalen Datenpaketen besteht, ähnlich wie ein verschlossener Brief, den man nicht unmittelbar lesen kann. Für die Heimlichkeit der E-Mail-Übertragung ist es unerheblich, ob der Inhalt der E-Mail durch die „Verschlüsselung" ein Geheimtext ist. Da der Zugriff auf eine unverschlüsselte E-Mail einen weitaus höheren Aufwand erfordert als das Mitlesen einer offenen Postkarte, ist der Vergleich von E-Mails mit offenen Postkarten nicht überzeugend[73]. Folglich ist der E-Mail-Verkehr als eine verborgene Kommunikation, die durch das Fernmeldegeheimnis geschützt wird, anzusehen.

c) Kein Grundrechtsschutz der im Zielserver ruhenden E-Mail durch das Fernmeldegeheimnis?

Im Vergleich zu anderen Formen der Telekommunikation (z. B. Kommunikation mittels des Mobiltelefons) besteht die Besonderheit des E-Mail-Verkehrs darin, dass sich die Übermittlung einer E-Mail technisch in drei Phasen aufteilen lässt[74]. Zuerst wird die E-Mail nach dem „Abschicken" auf dem Mailserver der Provider, die dem Absender die E-Mail-Dienste anbieten, kurz zwischengespeichert und sodann durch das Internet an den Zielserver (d. h. an den Mailserver der Provider, die dem Empfänger die E-Mail-Dienste anbieten) weitergesandt (Phase 1). Sodann wird die E-Mail auf dem Mailserver der dem Empfänger die E-Mail-Dienste anbietenden Provider (d. h. in der Mailbox des Empfängers) gespeichert (Phase 2). Schließlich

72 *Brüning/Helios* (Fn. 71), S. 155 (156); *Groß* (Fn. 10), S. 326 (327); *Pagenkopf* (Fn. 9), Art. 10 Rn. 14a.

73 *Härting*, NJW 2005, S. 1248.

74 Vgl. *Bär*, MMR 2000, S. 472 (475); *Nack*, in: Hannich, StPO, § 100a Rn. 19 f.; kritisch *Meininghaus*, Der Zugriff auf E-Mails, S. 264 f.

ruft der Empfänger die E-Mail ab (Phase 3)[75]. Bevor der Empfänger die E-Mail abruft, „ruht" sie im Mailserver der Provider. Deswegen kann die 2. Phase der E-Mail-Übertragung von wenigen Stunden bis zu mehreren Tagen oder gar Wochen dauern[76].

Zwar wird die E-Mail nach der „Sende-Bestätigung" zunächst kurz im Mailserver der Provider, die dem Absender die E-Mail-Dienste anbieten, zwischengespeichert, jedoch beginnt der Vorgang der E-Mail-Übertragung bereits in diesem Moment. Aus diesem Grund fällt eine E-Mail in den Bereich des Fernmeldegeheimnisses, wenn sie im Mailserver der Provider, durch die der Absender die E-Mail abschickt, zwischengespeichert ist[77].

Umstritten ist, ob die E-Mail, die bereits im Mailserver der dem Empfänger die E-Mail-Dienste anbietenden Provider (= im Mailbox des Empfängers) „ruht" und noch nicht vom Empfänger abgerufen wird (2. Phase der E-Mail-Übermittlung), auch durch das Fernmeldegeheimnis geschützt wird. In der Literatur wird vertreten, dass das Fernmeldegeheimnis nur die 1. und 3. Phase der E-Mail-Übertragung schütze. Falls sich die E-Mail-Übertragung in der 2. Phase befinde oder, anders ausgedrückt, falls die E-Mail bereits im Mailserver der dem Empfänger die E-Mail-Dienste anbietenden Provider ruhe und der Empfänger sie noch nicht abrufe, werde der Schutzbereich des Fernmeldegeheimnisses nicht betroffen. Denn der Telekommunikationsvorgang sei während der 2. Phase der E-Mail-Übermittlung auf zunächst unbestimmte Zeit unterbrochen. Dabei gehe es nicht um einen (laufenden) Vorgang der Telekommunikation, sondern um im Mailserver gespeicherte Daten. In diesem Zusammenhang stelle der staatliche Zugriff auf die E-Mail, die sich in der 2. Phase der E-Mail-Übertragung befindet, keine Telekommunikationsüberwachung dar und greife damit nicht in das Fernmeldegeheimnis des Art. 10 Abs. 1 GG ein[78]. Durch seinen Beschluss vom 31. 3. 2009 stimmt der Bundesgerichtshof dieser Meinung zu[79].

Ob diese Auffassung überzeugt, ist allerdings sehr zweifelhaft. Wie bereits dargelegt, endet der grundrechtliche Schutz des Fernmeldegeheimnisses zeitlich mit dem Abschluss des Übertragungsvorgangs. Falls die

75 *J. Kühling/A. Elbracht* und *S. Schlegel* gliedern die E-Mail-Kommunikation in vier Phasen: (1) Absendung, (2) Speicherung beim Provider, (3) Abruf durch den Empfänger, und (4) Speicherung beim Empfänger (vgl. *Kühling/Elbracht*, Telekommunikationsrecht, Rn. 40 mit Fn. 134; *Schlegel*, HRRS 2007, S. 44 (47), http://www.hrr-strafrecht.de). Ob der Empfänger nach dem Abruf die E-Mail auf seiner Festplatte speichert, spielt aber für die Diskussion über die E-Mail-Überwachung keine Rolle. Sobald die E-Mail abgerufen wird, fällt sie bereits in den Bereich der Beherrschbarkeit des Empfängers.

76 *Bär* (Fn. 74), S. 472 (475).

77 *Kleine-Voßbeck*, Electronic Mail, S. 36 f.; vgl. auch *Sachs/Krings*, JuS 2008, S. 481 (483): Das Fernmeldegeheimnis ist einschlägig, wenn (oder soweit) sich die Überwachung des Rechners ausschließlich auf die laufende Kommunikation erstreckt.

78 *Bär* (Fn. 74), S. 472 (474 f.); *Nack* (Fn. 74), § 100a Rn. 22.

79 BGH, MMR 2009, S. 391.

Sachverhaltsfrage, ob der Telekommunikationsvorgang bereits abgeschlossen ist, schwer festzulegen ist[80], sollte man auf das Beherrschbarkeitskriterium[81] abstellen[82]. Da sich die übermittelte Nachricht während des Übertragungsvorgangs nicht in der von Telekommunikationsteilnehmern beherrschbaren Privatsphäre, sondern in dem lediglich von Dritten (auch vom Staat) beherrschbaren Bereich befindet, gibt es eine Zugriffsmöglichkeit Dritter (auch des Staates). Ausgehend davon ist der grundrechtliche Schutz des Fernmeldgeheimnisses nicht nur für Vorgänge der Telekommunikation, sondern auch für die durch Telekommunikationsmittel übermittelten Daten, die sich noch nicht im Herrschaftsbereich der Telekommunikationsteilnehmer befinden und somit durch die Überwachungsmöglichkeit Dritter (des Staates) bedroht werden, notwendig. Insoweit basiert die grundrechtliche Spezialität des Fernmeldegeheimnisses auf der fehlenden Beherrschbarkeit und der Überwachungsmöglichkeit[83]. Die Frage, wie weit der Schutzbereich des Fernmeldegeheimnisses reicht, hängt davon ab, ob sich die übermittelten Daten noch im Herrschaftsbereich Dritter (auch des Staates) befinden. Sobald sich die Daten im Herrschaftsbereich der Telekommunikationsteilnehmer befinden, ist der grundrechtliche Schutz des Fernmeldgeheimnisses ausgeschlossen[84]. Die Beherrschbarkeit der Privatsphäre der Kommunikationsteilnehmer stellt deswegen die Schutzbereichsgrenze des Fernmeldgeheimnisses dar[85]. Wenn eine E-Mail im Mailserver der dem Empfänger die E-Mail-Dienste anbietenden Provider ruht und noch nicht vom Empfänger abgerufen wurde, befindet sie sich nicht im Herrschaftsbereich des Empfängers. In dieser Phase wird sie durch eine Überwachung, die von Dritten (auch vom Staat) durchgeführt wird, bedroht. Die 2. Phase einer E-Mail-Übermittelung lässt sich nicht als Unterbrechung eines Telekommunikationsvorgangs, sondern ein Teil eines gesamten laufenden Telekommunikationsvorgangs ansehen. Folglich gilt der Grundrechtsschutz des Fernmeldgeheimnisses, der auf der fehlenden Beherrschbarkeit und der Überwachungsmöglichkeit basiert, auch für die E-Mail, die im Mailserver der dem Empfänger die E-Mail-Dienste anbietenden Provider ruht und noch nicht vom Empfänger abge-

80 Es wird vertreten, dass die vom Bundesverfassungsgericht betonte „Einheitlichkeit des Übermittlungsvorgangs“ (BVerfGE 115, 166 (186 f.)) den Schutz des Fernmeldegeheimnisses für die auf dem Mailserver ruhende E-Mail begründen könne (vgl. *Jahn*, NStZ 2007, S. 255 (264)). Diese Auffassung ist unzutreffend. Denn das Bundesverfassungsgericht erklärte durch die „Einheitlichkeit des Übermittlungsvorgangs“ nur, dass der Schutz des Fernmeldegeheimnisses nicht in jedem Fall am Endgerät der Telekommunikationsanlage endet. Es nahm jedoch nicht zu der Frage Stellung, wann der Vorgang der Telekommunikation abgeschlossen ist.

81 Vgl. dazu BVerfGE 115, 166 (176, 185 f.).

82 *Kühling/Elbracht* (Fn. 75), Rn. 39.

83 Vgl. BVerfGE 115, 166 (185 f.); *Sankol*, MMR 2007, S. 692 (696).

84 *Geis/Geis*, MMR 2006 Heft 11, S. X.

85 BVerfGE 115, 166 (185 f.); *Kühling/Elbracht* (Fn. 75), Rn. 39; *Sankol* (Fn. 83), S. 692 (696).

rufen ist[86]. Auch das Bundesverfassungsgericht hat sich in seinem Beschluss vom 16. 06. 2009, dieser Auffassung angeschlossen[87]. Wenn die überwachende Polizei (mit Hilfe der E-Mail-Provider) in den Mailserver der Provider einen E-Mail-Filter einsetzt und dadurch die in diesen kontrollierten Mailserver ruhenden und noch nicht abgerufenen E-Mails abfängt und mitliest, greift diese verdeckte polizeiliche Maßnahme der Informationserhebung in das Fernmeldegeheimnis des Art. 10 Abs. 1 GG ein. Die Auffassung, dass der Grundrechtsschutz des Fernmeldgeheimnisses in der 2. Phase einer E-Mail-Übertragung fehle, ist aus grundrechtsdogmatischer Sicht unzutreffend.

Schließlich ist die Reichweite des Grundrechtsschutzes des Fernmeldegeheimnisses für die sog. Webmail zu erklären. Denn eine E-Mail-Kommunikation kann nicht nur durch die Verwendung eines E-Mail-Programms, sondern auch durch den Webmail-Service erfolgen. Während das E-Mail-Programm auf dem Computer der Telekommunikationsteilnehmer installiert werden muss und damit mit dem Mail-Server verbinden kann, bedarf die Webmail keiner lokalen Installation eines E-Mail-Programms. Durch einen Webbrowser, mit dem man eine Webseite finden und lesen kann[88], kann der Benutzer des Webmail-Services unmittelbar auf einer Webseite seine E-Mails verwalten, soweit er sich im Internet eingeloggt hat. Es wird vertreten, dass der Vorgang der Telekommunikation beendet sei, sobald die E-Mail in einer Mailbox auf dem Webmail-Server bereitgestellt werde. Der Empfänger sei nun in der Lage, die E-Mail zu lesen, zu speichern oder zu löschen. Deswegen falle die E-Mail ab diesem Zeitpunkt in den Herrschaftsbereich der Telekommunikationsteilnehmer und werde nicht durch das Fernmeldegeheimnis geschützt. Ob der Empfänger zusätzlich die E-Mail aus dem Webmail-Server abrufe, sei hierfür unerheblich[89]. Dem ist nicht zuzustimmen. Die Mailbox für die Webmail liegt nicht auf dem eigenen Server des Empfängers, sondern auf dem Server des Providers. Mit anderen Worten: Die Mailbox auf dem Webmail-Server ist kein Datenträger des Empfängers. Bevor sich der Empfänger in der Webseite der Webmail einloggt und damit weiß, dass eine neue E-Mail in der Mailbox auf dem Webmail-Server ruht, besteht die Überwachungsmöglichkeit, dass nämlich von Dritten (auch vom Staat) die neue in der Mailbox auf dem Webmail-Server ruhende E-Mail mitgelesen wird. Eine in der Mailbox auf dem Webmail-Server ruhende und noch nicht abgerufene E-Mail fällt nicht in den Herrschaftsbereich des Empfängers. Deswegen ist der Vorgang der

86 LG Hamburg, MMR 2008, S. 186 (187); LG Hanau, NJW 1999, S. 3647; *Germann*, Gefahrenabwehr und Strafverfolgung, S. 555 f.; *Hermes* (Fn. 6), Art. 10 Rn. 42; *Hufen* (Fn. 1), § 17 Rn. 25; *Jarass* (Fn. 6), Art. 10 Rn. 5; *Kemper*, NStZ 2005, 538 (543); *Sievers* (Fn. 64), S. 133.

87 BVerfG, 2 BvR 902/06 vom 16. 6. 2009, Rn. 46.

88 Z. B. Microsoft Internet Explorer, Mozilla-Browser (Firefox), Safari etc.

89 Vgl. *Geis/Geis* (Fn. 84), S. X (XI).

Telekommunikation im Fall der Webmail erst beendet, nachdem der Empfänger in der Webseite der Webmail eingeloggt und die neue in der Mailbox auf dem Webmail-Server ruhende E-Mail abgerufen hat. Ab diesem Zeitpunkt schützt das Fernmeldegeheimnis die E-Mail-Übertragung durch den Webmail-Service auch nicht mehr.

II. Schutz der per E-Mail übermittelten personenbezogenen Daten durch das Grundrecht auf informationelle Selbstbestimmung

1. Schutzbereich des Rechts auf informationelle Selbstbestimmung

Das Recht auf informationelle Selbstbestimmung wurde durch das Urteil des Bundesverfassungsgerichts vom 15. Dezember 1983 zum Volkszählungsgesetz[90] entwickelt[91]. Hier wurde das Recht auf informationelle Selbstbestimmung aus Art. 2 Abs. 1 (d. h. aus dem allgemeinen Persönlichkeitsrecht) in Verbindung mit Art. 1 Abs. 1 GG hergeleitet[92]. Es gewährleistet „die Befugnis des Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen“[93]. Anders ausgedrückt, ist es ein Recht des Einzelnen, selbst zu entscheiden, ob, wann und wem er zu welchem Zweck personenbezogene Daten offenbart[94].

Das allgemeine Persönlichkeitsrecht (Art. 2 Abs. 1 GG) enthält das Recht der Selbstdarstellung[95], d. h. das Recht des Einzelnen, darüber zu entscheiden, wie er sich gegenüber Dritten oder der Öffentlichkeit darstellen will[96]. Dazu gehört auch das Recht auf Selbstbestimmung über den persönlichen

90 BVerfGE 65, 1 ff.

91 *Hofmann* (Fn. 11), Art. 2 Rn. 26; *Kloepfer*, Informationsrecht, § 3 Rn. 48; *Kube*, in: Isensee/Kirchhof, HStR, Bd. 7, § 148 Rn. 66; *Kunig*, in: von Münch/Kunig, GG, Bd. 1, Art. 2 Rn. 38; *Michael/Morlok* (Fn. 8), Rn. 426; *Murswiek*, in: Sachs, GG, Art. 2 Rn. 72; *Hufen*, in: Badura/Dreier, FS BVerfG, S. 105 (117); *Pieroth/Schlink* (Fn. 9), Rn. 399; *Stern* (Fn. 6), S. 231; *von Münch*, Staatsrecht, Bd. 2, Rn. 319.

92 Demgegenüber sieht ein großer Teil der Lehre den Datenschutz als Teil jedes einzelnen Freiheitsrechts an (vgl. *Schmitt Glaeser* (Fn. 10), § 129 Rn. 82 f.).

93 BVerfGE 65, 1 (43); vgl. auch *Albers*, Informationelle Selbstbestimmung, S. 152 ff.; *Antoni*, in: Hömig, GG, Art. 1 Rn. 14; *Badura*, Staatsrecht, C Rn. 36; *Dreier* (Fn. 41), Art. 2 I Rn. 78 f.; *Hofmann* (Fn. 11), Art. 2 Rn. 26; *Hufen* (Fn. 1), § 12 Rn. 2; *Jarass* (Fn. 6), Art. 2 Rn. 44;. *Manssen* (Fn. 1), Rn. 224; *Murswiek* (Fn. 91), Art. 2 Rn. 72 f.; *Stern* (Fn. 6), S. 231; *Zippelius/Würtenberger* (Fn. 16), § 21 Rn. 35.

94 *Dreier* (Fn. 41), Art. 2 I Rn. 78; *Kube* (Fn. 91), § 148 Rn. 66; *Sodan* (Fn. 10), Art. 2 Rn. 6.

95 *Antoni* (Fn. 93), Art. 1 Rn. 14; *Dreier* (Fn. 41), Art. 2 I Rn. 71 ff.; *Epping* (Fn. 9), Rn. 622; *Jarass* (Fn. 6), Art. 2 Rn. 42; *Kunig* (Fn. 91), Art. 2 Rn. 34; *Murswiek* (Fn. 91), Art. 2 Rn. 71; *Pieroth/Schlink* (Fn. 9), Rn. 397.

96 BVerfGE 54, 148 (155); 63, 131 (142); *Jarass* (Fn. 6), Art. 2 Rn. 42; *Zippelius/Würtenberger* (Fn. 16), § 21 Rn. 34.

Bereich[97]. Von diesem Standpunkt aus ist das Recht auf informationelle Selbstbestimmung, das als eine gelungene juristische Entdeckung betrachtet wird[98], eine Fortentwicklung des Persönlichkeitsschutzes[99]. Zu betonen ist, dass es kein neues Grundrecht ist[100]. Vielmehr stellt es einen notwendigerweise auf neuartige Gefährdungslagen in der Informationsgesellschaft reagierenden Bestandteil des Persönlichkeitsschutzes dar[101].

Die Einwilligung des Betroffenen steht der Verletzung des Rechts auf informationelle Selbstbestimmung entgegen[102]. Hierbei wird die Frage aufgeworfen, ob die Einwilligung des Betroffenen den Eingriff ausschließen kann oder ihn nur rechtfertigt. Im Schrifttum wird die Einwilligung gelegentlich als die Rechtfertigung des Eingriffs betrachtet[103]. Allerdings wäre es richtiger, dass die Einwilligung des Betroffenen den Eingriff ausschließt[104]. Denn die Einwilligung gehört begrifflich zur Selbstbestimmung. Insofern stellt die Einwilligung des Betroffenen auch eine Art der Ausübung des Rechts auf informationelle Selbstbestimmung dar. Hierbei liegt kein Eingriff vor.

Da das Recht auf informationelle Selbstbestimmung, wie bereits dargelegt, die „Befugnis des Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen", gewährleistet[105], lässt sich der Datenschutz daraus herleiten. Hierbei ist zu beachten, dass sich der hier diskutierte Datenschutz, der sich aus dem Recht auf informationelle Selbstbestimmung, und zwar aus dem allgemeinen Persönlichkeitsrecht, ergibt, nur auf personenbezogene Daten bezieht[106]. Unter dem Begriff personenbezogener Daten versteht man – wie § 3 Abs. 1 Bundesdatenschutzgesetz (BDSG)[107] definiert – „Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren

97 Vgl. BVerfGE 54, 148 (155); 63, 131 (142); *Sachs* (Fn. 5), B 2 Rn. 55 f.; *Zippelius/Würtenberger* (Fn. 16), § 21 Rn. 34.

98 So *Stern* (Fn. 6), S. 231; a. A. *Starck*, in: von Mangoldt/Klein/Starck, GG, Bd. 1, Art. 2 Rn. 114: Der Ausdruck „informationelles Selbstbestimmungsrecht" ist nur eine wenig glückliche Umschreibung eines aktuell gewordenen Aspekts des Art. 2 Abs. 1 GG, ohne dass dem neuen Wort irgendeine grundrechtssteigernde oder tatbestandspräzisierende Bedeutung zukäme.

99 *Albers* (Fn. 93), S. 178 f.; *Stern* (Fn. 6), S. 232.

100 *Stern* (Fn. 6), S. 232; vgl. auch *Starck* (Fn. 98), Art. 2 Rn. 114; a. A. *Ipsen* (Fn. 1), Rn. 317.

101 *Stern* (Fn. 6), S. 232; vgl. auch *Badura* (Fn. 93), C Rn. 36; *Manssen* (Fn. 1), Rn. 224.

102 *Rossi*, Informationszugangsfreiheit, S. 138.

103 So *Kloepfer* (Fn. 91), § 3 Rn. 55.

104 *Schmitt Glaeser* (Fn. 10), § 129 Rn. 98.

105 BVerfGE 65, 1 (43).

106 *Dreier* (Fn. 41), Art. 2 I Rn. 80; *Scherzberg*, Öffentlichkeit, S. 368; *Starck* (Fn. 98), Art. 2 Rn. 114; *Stern* (Fn. 6), S. 233 f.

107 Neue Fassung vom 14. 1. 2003 (BGBl. 2003 I, S. 66); zuletzt geändert durch Art. 1 des Gesetzes vom 14. 8. 2009 (BGBl. 2009 I, S. 2814).

natürlichen Person". Insoweit müssen personenbezogene Daten individualisiert oder wenigstens individualisierbar sein[108]. Darüber hinaus handelt es sich beim Datenschutz, der sich aus dem Recht auf informationelle Selbstbestimmung als Ausfluss des Persönlichkeitsrechts ergibt, nur um Daten natürlicher Personen[109], weil er Ausfluss des Persönlichkeitsschutzes ist[110]. Zudem können nur natürliche Personen die Grundrechtsträger des aus dem allgemeinen Persönlichkeitsrecht in Verbindung mit der Menschenwürde hergeleiteten Rechts auf informationelle Selbstbestimmung sein[111].

Schließlich stellt sich noch eine Frage: Sind anonymisierte Daten personenbezogen? Ausgehend vom objektiv-rechtlichen Grundrechtsgehalt des Rechts auf informationelle Selbstbestimmung muss der Staat Schutzvorkehrungen treffen, damit das Individuum nicht zum bloßen Informationsobjekt wird[112]. Insofern gehört die Anonymisierung zu solchen informationellen Schutzvorkehrungen[113], weil sie das Gewinnen von Einzelangaben über persönliche oder sachliche Verhältnisse erschweren kann. Teilweise wird vertreten, dass anonymisierte Daten keine personenbezogenen Daten sind[114]. Diese Auffassung ist wenig überzeugend. Gemäß § 3 Abs. 6 BDSG führt die Anonymisierung personenbezogener Daten nicht absolut dazu, dass die anonymisierten Daten nicht mehr einer Person zugeordnet werden können. Bei der Anonymisierung personenbezogener Daten kann es (nur) um die Erschwerung der Identifizierung des Betroffenen gehen. In dieser Situation wird die Bestimmbarkeit nicht durch die Anonymisierung vollständig beseitigt. Aus diesem Grund bleiben auch anonymisierte Daten noch personenbezogene Daten[115].

108 *Scherzberg* (Fn. 106), S. 368; *Stern* (Fn. 6), S. 234.

109 Vgl. *Hufen* (Fn. 1), § 12 Rn. 6; *Kloepfer* (Fn. 91), § 3 Rn. 48; *Masing*, VVDStRL 63 (2004), S. 377 (416); *Scherzberg* (Fn. 106), S. 368; *Schmitt Glaeser* (Fn. 10), § 129 Rn. 88.

110 *Stern* (Fn. 6), S. 233.

111 Vgl. *Hufen* (Fn. 1), § 12 Rn. 6; *Manssen* (Fn. 1), Rn. 232; a. A. *Ipsen* (Fn. 1), Rn. 319: „Datenerhebungen über juristische Personen berühren notwendig die Persönlichkeitssphäre auch natürlicher Personen, so dass schon aus diesem Grund die informationelle Selbstbestimmung auch juristischen Personen zukommen muss".

112 Vgl. *Ipsen* (Fn. 1), Rn. 321; *Kloepfer* (Fn. 91), § 3 Rn. 52.

113 Vgl. *Kloepfer* (Fn. 91), § 3 Rn. 52; *Masing* (Fn. 109), S. 377 (404); *Rossi* (Fn. 102), S. 137.

114 So *Gola/Schomerus*, BDSG, § 3 Rn. 43f.; *Roßnagel*, NZV 2006, S. 281 (282); *Stern* (Fn. 6), S. 234.

115 *Dammann*, in: Simitis, BDSG, § 3 Rn. 24; *Rossi* (Fn. 102), S. 137.

2. Rechtfertigung des Eingriffs aufgrund einfachen Gesetzesvorbehaltes

Ein Eingriff in das Recht auf informationelle Selbstbestimmung liegt vor, wenn der Staat personenbezogene Daten erhebt und verarbeitet[116]. Hierbei ist zu beachten, dass sich das Recht auf informationelle Selbstbestimmung zwar aus Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 GG ergibt, es jedoch nicht – wie die Garantie der Menschenwürde – „unantastbar" ist. Denn Art. 1 Abs. 1 GG wirkt hier nur als objektiv-rechtliche Interpretationsrichtlinie und bildet mit Art. 2 Abs. 1 GG kein Zwillingsgrundrecht[117]. Demzufolge kommt es bei der Beschränkungsmöglichkeit des Rechts auf informationelle Selbstbestimmung auf die Schrankenregelung des Art. 2 Abs. 1 GG an.

Gemäß Art. 2 Abs. 1 GG kann die verfassungsmäßige Ordnung eine Grenze des allgemeinen Persönlichkeitsrechts darstellen. Unter dem Begriff der verfassungsmäßigen Ordnung in Art. 2 Abs. 1 GG versteht man die Gesamtheit der Normen, die formell und materiell mit der Verfassung in Einklang stehen[118]. Dementsprechend ist das allgemeine Persönlichkeitsrecht ein Grundrecht mit einfachem Gesetzesvorbehalt[119]. Der Eingriff in das Recht auf informationelle Selbstbestimmung bedarf folglich einer gesetzlichen Grundlage. Zu betonen ist, dass die Anforderungen an die Bestimmtheit des Gesetzes, das das allgemeine Persönlichkeitsrecht einschränkt, relativ hoch sind[120]. In diesem Zusammenhang ist nur eine hinreichend bestimmte gesetzliche Grundlage geeignet, den Eingriff in das Recht auf informationelle Selbstbestimmung zu rechtfertigen[121].

3. Schutz der Verkehrsdaten der E-Mail-Kommunikation durch das Recht auf informationelle Selbstbestimmung

Die Verkehrsdaten (Verbindungsdaten) der Telekommunikation fallen über das Fernmeldegeheimnis hinaus auch in den Schutzbereich des Rechts auf informationelle Selbstbestimmung[122]. Bei der Versendung einer E-Mail muss der Absender seine E-Mail-Adresse und die E-Mail-Adresse des Emp-

116 *Michael/Morlok* (Fn. 8), Rn. 426; *Murswiek* (Fn. 91), Art. 2 Rn. 88; *Pieroth/Schlink* (Fn. 9), Rn. 405.

117 Vgl. *Meinke*, Verbindung, S. 57; *Murswiek* (Fn. 91), Art. 2 Rn. 63; *Starck* (Fn. 98), Art. 2 Rn. 15.

118 Vgl. BVerfGE 96, 10 (21); 90, 145 (172); 103, 197 (215); *Dreier* (Fn. 41), Art. 2 I Rn. 54; *Epping* (Fn. 9), Rn. 638; *Jarass* (Fn. 6), Art. 2 Rn. 17; *Kunig* (Fn. 91), Art. 2 Rn. 22; *Murswiek* (Fn. 91), Art. 2 Rn. 89; *Pieroth/Schlink* (Fn. 9), Rn. 408; *Starck* (Fn. 98), Art. 2 Rn. 25; *Stern* (Fn. 6), S. 263.

119 BVerfGE 65, 1 (44); 79, 256 (269); *Dreier* (Fn. 41), Art. 2 I Rn. 86; *Jarass* (Fn. 6), Art. 2 Rn. 59; *Murswiek* (Fn. 91), Art. 2 Rn. 90; *Pieroth/Schlink* (Fn. 9), Rn. 408.

120 BVerfGE 65, 1 (46); *Jarass* (Fn. 6), Art. 2 Rn. 58; *Starck* (Fn. 98), Art. 2 Rn. 23.

121 *Epping* (Fn. 9), Rn. 642; *Dreier* (Fn. 41), Art. 2 I Rn. 86; *Hufen* (Fn. 1), § 12 Rn. 11.

122 BVerfGE 115, 166 (188).

fängers in der Kopfzeile der E-Mail eingeben. Da E-Mail-Adressen die Funktion des Namensersatzes haben und Einzelangaben über persönliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person sind, lassen sie sich als personenbezogene Daten, die durch das Recht auf informationelle Selbstbestimmung geschützt werden, ansehen[123]. Zudem kann auch die IP-Adresse des Absenders bei der E-Mail-Kommunikation ermittelt werden. Berücksichtigt man, dass IP-Adressen Merkmale, die der Identifizierung der Person dienen können, enthalten, stellen auch sie personenbezogene Daten dar[124].

Durch eine präventiv-polizeiliche E-Mail-Überwachung werden die E-Mail-Adressen (ggf. auch die IP-Adressen), die sich einerseits unter dem Aspekt des Telekommunikationsrechts als Verkehrsdaten der Telekommunikation und andererseits aus der Sicht des Datenschutzrechts als personenbezogene Daten der Telekommunikationsteilnehmer betrachten lassen, vom Staat erhoben, gespeichert[125]. Insoweit stellt diese verdeckte polizeiliche Maßnahme zur Informationserhebung einen Eingriff in das Recht auf informationelle Selbstbestimmung dar. Die Rechtfertigung dieses Eingriffs bedarf einer hinreichend bestimmten gesetzlichen Grundlage.

III. Schutz vor der heimlichen Infiltration eines informationstechnischen Systems durch das „Computergrundrecht"?

1. Lückenfüllende Funktion als Ausgangspunkt des Grundrechts auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme

Das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme, das sich aus dem allgemeinen Persönlichkeitsrecht (Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 GG) ergibt, wurde vom Bundesverfassungsgericht in seinem Urteil vom 27. 2. 2008[126] zur Füllung von Lücken im Grundrechtsschutz entwickelt[127]. Wie bereits dargelegt wurde, endet der Schutz des Fernmeldegeheimnisses in dem Moment, in dem die übermittelten Informationen beim Empfänger angekommen sind.

123 Vgl. OLG Bamberg, MMR 2006, S. 481 (482 f.); *Dammann* (Fn. 115), § 3 Rn. 10; *Jandt*, MMR 2006, S. 652 (654); *Roßnagel* (Fn. 114), S. 281 (282); *Warg*, MMR 2006, S. 77 (80 f.).

124 AG Wuppertal, MMR 2008, S. 632; LG Berlin, MMR 2007, S. 799; *Czychowski/Nordemann*, NJW 2008, S. 3095 (3096); *Dammann* (Fn. 115), § 3 Rn. 10; *Roßnagel* (Fn. 114), S. 281 (282); a. A. *Hoeren*, NJW 2008, S. 3099 f.

125 Dazu siehe 2. Kapitel C II 1 b).

126 BVerfGE 120, 274 ff.

127 Dazu *Bär*, MMR 2008, S. 325 ff.; *Britz*, DÖV 2008, S. 411 ff.; *Eifert*, NVwZ 2008, S. 521 ff.; *Gusy*, DuD 2009, S. 33 ff.; *Hömig*, JURA 2009, S. 207 ff.; *Hornung*, CR 2008, S. 299 ff.; *Kutscha*, NJW 2008, S. 1042 ff.; *Michael/Morlok* (Fn. 8), Rn. 429; *Murswiek* (Fn. 91), Art. 2 Rn. 73b f.; *Roßnagel/Schnabel*, NJW 2008, S. 3534 ff.; *Sachs/Krings* (Fn. 77), S. 481 ff.

Aus diesem Grund erklärte das Bundesverfassungsgericht, dass das Fernmeldegeheimnis nicht die Inhalte und Umstände (Verkehrsdaten) der Telekommunikation, die nach Abschluss eines Kommunikationsvorgangs im Herrschaftsbereich eines Kommunikationsteilnehmers gespeichert würden, schütze[128]. Zudem verwies das Bundesverfassungsgericht darauf, dass der Schutz der Privatsphäre nicht alle Daten, sondern nur die Daten, die der Privatsphäre zuzuordnen seien, gewährleiste. Allerdings erstrecke sich die staatliche Infiltration des informationstechnischen Systems auch auf die nicht in die Privatsphäre fallenden Daten[129]. Ferner erläuterte das Bundesverfassungsgericht, dass das Recht auf informationelle Selbstbestimmung, dessen Schutzbereich weiter als der Schutz der Privatsphäre sei[130], nur vor einzelnen Datenerhebungen schütze[131]. Insoweit hätten sowohl das Fernmeldegeheimnis als auch das Recht auf informationelle Selbstbestimmung (sowie der Schutz der Privatsphäre) Schutzlücken[132].

Aus diesem Grund entwickelte das Bundesverfassungsgericht das sog. „Computergrundrecht": Da die Nutzung der Informationstechnik eine früher nicht absehbare Bedeutung für die Persönlichkeit und die Entfaltung des Einzelnen habe[133], würden die erwähnten Schutzlücken zu neuartigen Gefährdungen der Persönlichkeit in der Informationsgesellschaft führen. In diesem Zusammenhang sei das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme zu entwickeln, damit die Nutzung eines informationstechnischen Systems lückenlos gewährleistet werden könne. Dieses schütze das Interesse des Nutzers, dass die von einem informationstechnischen System erzeugten, verarbeiteten und gespeicherten Daten vertraulich bleiben[134]. Dieses Grundrecht sei umfassend und subsidiär gegenüber dem Fernmeldegeheimnis und dem Recht auf informationelle Selbstbestimmung[135].

2. Grundrechtsdogmatische Probleme des Grundrechts auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme

Es ist sehr zweifelhaft, ob die Schaffung des Grundrechts auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme notwendig war. Der Argumentation, dass die Telekommunikationsdaten

128 BVerfGE 120, 274 (307 f.).
129 BVerfGE 120, 274 (311).
130 BVerfGE 120, 274 (311 f.).
131 BVerfGE 120, 274 (313).
132 BVerfGE 120, 274 (308, 312 f.).
133 BVerfGE 120, 274 (303).
134 BVerfGE 120, 274 (314).
135 BVerfGE 120, 274 (302).

nach Abschluss des Telekommunikationsvorgangs nicht durch das Fernmeldegeheimnis (Art. 10 Abs. 1 GG) geschützt werden, lässt sich folgen. Der Auffassung, dass das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme die Schutzlücke des Privatsphäreschutzes und des Rechts auf informationelle Selbstbestimmung füllen müsse, ist aber nicht zuzustimmen.

Der Schutz der Privatsphäre ergibt sich aus dem allgemeinen Persönlichkeitsrecht (Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 GG)[136]. Wenn Daten nicht in die Privatsphäre fallen, sind sie i. d. R. vom Schutz des allgemeinen Persönlichkeitsrechts nicht erfasst. Ausgehend hiervon ist schwer zu verstehen, warum das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme, das nach der Auffassung des Bundesverfassungsgerichts zur Füllung der Lücke des Privatsphäreschutzes (= Daten, die sich nicht in der Privatsphäre befinden) dient[137], seine Wurzel im allgemeinen Persönlichkeitsrecht, das die Privatsphäre schützt, finden kann. Auch wenn das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme wirklich unabhängig vom Schutz der privaten Daten (Privatsphäre) wäre und somit die bloße Integrität informationstechnischer Systeme gewährleisten würde[138], ist der persönliche Schutzbereich dieses Grundrechts fragwürdig. Denn ein informationstechnisches System selbst kann keinesfalls als ein Grundrechtsträger angesehen werden[139].

Die Behauptung des Bundesverfassungsgerichts, dass das Recht auf informationelle Selbstbestimmung eine Schutzlücke habe, basiert auf dem Argument, dass das Recht auf informationelle Selbstbestimmung nur vor einzelnen Datenerhebungen schütze[140]. Jedoch findet eine solche Beschränkung der Reichweite des Rechts auf informationelle Selbstbestimmung keine Stütze[141]. Diese zweifelhafte Behauptung des Bundesverfassungsgerichts übersieht, dass sich das Recht auf informationelle Selbstbestimmung aus dem Auffanggrundrecht des Art. 2 Abs. 1 GG[142] ergibt. Da das Recht auf informationelle Selbstbestimmung seine Grundlage in diesem Auffanggrundrecht findet, soll es wegen des umfassenden (sachlichen) Grundrechts-

136 BVerfGE 90, 255 (260); *Dreier* (Fn. 41), Art. 2 I Rn. 70; *Jarass* (Fn. 6), Art. 2 Rn. 47.

137 Vgl. BVerfGE 120, 274 (311).

138 Kritisch dazu *Eifert* (Fn. 127), S. 521 (522).

139 *Eifert* (Fn. 127), S. 521 (522).

140 Vgl. BVerfGE 120, 274 (312 f.).

141 Kritisch auch *Britz* (Fn. 127), S. 411 (413); *Manssen* (Fn. 1), Rn. 225; *Sachs/Krings* (Fn. 77), S. 481 (483 f.).

142 Art. 2 Abs. 1 GG schützt sowohl die allgemeine Handlungsfreiheit als auch das allgemeine Persönlichkeitsrecht. Beide Rechte haben Auffangfunktion (vgl. *Murswiek* (Fn. 91), Art. 2 Rn. 10, 66; a. A. *Epping* (Fn. 9), Rn. 648).

tatbestands des Art. 2 Abs. 1 GG die personenbezogenen Daten umfassend schützen. Ob die staatliche Tätigkeit eine einzelne Datenerhebung oder eine Infiltration des informationstechnischen Systems, durch die der Staat sich einen äußerst großen Datenbestand verschaffen kann, darstellt, spielt keine Rolle für den Schutzumfang des Rechts auf informationelle Selbstbestimmung, das in Bezug auf den Datenschutz eine umfangreiche Gewährleistung darstellt. Vertritt man, dass das Recht auf informationelle Selbstbestimmung hinsichtlich des Datenschutzes eine Schutzlücke habe, steht diese Ansicht dem uferlosen (sachlichen) Grundrechtstatbestand des Art. 2 Abs. 1 GG entgegen. Ferner führt die unzutreffende Meinung, dass das sich aus Art. 2 Abs. 1 GG ergebende Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme die Schutzlücke des Rechts auf informationelle Selbstbestimmung, das ebenfalls aus Art. 2 Abs. 1 GG hergeleitet wird, füllen könne, zu einer befremdlichen Konsequenz: Art. 2 Abs. 1 GG kann die Schutzlücke des Art. 2 Abs. 1 GG füllen. Deswegen ist festzuhalten, dass das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme nur als Unterfall der informationellen Selbstbestimmung angesehen werden kann[143]. Seine grundrechtliche Eigenständigkeit ist zu verneinen[144].

3. Keine Notwendigkeit des neuen Computergrundrechts hinsichtlich der präventiv-polizeilichen E-Mail-Überwachung

Zwar stellt der E-Mail-Verkehr die Nutzung von Informationstechnik dar, jedoch ist die Schaffung eines neuen Computergrundrechts gegen eine präventiv-polizeiliche E-Mail-Überwachung nicht notwendig. Wie oben bereits dargelegt wurde, schützt das Recht auf informationelle Selbstbestimmung umfassend die personenbezogenen Daten. Diese umfassende grundrechtliche Gewährleistung gilt auch für die Daten, die durch E-Mail übertragen und im Mailserver gespeichert werden. Aus der Sicht des Datenschutzes stellt die aus dem Recht auf informationelle Selbstbestimmung hergeleitete Gewährleistung einen hinreichenden Grundrechtschutz gegen die präventiv-polizeiliche E-Mail-Überwachung dar. Die staatliche heimliche Datenerhebung durch präventiv-polizeilichen Zugriff auf die E-Mail-Kommunikation erweitert den Anwendungsbereich des Rechts auf informationelle Selbstbestimmung in der virtuellen Welt. Diese verdeckte polizeiliche Maßnahme eröffnet allerdings keine Möglichkeit eines neuen

143 *Britz* (Fn. 127), S. 411 (413 f.); *Eifert* (Fn. 138), S. 521 (522); a. A. *Hoffmann-Riem*, JZ 2008, S. 1009 (1015 f., 1019); *Kube* (Fn. 91), § 148 Rn. 70.

144 *Britz* (Fn. 127), S. 411 (413 f.); *Eifert* (Fn. 138), S. 521 (522); *Sachs/Krings* (Fn. 77), S. 481 (483); wohl auch *Murswiek* (Fn. 91), Art. 2 Rn. 73c; *Sodan* (Fn. 10), Art. 10 Rn. 6; a. A. *Hoffmann-Riem* (Fn. 143), S. 1009 (1015 f., 1019); *Kube* (Fn. 91), § 148 Rn. 70; *Michael/Morlok* (Fn. 8), Rn. 429.

Computergrundrechts, das vor staatlicher Datenerhebung im Internet schützt.

Zudem ist ein neues Computergrundrecht, das sich gegen die präventiv-polizeiliche E-Mail-Überwachung richtet, aber keinen Datenschutz betrifft, grundrechtsdogmatisch sehr zweifelhaft. Wenn ein solches Computergrundrecht, das keinen Zusammenhang zum Datenschutz hat, anerkannt werden könnte, ist es unter dem Aspekt des sachlichen Grundrechtstatbestands schwer zu verstehen, was der Schutzgegenstand dieses Grundrechts eigentlich ist[145]. Falls das Computergrundrecht sachlich – ausgehend von seinem Namen – nur die Integrität informationstechnischer Systeme schützt, ist es aus dem Gesichtspunkt der Grundrechtsberechtigung problematisch, weil das Internet oder der Mailserver selbst nicht als ein Grundrechtsträger betrachtet werden kann. Der Grundrechtsschutz gegen eine präventiv-polizeiliche E-Mail-Überwachung ist nur sinnvoll, wenn eine Verknüpfung mit Teilnehmern der E-Mail-Kommunikation vorliegt. Dies bezieht sich auf den Datenschutz im Internet. Er fällt in den Schutzbereich des Rechts auf informationelle Selbstbestimmung.

IV. Garantie des Eigentums?

1. Geschäfts- und Betriebsgeheimnis als Schutzgegenstand des Eigentums

Art. 14 Abs. 1 Satz 1 GG schützt das Eigentum. Hierbei ist zu betonen, dass der verfassungsrechtliche Eigentumsbegriff nicht mit dem zivilrechtlichen Begriff identisch ist[146]. Unter dem Begriff des Eigentums im Sinne des Art. 14 Abs. 1 Satz 1 GG werden alle privatrechtlichen vermögenswerten Rechte verstanden[147]. Insoweit entsprechen Geschäfts- und Betriebsgeheimnisse dem Begriff des Eigentums im Sinne des Art. 14 Abs. 1 Satz 1 GG, weil sie einen durch den Einsatz von Kapital und Arbeit erwirtschafteten Vermögenswert darstellen[148]. Dabei geht es beispielsweise um Aus-

145 Zur Unklarheit des Schutzgegenstands des „Computergrundrechts“ *Sachs/Krings* (Fn. 77), S. 481 (484).

146 *Antoni* (Fn. 93), Art. 14 Rn. 4; *Ipsen* (Fn. 1), Rn. 721; *Manssen* (Fn. 1), Rn. 640; *Sodan* (Fn. 10), Art. 14 Rn. 7; *Wieland*, in: Dreier, GG, Bd. 1, Art. 14 Rn. 38; *Zippelius/Würtenberger* (Fn. 16), § 31 Rn. 17.

147 BVerfGE 83, 201 (209); *Depenheuer*, in: von Mangoldt/Klein/Starck, GG, Bd. 1, Art. 14 Rn. 113; *Hofmann* (Fn. 11), Art. 14 Rn. 12; *Jarass* (Fn. 6), Art. 14 Rn. 7; *Manssen* (Fn. 1), Rn. 640; *Michael/Morlok* (Fn. 8), Rn. 381; *Pieroth/Schlink* (Fn. 9), Rn. 981; *Sodan* (Fn. 10), Art. 14 Rn. 8; *Wendt*, in: Sachs, GG, Art. 14 Rn. 22; *Wieland* (Fn. 146), Art. 14 Rn. 46; *Zippelius/Würtenberger* (Fn. 16), § 31 Rn. 17.

148 *Breuer*, in: Isensee/Kirchhof, HStR, Bd. 6, 2. Aufl., § 148 Rn. 26; *Jarass* (Fn. 6), Art. 14 Rn. 18; *Rossi* (Fn. 102), S. 141; vgl. auch *Depenheuer* (Fn. 147), Art. 14 Rn. 134.

schreibungsunterlagen, Vertragsabschlüsse, Daten über Produktionsmittel und Marktstrategien[149].

Wie bereits dargelegt wurde, schützt das Recht auf informationelle Selbstbestimmung nur die personenbezogenen Daten. Mit anderen Worten: Nur natürliche Personen können Träger des Rechts auf informationelle Selbstbestimmung sein. Dies bedeutet allerdings nicht, dass die Daten der Unternehmen nicht durch Grundrechte geschützt werden. Jedenfalls lassen sich Geschäfts- und Betriebsgeheimnisse als Schutzgegenstand des Eigentums im Sinne des Art. 14 Abs. 1 Satz 1 GG ansehen[150]. Aus diesem Grund kann auch eine juristische Person (des Privatrechts) der Träger der Eigentumsgarantie sein[151].

2. Schutz des Eigentums vor präventiv-polizeilicher E-Mail-Überwachung?

Die meisten polizei- und ordnungsgesetzlichen Ermächtigungsvorschriften zur Telekommunikationsüberwachung erlauben sowohl die Erhebung der Telekommunikationsverkehrsdaten als auch die Gewinnung der Telekommunikationsinhalte[152]. Berücksichtigt man, dass die Zielperson, deren E-Mail-Kommunikation zu überwachen ist, per E-Mail einen kommerziellen Informationsaustausch durchführen kann, ist es denkbar, dass auch betriebsbezogene Daten durch eine präventiv-polizeiliche E-Mail-Überwachung, die eine Maßnahme zur Erhebung der Inhalte der E-Mail-Kommunikation darstellt, betroffen werden. In der Tat kann die Polizei nicht vorhersehen, ob der zu überwachende E-Mail-Verkehr nur personenbezogene Daten oder darüber hinaus noch betriebsbezogene Daten umfasst.

Der Umstand, dass die betriebsbezogenen Daten, die durch Art. 14 Abs. 1 Satz 1 GG geschützt werden, durch den präventiv-polizeilichen Zugriff auf die E-Mail-Kommunikation betroffen werden, führt aber nicht dazu, dass von einem Eingriff in die Eigentumsgarantie auszugehen ist. Ein solcher liegt nur vor, wenn eine geschützte Rechtsposition entzogen wird oder die Eigentümerbefugnisse (Nutzung, Verfügung oder Veräußerung) beschränkt werden[153]. Durch die präventiv-polizeiliche E-Mail-Überwachung können

149 *Scherzberg* (Fn. 106), S. 373.

150 *Hufen* (Fn. 1), § 12 Rn. 6. Nach der Auffassung des Bundesverfassungsgerichts lässt sich der Schutz der Geschäfts- und Betriebsgeheimnisse auch aus der Berufsfreiheit (Art. 12 Abs. 1 GG) herleiten (vgl. BVerfGE 115, 205 (229 ff.); ebenso *Zippelius/Würtenberger* (Fn. 16), § 30 Rn. 4).

151 *Antoni* (Fn. 93), Art. 14 Rn. 3; *Hofmann* (Fn. 11), Art. 14 Rn. 3; *Hufen* (Fn. 1), § 38 Rn. 18; *Jarass* (Fn. 6), Art. 14 Rn. 27; *Sodan* (Fn. 10), Art. 14 Rn. 20; *Wendt* (Fn. 147), Art. 14 Rn. 16; *Wieland* (Fn. 146), Art. 14 Rn. 68.

152 In Baden-Württemberg bezieht sich die präventiv-polizeiliche Telekommunikationsüberwachung nach § 23a Abs. 1 bwPolG nur auf die Erhebung der Telekommunikationsverkehrsdaten.

153 *Jarass* (Fn. 6), Art. 14 Rn. 29; *Manssen* (Fn. 1), Rn. 649; *Wendt* (Fn. 147), Art. 14 Rn. 52.

zwar die den Vermögenswert darstellenden betriebsbezogenen Daten (Geschäfts- und Betriebsgeheimnisse) erfasst werden. Allerdings entzieht der präventiv-polizeiliche Zugriff auf die E-Mail-Kommunikation die vermögenswerte Rechtsposition der Zielperson nicht. Auch Eigentümerbefugnisse zur Nutzung oder Verfügung der betriebsbezogenen Daten werden durch die präventiv-polizeiliche Überwachung eines E-Mail-Verkehrs nicht beeinträchtigt. Insoweit stellt die präventiv-polizeiliche E-Mail-Überwachung keinen Eingriff in das Eigentum der Kommunikationsteilnehmer dar. Obwohl ein Eigentumseingriff durch die Offenbarung der betriebsbezogenen Daten möglich ist[154], kann jedoch eine solche Eingriffskonstellation, die zur staatlichen Preisgabe der privaten Geschäfts- und Betriebsgeheimnisse führt, nicht in gleicher Weise für eine polizeiliche Überwachung der betriebsbezogenen Daten gelten.

V. Eingriff in die Meinungs- und Informationsfreiheit durch präventiv-polizeiliche E-Mail-Überwachung?

Es stellt sich die Frage, ob die präventiv-polizeiliche E-Mail-Überwachung in den Schutzbereich des Art. 5 Abs. 1 S. 1 GG eingreift. Art. 5 Abs. 1 Satz 1 GG schützt die Meinungs- und Informationsfreiheit. Zunächst gewährleistet Art. 5 Abs. 1 Satz 1 Hs. 1 GG die Äußerung und Verbreitung von Meinungen. Ferner hat jeder gemäß Art. 5 Abs. 1 Satz 1 Hs. 2 GG das Recht, sich aus allgemein zugänglichen Quellen ungehindert zu unterrichten. Damit fallen sowohl die Kommunikationsabgabe als auch die Kommunikationsaufnahme in den Schutzbereich des Art. 5 Abs. 1 Satz 1 GG[155].

Das Absenden einer E-Mail kann mit der Äußerung und Verbreiten einer Meinung einhergehen. Zudem geht es beim Empfang einer E-Mail um die Kommunikationsaufnahme. Dies sieht so aus, als ob eine Grundrechtskonkurrenz zwischen Art. 10 Abs. 1 GG (Fernmeldegeheimnis) und Art. 5 Abs. 1 Satz 1 GG (Meinungs- und Informationsfreiheit) bei der Durchführung einer präventiv-polizeilichen E-Mail-Überwachung bestünde. Allerdings ist der Auffassung, dass die präventiv-polizeiliche E-Mail-Überwachung in den Schutzbereich des Art. 5 Abs. 1 Satz 1 GG eingreife, nicht zu folgen. Zunächst ist von Bedeutung, dass das Fernmeldegeheimnis und die Meinungsfreiheit unterschiedliche Schutzbereiche haben[156]: Das Fernmeldegeheimnis schützt die Vertraulichkeit der Telekommunikation. Im

154 Ein solcher Eigentumseingriff wird vor allem im Bereich des Informationsfreiheitsgesetzes zu Grunde gelegt. Daher lässt sich die Eigentumsgarantie als eine Grenze der Informationszugangsfreiheit ansehen (vgl. dazu *Kloepfer* (Fn. 91), § 3 Rn. 56 ff.; *Kugelmann*, NJW 2005, S. 3609 (3612); *Rossi* (Fn. 102), S. 140 ff.; *Scherzberg* (Fn. 106), S. 372 ff.; *Schmitz/Jastrow*, NVwZ 2005, S. 984 (993); *Schoch*, Die Verwaltung 35 (2002), S. 149 (166 f.)).

155 *Jarass* (Fn. 6), Art. 5 Rn. 1.

156 Nach *H. Bethge* lässt sich das Fernmeldegeheimnis als ein Korrespondenzgrundrecht der Meinungsfreiheit ansehen (vgl. *Bethge*, in: Sachs, GG, Art. 5 Rn. 48b).

Vergleich dazu gewährleistet die Meinungsfreiheit die Verlässlichkeit der freien Kommunikation[157]. So läge ein Eingriff in die Meinungsfreiheit vor, wenn die Meinungsäußerung per E-Mail durch staatliche Anordnung verboten wird. Jedoch kann die präventiv-polizeiliche E-Mail-Überwachung nur die Nachrichten der E-Mail-Kommunikation, die technisch auf den digitalen Datenpaketen basieren, erheben. Der präventiv-polizeiliche Zugriff auf den E-Mail-Verkehr führt nicht zur Verhinderung der E-Mail-Kommunikation. Bei der Durchführung einer präventiv-polizeilichen E-Mail-Überwachung wird mithin nur die Vertraulichkeit der Telekommunikation, nicht aber die Verlässlichkeit der freien Kommunikation beeinträchtigt. Zudem sind die Nachrichten der E-Mail in der Regel nicht zur Veröffentlichung bestimmt. Zwar lässt sich das Internet als allgemein zugängliche Informationsquelle im Sinne des Art. 5 Abs. 1 Satz 1 Hs. 2 GG ansehen[158], jedoch ist es zweifelhaft, ob der Empfang einer E-Mail „aus allgemein zugänglichen Quellen" erfolgt. Auch wenn dieses Bedenken beseitigt werden könnte, geht es bei der Durchführung einer präventiv-polizeilichen E-Mail-Überwachung gleichwohl nicht um den Eingriff in die Informationsfreiheit. Denn die präventiv-polizeiliche E-Mail-Überwachung führt nicht zur Verhinderung der Kommunikationsaufnahme, sondern nur zum staatlichen Mitlesen der Kommunikationsinhalte. Zusammenfassend lässt sich festhalten, dass die präventiv-polizeiliche E-Mail-Überwachung nicht in Schutzbereiche der Meinungs- und Informationsfreiheit eingreift.

VI. Grundrechtskonkurrenz

Da die E-Mail-Kommunikation sowohl durch das Fernmeldegeheimnis als auch durch das Recht auf informationelle Selbstbestimmung geschützt wird, ist auf Fragen der Grundrechtskonkurrenz einzugehen. Wie bereits dargelegt, schützt das Fernmeldegeheimnis nicht nur die Vertraulichkeit des Telekommunikationsinhalts, sondern auch die Vertraulichkeit des Telekommunikationsvorgangs. Zeitlich endet der Schutz des Fernmeldegeheimnisses, wenn die übermittelten Informationen beim Empfänger angekommen sind. Deswegen fallen die Inhalte und die Verkehrsdaten der E-Mail-Kommunikation im Laufe des Übertragungsvorgangs einerseits in den Schutzbereich des Fernmeldegeheimnisses. Andererseits werden die

157 *Hermes* (Fn. 6), Art. 10 Rn. 95. Falls die Meinungsäußerung oder -verbreitung durch staatliche Maßnahme verboten, behindert oder geboten wird, d. h. wenn die Verlässlichkeit des freien Meinungsaustauschs nicht gesichert ist, liegt ein Eingriff in die Meinungsfreiheit vor (vgl. *Jarass* (Fn. 6), Art. 5 Rn. 9; *Schulze-Fielitz*, in: Dreier, GG, Bd. 1, Art. 5 I, II Rn. 124).

158 *Bethge* (Fn. 156), Art. 5 Rn. 54; *Hufen* (Fn. 1), § 26 Rn. 6; *Ipsen* (Fn. 1), Rn. 431; *Jarass* (Fn. 6), Art. 5 Rn. 16; *Kannengießer*, in: Schmidt-Bleibtreu/Hofmann/Hopfauf, GG, Art. 5 Rn. 9; *Schoch*, JURA 2008, S. 25 (28); *Schulze-Fielitz* (Fn. 157), Art. 5 I, II Rn. 77; *Sodan* (Fn. 10), Art. 5 Rn. 13; *Starck* (Fn. 98), Art. 5 Rn. 42; *Stern* (Fn. 6), S. 1404; *Zippelius/Würtenberger* (Fn. 16), § 26 Rn. 45.

Verkehrsdaten zugleich durch das Recht auf informationelle Selbstbestimmung geschützt, soweit sie personenbezogene Daten darstellen[159]. Hinsichtlich des Verhältnisses von Art. 10 Abs. 1 und Art. 2 Abs. 1 GG ist das Fernmeldegeheimnis lex specialis gegenüber dem Recht auf informationelle Selbstbestimmung[160]. Das Fernmeldegeheimnis (spezielle Garantie) verdrängt aufgrund der unechten Grundrechtskonkurrenz bzw. Gesetzeskonkurrenz[161] das Recht auf informationelle Selbstbestimmung (allgemeine Gewährleistung).

Sobald der Empfänger die E-Mail aus dem Mailserver abgerufen hat, endet nicht nur der Telekommunikationsvorgang, sondern auch der Schutz des Fernmeldegeheimnisses. Ab diesem Zeitpunkt werden die Verkehrsdaten der E-Mail-Kommunikation nicht durch das Fernmeldegeheimnis (Art. 10 Abs. 1 GG), sondern durch das Recht auf informationelle Selbstbestimmung (Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 GG) geschützt, soweit sie personenbezogene Daten darstellen[162]. Zu betonen ist, dass sich die präventivpolizeiliche E-Mail-Überwachung nicht auf die nach Abschluss des Telekommunikationsvorgangs durchgeführte Informationserhebung bezieht. Zwar könnte die Polizei nach Abschluss des Telekommunikationsvorgangs weiterhin durch heimlichen Zugriff auf Computer-Festplatten der Telekommunikationsteilnehmer die Inhalte oder Verkehrsdaten einer abgeschlossenen E-Mail-Kommunikation erheben, jedoch ist der Eingriff in das Recht auf informationelle Selbstbestimmung nach Abschluss des Telekommunikationsvorgangs kein Thema der präventiv-polizeilichen E-Mail-Überwachung. Denn die polizeiliche versteckte Informationserhebung, die durch Zugriff auf Computer-Festplatten der Telekommunikationsteilnehmer nach Abschluss des Telekommunikationsvorgangs durchgeführt wird, entspricht begrifflich nicht der Telekommunikationsüberwachung[163]. Vielmehr stellt eine solche polizeiliche Informationserhebung eine „Online-Durchsuchung" dar. Die Abgrenzung zwischen der Telekommunikationsüberwachung und der „Online-Durchsuchung" ist hier von Bedeutung[164].

159 Z. B. die E-Mail-Adressen von Absender und Empfänger.

160 BVerfGE 100, 313 (358); 107, 299 (312); 110, 33 (53); 113, 348 (364); BVerfG, NJW 2007, S. 351 (354 f.); *Gusy* (Fn. 5), Art. 10 Rn. 103; *Hermes* (Fn. 6), Art. 10 Rn. 94; *Jarass* (Fn. 6), Art. 10 Rn. 2; *Löwer* (Fn. 6), Art. 10 Rn. 55; *Meininghaus* (Fn. 74), S. 75; *Pagenkopf* (Fn. 9), Art. 10 Rn. 52.

161 Vgl. dazu *Dreier* (Fn. 41), Vorb. Rn. 155; *Jarass* (Fn. 6), Vorb. vor Art. 1 Rn. 18; *Michael/Morlok* (Fn. 8), Rn. 54; *Sachs* (Fn. 41), vor Art. 1 Rn. 136; *Sodan* (Fn. 10), Art. 1 Vorb. Rn. 3.

162 *Hornung*, DuD 2007, S. 575 (578 f.).

163 Vgl. BT-Drs. 16/9588, S. 70. Zur Abgrenzung zwischen der Online-Durchsuchung und der Überwachung einer Internet-basierten Telekommunikation siehe auch 2. Kapitel C I 3.

164 Es wird vertreten, dass die Online-Durchsuchung zwar von der Telekommunikationsüberwachung zu unterscheiden sei. Jedoch stelle eine Online-Durchsuchung auch einen Eingriff in das Fernmeldegeheimnis des Art. 10 Abs. 1 GG dar. Beispielsweise verstoße das uneingeschränkte nachträgliche Auslesen des Inhalts von E-Mail-Korrespondenz im Wege der

B. Eingriff in die Berufsfreiheit der Diensteanbieter

Die Durchführung einer präventiv-polizeilichen E-Mail-Überwachung greift nicht nur in Grundrechte der Telekommunikationsteilnehmer ein. Da die polizei- und ordnungsgesetzlichen Ermächtigungsvorschriften zur Telekommunikationsüberwachung den Diensteanbietern eine Mitwirkungspflicht auferlegen[165], kommt auch ein Eingriff in Art. 12 Abs. I GG in Betracht, den es ggf. auf seine Rechtfertigung hin zu befragen gilt[166].

I. Einheitliches Grundrecht der Berufsfreiheit

Die Berufsfreiheit wird durch Art. 12 Abs. 1 GG geschützt. Unter dem Begriff des Berufs versteht man jede auf Erwerb gerichtete Tätigkeit, die der Schaffung und Erhaltung einer Lebensgrundlage dient bzw. dazu beiträgt[167]. Der ein einheitliches Grundrecht der Berufsfreiheit enthaltende

---

Online-Durchsuchung gegen das Fernmeldegeheimnis, weil sich hierdurch Kenntnis von einer – wenn auch bereits abgeschlossenen – Telekommunikation verschafft werde (vgl. *Huber*, NVwZ 2007, S. 880 (882 f.)). Diese Auffassung kann nicht überzeugen. Der Schutz des Fernmeldegeheimnisses setzt voraus, dass eine laufende Telekommunikation vorliegt. Deswegen ist der Schutzbereich des Fernmeldegeheimnisses nicht (mehr) eröffnet, sobald die Telekommunikation (= Schutzgegenstand des Fernmeldegeheimnisses) schon abgeschlossen ist. Diese Konsequenz gilt auch für den Schutz der Inhaltsdaten und Verkehrsdaten einer beendeten Telekommunikation. Denn das Fernmeldegeheimnis schützt (nur) die Inhalte und Umstände der laufenden Telekommunikation (vgl. BVerfGE 120, 274 (307 f.)). Die Daten, die sich auf eine bereits abgeschlossene Telekommunikation beziehen, stellen keine Inhalte und Umstände der laufenden Telekommunikation dar. Bei der Online-Durchsuchung ist das Fernmeldegeheimnis folglich nicht betroffen (BVerfGE 120, 274 (307 f.); *Hornung* (Fn. 162), S. 575 (578); *Rux*, JZ 2007, S. 285 (292)).

165 § 23a Abs. 5 bwPolG; Art. 34b bayPAG; § 33b Abs. 6 bbgPolG; § 10a Abs. 3 hambGDatPol; § 15a Abs. 1, Abs. 2 hessSOG; § 34a Abs. 6 mvSOG; § 33a Abs. 7 ndsSOG; § 31 Abs. 6 rpPOG; § 28b Abs. 2 saarlPolG; § 185a Abs. 4 shLVwG; § 34a Abs. 1 thürPAG.

166 Ein Eingriff in die Eigentumsgarantie der E-Mail-Provider kommt nicht in Betracht. Denn die technische Mithilfe der Diensteanbieter, die in Polizei- und Ordnungsgesetzen vorgeschriebenen wird, stellt keine unentgeltliche Indienstnahme Privater dar (dazu siehe 6. Kapitel B IV). Zwar wird in der Literatur vertreten, dass die Indienstnahme Privater in das durch Art. 14 GG geschützte Grundrecht eingreife, wenn dadurch die Innehabung und Verwendung vorhandener Vermögensgüter begrenzt werde (*Depenheuer* (Fn. 147), Art. 14 Rn. 136), jedoch geht es bei der technischen Mithilfe der E-Mail-Provider nicht um das Erworbene, sondern um den Erwerb. Demzufolge liegt kein Eingriff in die Eigentumsgarantie vor (vgl. *Jarass*, VSSR 2007, S. 103 (108)).

167 BVerfGE 7, 377 (397); 54, 301 (313); 102, 197 (212); 105, 252 (265); 111, 10 (28); 115, 205 (229); *Epping* (Fn. 9), Rn. 364; *Hufen* (Fn. 1), § 35 Rn. 6; *Ipsen* (Fn. 1), Rn. 635; *Jarass* (Fn. 6), Art. 12 Rn. 4; *Mann*, in: Sachs, GG, Art. 12 Rn. 45; *Manssen*, in: von Mangoldt/Klein/Starck, GG, Bd. 1, Art. 12 Rn. 37; *Michael/Morlok* (Fn. 8), Rn. 340.

Art. 12 Abs. 1 GG[168] gewährleistet die Berufswahlfreiheit, die Berufsausübungsfreiheit und die Arbeitsplatzwahlfreiheit. Die Berufswahlfreiheit betrifft die Entscheidung, einen Beruf zu ergreifen oder nicht zu ergreifen[169]. Bei der Berufsausübungsfreiheit geht es um die Bestimmung von Form, Mittel, Umfang und Inhalt der Berufstätigkeit[170]. Die Arbeitsplatzwahlfreiheit erstreckt sich auf das Recht, einen konkreten Arbeitsplatz nach eigener Wahl anzunehmen, beizubehalten und aufzugeben[171]. Zwar scheint es nach dem Wortlaut des Art. 12 Abs. 1 Satz 2 GG, als ob der Gesetzesvorbehalt nur für die Berufsausübungsfreiheit gelten würde, jedoch betrifft er auch die Berufswahlfreiheit und die Arbeitsplatzwahlfreiheit, weil die Berufsfreiheit (Art. 12 Abs. 1 GG) ein einheitliches Grundrecht darstellt[172]. In Bezug auf den persönlichen Schutzbereich sind alle Deutschen (im Sinne des Art. 116 GG) Grundrechtsträger des Art. 12 Abs. 1 GG. Nach Art. 19 Abs. 3 GG kann das Grundrecht der Berufsfreiheit auch auf juristische Personen des Privatrechts anwendbar sein[173].

Ein (klassischer) Eingriff in die Berufsfreiheit liegt vor, wenn die berufliche Tätigkeit oder die Berufswahl durch Regelungen, die sich unmittelbar auf die Berufstätigkeit beziehen, geregelt oder beeinträchtigt wird (Eingriff durch Regelung mit subjektiv berufsregelnder Tendenz)[174]. Dazu gehören verbindliche Vorgaben hinsichtlich des Ob und des Wie einer bestimmten

168 Vgl. dazu BVerfGE 7, 377 (400); *Breuer*, in: Isensee/Kirchhof, HStR, Bd. 6, 2. Aufl., § 147 Rn. 32; *Dietlein*, in: Stern, Staatsrecht, Bd. IV/1, S. 1770; *Epping* (Fn. 9), Rn. 367; *Hufen* (Fn. 1), § 35 Rn. 5; *Ipsen* (Fn. 1), Rn. 634; *Jarass* (Fn. 6), Art. 12 Rn. 1; *Mann* (Fn. 167), Art. 12 Rn. 14; *Manssen* (Fn. 167), Art. 12 Rn. 2; *Pieroth/Schlink* (Fn. 9), Rn. 878; *Wieland* (Fn. 146), Art. 12 Rn. 41; *Zippelius/Würtenberger* (Fn. 16), § 30 Rn. 23.

169 *Breuer* (Fn. 168), § 147 Rn. 56; *Epping* (Fn. 9), Rn. 369; *Jarass* (Fn. 6), Art. 12 Rn. 8; *Manssen* (Fn. 167), Art. 12 Rn. 50; *Pieroth/Schlink* (Fn. 9), Rn. 882; *Mann* (Fn. 167), Art. 12 Rn. 78. Deswegen betrifft die Berufswahl das „Ob" der beruflichen Betätigung (*Sodan* (Fn. 10), Art. 12 Rn. 14).

170 *Breuer* (Fn. 168), § 147 Rn. 57; *Epping* (Fn. 9), Rn. 370; *Jarass* (Fn. 6), Art. 12 Rn. 8; *Mann* (Fn. 167), Art. 12 Rn. 79; *Manssen* (Fn. 167), Art. 12 Rn. 65 ff. Insoweit betrifft die Berufsausübung das „Wie" der beruflichen Betätigung (*Dietlein* (Fn. 168), S. 1800; *Sodan* (Fn. 10), Art. 12 Rn. 14).

171 *Breuer* (Fn. 168), § 147 Rn. 66; *Jarass* (Fn. 6), Art. 12 Rn. 9; *Mann* (Fn. 167), Art. 12 Rn. 86; *Manssen* (Fn. 167), Art. 12 Rn. 57.

172 BVerfGE 54, 237 (246); 84, 133 (148); 85, 360 (373); 110, 304 (321); *Dietlein* (Fn. 168), S. 1883 f.; *Epping* (Fn. 9), Rn. 388; *Hufen* (Fn. 1), § 35 Rn. 26 f.; *Ipsen* (Fn. 1), Rn. 653; *Jarass* (Fn. 6), Art. 12 Rn. 19; *Mann* (Fn. 167), Art. 12 Rn. 107; *Manssen* (Fn. 167), Art. 12 Rn. 103; *Michael/Morlok* (Fn. 8), Rn. 352; *Pieroth/Schlink* (Fn. 9), Rn. 878; *Sodan* (Fn. 10), Art. 12 Rn. 25.

173 BVerfGE 115, 205 (229); *Dietlein* (Fn. 168), S. 1832; *Epping* (Fn. 9), Rn. 363; *Hufen* (Fn. 1), § 35 Rn. 12; *Jarass* (Fn. 6), Art. 12 Rn. 10a; *Mann* (Fn. 167), Art. 12 Rn. 37; *Manssen* (Fn. 167), Art. 12 Rn. 266; *Sodan* (Fn. 10), Art. 12 Rn. 19.

174 *Jarass* (Fn. 6), Art. 12 Rn. 11; *Mann* (Fn. 167), Art. 12 Rn. 93; *Manssen* (Fn. 167), Art. 12 Rn. 73.

beruflichen Tätigkeit[175]. Über den klassischen Eingriff hinaus können auch Regelungen, die sich nicht auf die berufliche Tätigkeit selbst beziehen, zum Eingriff in die Berufsfreiheit führen, wenn sie „Rahmenbedingungen der Berufsausübung verändern, infolge ihrer Gestaltung in einem engen Zusammenhang mit der Ausübung eines Berufs stehen und objektiv eine berufsregelnde Tendenz haben" (Eingriff durch Regelung mit objektiv berufsregelnder Tendenz)[176].

Eingriffe in die Berufsfreiheit müssen verhältnismäßig sein. Diese Verhältnismäßigkeitsprüfung wird durch die „Drei-Stufen-Theorie", die das Bundesverfassungsgericht in seinem Apotheken-Urteil[177] entwickelt hat, konkretisiert[178]. Nach der Drei-Stufen-Theorie wird zwischen Berufsausübungsbeschränkungen (1. Stufe), subjektiven Berufswahlbeschränkungen (2. Stufe) und objektiven Berufswahlbeschränkungen (3. Stufe) unterschieden. Die Berufsausübungsbeschränkungen können durch jede vernünftige Erwägung des Gemeinwohls legitimiert werden[179]. Insoweit ist jeder legitime Zweck ausreichend[180]. Die subjektiven Berufswahlbeschränkungen sind zulässig, wenn sie dem Schutz eines überragenden bzw. besonders wichtigen Gemeinschaftsgutes dienen[181]. Ob die objektiven Berufswahlbeschränkungen gerechtfertigt sind, hängt davon ab, ob sie zur Abwehr nachweisbarer bzw. höchstwahrscheinlicher Gefahren für ein überragend wichtiges Gemeinschaftsgut zwingend geboten sind[182].

Da sich der (einheitliche) Schutzbereich der Berufsfreiheit nach dem Wortlaut des Art. 12 Abs. 1 GG in die Berufswahl und die Berufsausübung aufteilen lässt und diese Aufgliederung zugleich ein Indiz für die Intensität des Eingriffs in den Schutzbereich der Berufsfreiheit darstellt[183], kann man in der Regel bereits bei der Prüfung der Frage, ob ein Eingriff in die Berufs-

175 Vgl. *Jarass* (Fn. 6), Art. 12 Rn. 11; *Pieroth/Schlink* (Fn. 9), Rn. 894.

176 BVerfGE 110, 274 (288); 111, 191 (213); *Epping* (Fn. 9), Rn. 386 f.; *Jarass* (Fn. 6), Art. 12 Rn. 12; *Mann* (Fn. 167), Art. 12 Rn. 95; *Sodan* (Fn. 10), Art. 12 Rn. 20; *Zippelius/Würtenberger* (Fn. 16), § 30 Rn. 16; a. A. *Cremer*, DÖV 2003, S. 921 (928); *Manssen* (Fn. 167), Art. 12 Rn. 74.

177 BVerfGE 7, 377 ff.

178 BVerfGE 19, 330 (337): strikte Wahrung des Prinzips der Verhältnismäßigkeit; 46, 120 (138): Ergebnis einer strikten Anwendung des Verhältnismäßigkeitsgrundsatzes; *Jarass* (Fn. 6), Art. 12 Rn. 24; *Manssen* (Fn. 167), Art. 12 Rn. 139; *Zippelius/Würtenberger* (Fn. 16), § 30 Rn. 25.

179 BVerfGE 70, 1 (28); 85, 248 (259); 103, 1 (10); *Hofmann* (Fn. 11), Art. 12 Rn. 50; *Hufen* (Fn. 1), § 35 Rn. 30; *Jarass* (Fn. 6), Art. 12 Rn. 36; *Zippelius/Würtenberger* (Fn. 16), § 30 Rn. 27.

180 *Epping* (Fn. 9), Rn. 405.

181 BVerfGE 69, 209 (218); 103, 172 (183); *Epping* (Fn. 9), Rn. 406; *Hufen* (Fn. 1), § 35 Rn. 31; *Jarass* (Fn. 6), Art. 12 Rn. 37; *Zippelius/Würtenberger* (Fn. 16), § 30 Rn. 34.

182 BVerfGE 102, 197 (214); *Epping* (Fn. 9), Rn. 407; *Hufen* (Fn. 1), § 35 Rn. 32; *Jarass* (Fn. 6), Art. 12 Rn. 39; *Pieroth/Schlink* (Fn. 9), Rn. 925; *Zippelius/Würtenberger* (Fn. 16), § 30 Rn. 36.

183 Vgl. *Pieroth/Schlink* (Fn. 9), Rn. 920.

freiheit vorliegt, gleichzeitig festlegen, auf welcher Stufe (Berufsausübungsbeschränkung/subjektive Berufswahlbeschränkung/objektive Berufswahlbeschränkung) der Eingriff steht und wie intensiv der Eingriff ist[184]. Ausgehend davon lässt sich die Drei-Stufen-Theorie – aus Sicht des Prüfungsschemas – schon bei der Prüfung der Legitimität des verfolgten Zwecks (= 1. Schritt der Verhältnismäßigkeitsprüfung) anwenden[185]. Denn ob der Zweck, den das in die Berufsfreiheit eingreifende Gesetz verfolgt, legitim ist, hängt davon ab, ob sein Gewicht nach der Drei-Stufen-Theorie der jeweiligen Eingriffsstufe entspricht. Falls das Gewicht des verfolgten Zwecks die abgestufte Anforderung der Drei-Stufen-Theorie nicht erfüllt und damit die Legitimität des verfolgten Zwecks zu verneinen ist, ist die weitergehende Verhältnismäßigkeitsprüfung (Prüfung der Geeignetheit, Erforderlichkeit und Angemessenheit) überflüssig, weil das geprüfte Gesetz bereits wegen seines illegitimen Zwecks verfassungswidrig ist und nicht mehr gerechtfertigt werden kann. Zu beachten ist, dass sich die Prüfung der Angemessenheit, die sich auf die Güterabwägung bezieht, nicht (völlig) durch die Drei-Stufen-Theorie, die die Je-desto-Formel umschreibt[186], ersetzen lässt. Denn es kann sein, dass eine auf niedriger Eingriffsstufe stehende staatliche Maßnahme, die in die Berufsfreiheit eingreift, zu einer besonders starken Eingriffsintensität führt[187]. In dieser Konstellation ist die Eingriffsstufe ausnahmsweise nicht vereinbar mit der Eingriffsintensität. Die erhöhte Eingriffsintensität ist bei der Prüfung der Angemessenheit mit dem Schutzgrad des verfolgten Zwecks abzuwägen[188].

II. Eingriff in die Berufsausübungsfreiheit der Diensteanbieter durch polizei- und ordnungsgesetzliche Regelungen über Mitwirkungspflichten

Ohne technische Hilfe der E-Mail-Provider kann die präventiv-polizeiliche E-Mail-Überwachung schwierig sein. Zur Ermöglichung der Telekommunikationsüberwachung regeln alle polizei- und ordnungsgesetzliche Ermächtigungsvorschriften zur Telekommunikationsüberwachung die Mitwir-

184 Vgl. *Michael/Morlok* (Fn. 8), Rn. 674; *Pieroth/Schlink* (Fn. 9), Rn. 920 ff.; a. A. *Epping* (Fn. 9), Rn. 396.

185 Im Ergebnis so auch *Epping* (Fn. 9), Rn. 396; wohl anders aber *Jarass* (Fn. 6), Art. 12 Rn. 24: Die Stufenlehre spielt vor allem im Rahmen der Verhältnismäßigkeit i. e. S. eine Rolle.

186 Vgl. BVerfGE 7, 377 (404 f.).

187 Vgl. *Epping* (Fn. 9), Rn. 409; *Hufen* (Fn. 1), § 35 Rn. 33; *Jarass* (Fn. 6), Art. 12 Rn. 36; *Mann* (Fn. 167), Art. 12 Rn. 146 f.; *Pieroth/Schlink* (Fn. 9), Rn. 922 ff.

188 Vgl. BVerfGE 101, 331 (347); 103, 172 (183); 108, 150 (160): Eingriffszweck und Eingriffsintensität müssen in einem angemessenen Verhältnis stehen.

kungspflicht der Diensteanbieter[189]. Deutlich regeln diese polizei- und ordnungsgesetzlichen Vorschriften unmittelbar das Wie der Berufstätigkeit der Diensteanbieter. Dadurch liegt ein Eingriff in die Berufsfreiheit (Berufsausübungsfreiheit) der Diensteanbieter vor[190].

Zu beachten ist, dass der Eingriff in Grundrechte der Diensteanbieter, der sich aus den Vorschriften des TKG ergibt, von den Grundrechtseingriffen im Rahmen der präventiv-polizeilichen E-Mail-Überwachung zu trennen ist. Wie bereits im 1. Kapitel ausgeführt wurde, sind die Anbieter der Telekommunikationsdienste nach § 110 Abs. 1 Satz 1 TKG verpflichtet, auf eigene Kosten technische Einrichtungen zur Telekommunikationsüberwachung vorzuhalten. Diese Vorschrift des TKG regelt zwar die Vorkehrung für die Umsetzung einer E-Mail-Überwachung und kann somit zum Eingriff in die Berufsfreiheit oder das Eigentum der E-Mail-Provider führen[191], jedoch stellt sie selbst keine gesetzliche Grundlage für präventiv-polizeiliche Telekommunikationsüberwachung dar[192]. Insoweit sind die Prüfungsgegenstände der Verfassungsmäßigkeit des Grundrechtseingriffs, der sich aus der Durchführung einer präventiv-polizeilichen E-Mail-Überwachung herleitet, nur die einschlägigen polizei- und ordnungsgesetzlichen Vorschriften, nicht aber § 110 TKG.

C. Zusammenfassung des 4. Kapitels

Bei der präventiv-polizeilichen Telekommunikationsüberwachung ist das Fernmeldegeheimnis der Telekommunikationsteilnehmer betroffen. Dieser grundrechtliche Schutz gilt auch für die 2. Phase der E-Mail-Übermittlung. Die bereits im Mailserver ruhende und noch nicht vom Empfänger abgerufene E-Mail wird durch das Fernmeldegeheimnis geschützt. Durch den präventiv-polizeilichen Zugriff auf die E-Mail-Kommunikation wird zwar auch in das Recht auf informationelle Selbstbestimmung eingegriffen, allerdings ist das Fernmeldegeheimnis lex specialis gegenüber dem Recht auf informationelle Selbstbestimmung. In Bezug auf den Grundrechtseingriff, zu dem die präventiv-polizeiliche Überwachung führt, kommt das vom Bundesverfassungsgericht entwickelte Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme (Computergrundrecht) nicht in Betracht, weil es im Laufe des Vorgangs einer E-Mail-

189 Nachweise siehe oben Fn. 165. In Hessen kann die Polizei nach § 15a Abs. 1 hessSOG von einem Diensteanbieter verlangen, dass er die Kenntnisnahme des Inhalts der Telekommunikation ermöglicht und die näheren Umstände der Telekommunikation übermittelt.

190 Vgl. *Friedrich*, Verpflichtung privater Telekommunikationsunternehmen, S. 94; *Schenke* (Fn. 3), S. 1 (37); *Waechter*, VerwArch 87 (1996), S. 68 (71).

191 *Bock*, in: Geppert/Piepenbrock/Schütz/Schuster, TKG, § 110 Rn. 16 f.; *Klesczewski*, in: Säcker, TKG2009, § 110 Rn. 22; *von Hammerstein*, MMR 2004, S. 222 (223).

192 Dazu siehe 1. Kapitel A II.

Kommunikation keine Schutzlücke des Fernmeldegeheimnisses gibt. Zudem ist die Eigentumsgarantie (Art. 14 GG) auch nicht betroffen, wenn Geschäfts- und Betriebsgeheimnisse durch die präventiv-polizeiliche E-Mail-Überwachung erhoben werden. Denn die polizeiliche Informationserhebung ist keine Offenbarung der betriebsbezogenen Daten. Ferner bezieht sich der präventiv-polizeiliche Zugriff auf die E-Mail-Kommunikation auch nicht auf den Eingriff in die Kommunikationsfreiheit des Art. 5 Abs. 1 Satz 1 GG, weil diese verdeckte polizeiliche Maßnahme zur Informationserhebung keine Kommunikation verhindert.

Bei der Durchführung einer präventiv-polizeilichen E-Mail-Überwachung wird in die Berufsfreiheit der Diensteanbieter eingegriffen. Die Anbieter der Telekommunikationsdienste sind nach polizei- und ordnungsgesetzlichen Vorschriften zur Telekommunikationsüberwachung verpflichtet, die Durchführung einer Telekommunikationsüberwachung zu ermöglichen. Dabei geht es um eine Belastung für die Berufsausübung der E-Mail-Provider.

5. Kapitel: Verfassungsrechtliche Rechtfertigung präventiv-polizeilicher E-Mail-Überwachung

Im Folgenden ist die verfassungsrechtliche Rechtfertigung des präventiv-polizeilichen Zugriffs auf die E-Mail-Kommunikation näher zu behandeln. Da die präventiv-polizeiliche Telekommunikationsüberwachung, die der verdeckten Informationserhebung zur Gefahrenabwehr dient und damit zum Grundrechtseingriff führt, nicht vom Grundgesetz generell verboten ist[1], lässt sie sich rechtfertigen, soweit sie den verfassungsrechtlichen Anforderungen entspricht. Ausgehend davon ist zunächst zu prüfen, ob diese heimlichen polizeilichen Maßnahmen zur Informationsgewinnung formell verfassungsmäßig sind. Dabei geht es um die Frage, ob eine gesetzliche Ermächtigungsgrundlage, die der verfassungsrechtlichen Ordnung der Gesetzgebungskompetenzverteilung entspricht, die Durchführung einer präventiv-polizeilichen E-Mail-Überwachung stützt. Darüber hinaus ist die Prüfung der materiellen Verfassungsmäßigkeit erforderlich. Hierbei geht es darum, ob diese neue polizeiliche Befugnis den anderen verfassungsrechtlichen Rechtfertigungsvoraussetzungen genügt.

A. Formelle Verfassungsmäßigkeit präventiv-polizeilicher E-Mail-Überwachung

Wie im 4. Kapitel entwickelt, greift die Durchführung einer präventiv-polizeilichen E-Mail-Überwachung in das Fernmeldegeheimnis der betroffenen Telekommunikationsteilnehmer und in die Berufsausübungsfreiheit der E-Mail-Provider ein. Diese beiden Grundrechte sind Grundrechte mit (einfachem) Gesetzesvorbehalt (Art. 10 Abs. 2 Satz 1, Art. 12 Abs. 1 Satz 2 GG)[2]. Deswegen hängt die Frage, ob die Maßnahme der präventiv-polizeilichen E-Mail-Überwachung formell verfassungsmäßig ist, aus der Sicht des Gesetzesvorbehalts davon ab, ob diese polizeiliche Tätigkeit eine gesetzliche Ermächtigungsgrundlage finden kann, die in Einklang mit der verfassungsrechtlichen Ordnung der Kompetenzverteilung steht. Insoweit lässt sich die Prüfung der formellen Verfassungsmäßigkeit in zwei Schritte gliedern. Erstens ist (auf der Ebene der Gesetzgebung) zu prüfen, welches Gesetz-

1 *Götz*, PolR, § 17 Rn. 46; *Gusy*, Die Polizei 2004, S. 61 (64).

2 Zur Typologie der Gesetzesvorbehalte *Hufen*, Grundrechte, § 9 Rn. 9 ff.; *von Münch*, Bd. 2, Rn. 246; *Pieroth/Schlink*, Grundrechte, Rn. 263 ff.; *Zippelius/Würtenberger*, Staatsrecht, § 19 Rn. 44 ff.

gebungsorgan (Bundesgesetzgeber oder Landesgesetzgeber) die Gesetzgebungskompetenz für die präventiv-polizeiliche Telekommunikationsüberwachung hat. Durch diesen Prüfungsschritt kann man festlegen, ob die geltenden polizei- und ordnungsgesetzlichen Ermächtigungsvorschriften zur Telekommunikationsüberwachung, die als ausdrückliche Rechtsgrundlagen des präventiv-polizeilichen Zugriffs auf die E-Mail-Kommunikation betrachtet werden, formell verfassungsmäßig sind. Zweitens ist (auf der Ebene der Gesetzesanwendung) zu prüfen, ob in den Bundesländern, in denen eine explizite polizei- und ordnungsgesetzliche Ermächtigungsvorschrift zur Telekommunikationsüberwachung nicht besteht, diese Maßnahme auf andere Rechtsgrundlagen gestützt werden kann.

I. Verfassungsrechtliche Ordnung der Kompetenzverteilung zwischen Bund und Ländern als Prüfungsmaßstab

1. Gesetzgebungskompetenz der Länder für die Gefahrenabwehr

Wie im 3. Kapitel ausgeführt wurde, stellt die Gefahrenabwehr weder den Gegenstand ausschließlicher Bundesgesetzgebung (Art. 73 GG) noch den Gegenstand konkurrierender Gesetzgebung (Art. 74 GG) dar. Gemäß Art. 70 Abs. 1 GG hat der Landesgesetzgeber die Gesetzgebungsbefugnis für die Gefahrenabwehr[3]. Insoweit fällt die präventiv-polizeiliche Telekommunikationsüberwachung, die der Gefahrenabwehr dient, in den Bereich der Landesgesetzgebungskompetenz[4]. Die landesrechtlichen polizei- und ordnungsgesetzlichen Ermächtigungsvorschriften zur Telekommunikationsüberwachung, in denen der präventiv-polizeiliche Zugriff auf die E-Mail-Kommunikation eine ausdrückliche Rechtsgrundlage findet, sind kompetenzgemäß.

2. Gesetzgebungskompetenz des Bundes für die präventiv-polizeiliche Telekommunikationsüberwachung nach Art. 73 Abs. 1 Nr. 7 GG?

Zwar dient die präventiv-polizeiliche Telekommunikationsüberwachung dem Zweck der Gefahrenabwehr, jedoch ist zu berücksichtigen, dass sich die präventiv-polizeiliche Telekommunikationsüberwachung auf den Zugriff auf die Telekommunikation bezieht. Da die Telekommunikation gemäß Art. 73 Abs. 1 Nr. 7 GG ein Gegenstand der ausschließlichen Bundesgesetzgebungskompetenz ist, wird die Frage aufgeworfen: Kann der Bund aus Art. 73 Abs. 1 Nr. 7 GG (Gesetzgebungsbefugnis für die Telekom-

3 Dazu siehe 3. Kapitel A I 2 a).

4 BVerfGE 113, 348 (368); *Gusy* (Fn. 1), S. 61 (62 f.); *Löwer*, in: von Münch/Kunig, GG, Bd. 1, Art. 10 Rn. 29; *Pieroth*, in: Jarass/Pieroth, GG, Art. 73 Rn. 27; *R. P. Schenke*, AöR 125 (2000), S. 1 (14); *Tischer*, System der informationellen Befugnisse, S. 473 f.; a. A. *Kutscha*, LKV 2003, S. 114 (116); *Randl*, NVwZ 1992, S. 1070 (1072).

munikation) seine Gesetzgebungskompetenz für die Telekommunikationsüberwachung herleiten und damit im Sachbereich der Telekommunikationsüberwachung die Landesgesetzgebungskompetenz verdrängen?

a) Keine ausdrücklich normierte Bundeskompetenz für präventiv-polizeiliche Telekommunikationsüberwachung nach Art. 73 Abs. 1 Nr. 7 GG

Das Bundesverfassungsgericht und die Literatur beschränken die Kompetenz des Bundes, die sich aus Art. 73 Abs. 1 Nr. 7 GG ergibt, auf die technische Seite der Telekommunikationsinfrastruktur und der Informationsübermittlung. Deswegen fallen inhaltliche Fragen der Telekommunikation (die übermittelten Inhalte oder die Art der Nutzung der Telekommunikation) nicht in den Anwendungsbereich des Art. 73 Abs. 1 Nr. 7 GG[5]. Da durch die Telekommunikationsüberwachung sowohl die Inhaltsdaten als auch die Verkehrsdaten erhoben werden, bezieht sich diese Maßnahme nicht nur auf den Zugriff auf die Inhalte der Telekommunikation, sondern auch auf die technischen Umstände der Telekommunikation[6]. Davon ausgehend erscheint es naheliegend, dass eine Bundesgesetzgebungskompetenz für die Telekommunikationsüberwachung aus Art. 73 Abs. 1 Nr. 7 GG hergeleitet werden kann. Allerdings ist eine solche Bundesgesetzgebungskompetenz für die Telekommunikationsüberwachung (im Rahmen der Erhebung der Telekommunikationsverkehrsdaten), die sich aus Art. 73 Abs. 1 Nr. 7 GG ergibt, zu verneinen. Der Grund ist einfach: Falls der Bundesgesetzgeber aufgrund seiner aus Art. 73 Abs. 1 Nr. 7 GG hergeleiteten Gesetzgebungskompetenz eine gesetzliche Vorschrift, die die Telekommunikationsüber-

5 BVerfGE 113, 348 (368); 114, 371 (385); *Degenhart*, in: Sachs, GG, Art. 73 Rn. 34; *Gusy* (Fn. 1), S. 61 (62); *Heintzen*, in: von Mangoldt/Klein/Starck, GG, Bd. 2, Art. 73 Rn. 69; *Kunig*, in: von Münch/Kunig, GG, Bd. 3, Art. 73 Rn. 31; *Masing*, in: Isensee/Kirchhof, HStR, Bd. 4, § 90 Rn. 23; *Pieroth* (Fn. 4), Art. 73 Rn. 26; *Rengeling*, in: Isensee/Kirchhof, HStR, Bd. 6, 3. Aufl., § 135 Rn. 119; *Sannwald*, in: Schmidt-Bleibtreu/Hofmann/Hopfauf, GG, Art. 73 Rn. 82; *Schnapauff*, in: Hömig, GG, Art. 73 Rn. 11; *Haratsch*, in: Sodan, GG, Art. 73 Rn. 16; *Schenke* (Fn. 4), S. 1 (8); *Stettner*, in: Dreier, GG, Bd. 2 Supplementum, Art. 73 Rn. 40; *Tischer* (Fn. 4), S. 473 f.; *Wuttke*, Polizeirecht und Zitiergebot, S. 248.

6 Im Schrifttum wird vertreten, dass es bei der Telekommunikationsüberwachung nicht um die technische Seite des Übermittelungsvorgangs gehe (*Degenhart* (Fn. 5), Art. 73 Rn. 34; *Schenke* (Fn. 4), S. 1 (8)). Diese Meinung greift zu kurz. Jedenfalls ist nicht zu leugnen, dass sich die Verkehrsdaten (Umstände des Telekommunikationsvorgangs) auf die technische Seite des Übermittelungsvorgangs beziehen (a. A. *Degenhart* (Fn. 5), Art. 73 Rn. 34). Zwar beschränkt sich die präventiv-polizeiliche Telekommunikationsüberwachung in Baden-Württemberg auf die Erhebung der Verkehrsdaten (§ 23a Abs. 1 S. 1 bwPolG), diese polizeiliche Gewinnung der Telekommunikationsverkehrsdaten dient jedoch der Gefahrenabwehr. Zweifellos ist, dass der baden-württembergische Gesetzgeber eine Kompetenz für die Telekommunikationsüberwachung zur Gefahrenabwehr hat. Zu prüfen ist nur, ob der Bundesgesetzgeber eine Gesetzgebungskompetenz, die im Sachbereich der Telekommunikationsüberwachung die Landesgesetzgebungskompetenz verdrängen kann, besitzt.

wachung erlaubt, erlässt, ist unklar, welchen Zweck eine solche gesetzliche Vorschrift verfolgt. Die Telekommunikation als solche kann nicht den Zweck einer Telekommunikationsüberwachung darstellen. Eine Telekommunikationsüberwachung, die der Erfüllung der in Art. 73 Abs. 1 Nr. 7 GG vorgeschriebenen Bundesaufgabe dient, ist nicht denkbar. Deswegen ist auch die Telekommunikationserhebung, bei der es nicht um die Erhebung der Inhaltsdaten, sondern nur um die Erhebung der Verkehrsdaten geht, kein Gegenstand der in Art. 73 Abs. 1 Nr. 7 GG geregelten Gesetzgebungskompetenz. Aus Art. 73 Abs. 1 Nr. 7 GG ergibt sich keine Bundesgesetzgebungskompetenz für die Telekommunikationsüberwachung[7]. Diese Konsequenz gilt nicht nur für die präventive Telekommunikationsüberwachung, sondern auch für die repressive Telekommunikationsüberwachung.

b) Keine ungeschriebene Bundeskompetenz kraft Sachzusammenhangs und Annexes für präventiv-polizeiliche Telekommunikationsüberwachung

Über die im Grundgesetz ausdrücklich zugewiesenen Bundeskompetenzen hinaus erkennen das Bundesverfassungsgericht und die Literatur auch ungeschriebene Bundeskompetenzen an[8]. Die ungeschriebenen Bundeskompetenzen knüpfen an eine im Grundgesetz normierte Bundeskompetenz an[9]. Dazu gehören die Bundeskompetenz kraft Sachzusammenhangs und die Annexkompetenz des Bundes[10]. Zwar ergibt sich keine normierte Bundeskompetenz für die präventiv-polizeiliche Telekommunikationsüberwachung aus Art. 73 Abs. 1 Nr. 7 GG, jedoch ist zu erörtern, ob es eine unmittelbar an Art. 73 Abs. 1 Nr. 7 GG anknüpfende ungeschriebene Bundeskompetenz für die präventiv-polizeiliche Telekommunikationsüberwachung gibt.

aa) Keine ungeschriebene Bundeskompetenz kraft Sachzusammenhangs

Eine ungeschriebene Bundeskompetenz kraft Sachzusammenhangs wird bejaht, „wenn eine dem Bund zugewiesene Materie verständigerweise nicht

7 BVerfGE 113, 348 (368); *Degenhart* (Fn. 5), Art. 73 Rn. 34; *Gusy* (Fn. 1), S. 61 (62); *Pieroth* (Fn. 4), Art. 73 Rn. 27; *Schenke* (Fn. 4), S. 1 (8); *Haratsch* (Fn. 5), Art. 73 Rn. 16.

8 Kritisch dazu *J. Ipsen*, Staatsorganisationsrecht, Rn. 600; *Maurer*, Staatsrecht, § 10 Rn. 31; *Stettner*, Kompetenzlehre, S. 424.

9 Nach Rechtsprechung und Literatur sind auch die ungeschriebenen Bundeskompetenzen kraft Natur der Sache, die keine Anknüpfung an eine geschriebene Bundeskompetenz haben, anerkannt. Die Problematik der Bundeskompetenz kraft Natur der Sache wird weiter unten entwickelt (siehe A I 4 dieses Kapitels).

10 Vgl. BVerfGE 26, 246 (257); 98, 265 (299); *Degenhart* (Fn. 5), Art. 70 Rn. 30; *Ehlers*, JURA 2000, S. 323 (324 f.); *Kunig* (Fn. 5), Art. 70 Rn. 23; *Rozek*, in: von Mangoldt/Klein/Starck, GG, Bd. 2, Art. 70 Rn. 39; *Sannwald* (Fn. 5), Vorb. v. Art. 70 Rn. 20.

geregelt werden kann, ohne dass zugleich eine andere Materie mit geregelt wird, wenn also das Übergreifen in einen an sich den Ländern übertragenen Kompetenzbereich für die Regelung der zugewiesenen Materie unerlässlich ist“[11]. Insoweit besteht das Verhältnis zwischen der ungeschriebenen Bundeskompetenz kraft Sachzusammenhangs und der geschriebenen Bundeskompetenz darin, dass die ungeschriebene Bundeskompetenz kraft Sachzusammenhangs eine unerlässliche Voraussetzung für die im Grundgesetz ausdrücklich normierte Bundeskompetenz darstellt[12].

Eine ungeschriebene Bundesgesetzgebungskompetenz kraft Sachzusammenhang für die präventiv-polizeiliche Telekommunikationsüberwachung lässt sich nur anerkennen, wenn die präventiv-polizeiliche Telekommunikationsüberwachung eine unentbehrliche Voraussetzung für die Regelung der technischen Seite von Telekommunikationen ist. Das logische Verhältnis zwischen präventiv-polizeilicher Telekommunikationsüberwachung und der Fernmeldetechnik folgt allerdings einem umgekehrten Zusammenhang: Die Durchführung einer präventiv-polizeilichen Telekommunikation setzt die Funktionsfähigkeit der Fernmeldetechnik voraus[13]. Dies entspricht nicht der Annahme der ungeschriebenen Bundeskompetenz kraft Sachzusammenhangs. Deswegen kann keine an Art. 73 Abs. 1 Nr. 7 GG anknüpfende ungeschriebene Bundeskompetenz kraft Sachzusammenhangs für die präventiv-polizeiliche Telekommunikationsüberwachung anerkannt werden[14].

bb) Keine ungeschriebene Bundeskompetenz kraft Annexes

Eine ungeschriebene Bundeskompetenz kraft Annexes liegt vor, wenn sie für die Vorbereitung und Durchführung einer geschriebenen Bundeskompetenz erforderlich ist[15] und damit in einem unlösbaren Zusammenhang zur geschriebenen Bundeskompetenz steht[16]. Im Schrifttum wird teilweise vertreten, dass die Annexkompetenz von der Bundeskompetenz kraft Sachzusammenhangs zu unterscheiden sei, obwohl beide ungeschriebene Bun-

11 BVerfGE 110, 33 (48); vgl. auch *Degenhart* (Fn. 5), Art. 70 Rn. 42; *Ehlers* (Fn. 10), S. 323 (324); *Haratsch* (Fn. 5), Art. 70 Rn. 17; *Kunig* (Fn. 5), Art. 70 Rn. 24; *Pieroth* (Fn. 4), Art. 70 Rn. 9; *Rozek* (Fn. 10), Art. 70 Rn. 45; *Zippelius/Würtenberger* (Fn. 2), § 45 Rn. 41.

12 Vgl. BVerfGE 3, 407 (421); 98, 265 (299); *Kunig* (Fn. 5), Art. 70 Rn. 24; *Maurer* (Fn. 8), § 10 Rn. 28; *von Münch/Mager*, Staatsrecht, Bd. 1, Rn. 392; *Rozek* (Fn. 10), Art. 70 Rn. 45; *Sannwald* (Fn. 5), Vorb. v. Art. 70 Rn. 27; *Stern*, Staatsrecht, Bd. II, S. 611; *Zippelius/Würtenberger* (Fn. 2), § 45 Rn. 41.

13 *Gusy* (Fn. 1), S. 61 (62); *Schenke* (Fn. 4), S. 1 (10).

14 *Gusy* (Fn. 1), S. 61 (62); *Schenke* (Fn. 4), S. 1 (10).

15 *Degenhart* (Fn. 5), Art. 70 Rn. 37 f.; *Haratsch* (Fn. 5), Art. 70 Rn. 18; *Kunig* (Fn. 5), Art. 70 Rn. 25; *Rozek* (Fn. 10), Art. 70 Rn. 48; *Sannwald* (Fn. 5), Vorb. v. Art. 70 Rn. 29; *Stettner* (Fn. 5), Art. 70 Rn. 74.

16 *Kunig* (Fn. 5), Art. 70 Rn. 25; *Rozek* (Fn. 10), Art. 70 Rn. 48; *Zippelius/Würtenberger* (Fn. 2), § 45 Rn. 43.

deskompetenzen die Anknüpfung an eine im Grundgesetz ausdrücklich festgeschriebene Bundeskompetenz betreffen würden[17]. Im Gegensatz zur Bundeskompetenz kraft Sachzusammenhangs, die eine Ausdehnung der Kompetenz in die „Breite" darstelle, sei die Annexkompetenz als eine „Tiefe" der Gesetzgebungszuständigkeit zu betrachten[18]. Richtiger dürfte jedoch sein, dass die Annexkompetenz ein Unterfall der Kompetenz kraft Sachzusammenhangs ist oder die beiden Begriffe identisch sind[19]. Denn sowohl die Bundeskompetenz kraft Annexes als auch die Bundeskompetenz kraft Sachzusammenhangs bedürfen der Anknüpfung an die geschriebene Bundeskompetenz. Zudem kann sich die ungeschriebene Bundeskompetenz kraft Annexes auf das Übergreifen in einen Kompetenzbereich der Länder (z. B. Gefahrenabwehr[20]) beziehen, wenn es um den Annex der Zuständigkeitsmaterie des Bundes geht. Ausgehend davon können sich beide ungeschriebenen Bundeskompetenzen auf sowohl eine „Tiefe" wie auch eine „Breite" der Gesetzgebungszuständigkeit des Bundes erstrecken. Aus diesem Grund ist schwer einzusehen, warum sie nach dem Charakter der betroffenen Materie (d. h. ob die betroffene Materie für den Bund ein eigener oder fremder Zuständigkeitsbereich ist) voneinander unterschieden werden können[21].

Obwohl sich die Gefahrenabwehr als eine ungeschriebene Bundeskompetenz kraft Annexes ansehen lässt[22], ist zu beachten, dass hierdurch kein

17 So *Degenhart* (Fn. 5), Art. 70 Rn. 43; *Ehlers* (Fn. 10), S. 323 (325); *Maurer* (Fn. 8), § 10 Rn. 29; *Stettner* (Fn. 5), Art. 70 Rn. 73.

18 So *Degenhart* (Fn. 5), Art. 70 Rn. 43; *Ehlers* (Fn. 10), S. 323 (325); *Haratsch* (Fn. 5), Art. 70 Rn. 17 f.; *Maurer* (Fn. 8), § 10 Rn. 29; *Sannwald* (Fn. 5), Vorb. v. Art. 70 Rn. 29; *Stettner* (Fn. 5), Art. 70 Rn. 73.

19 So zutreffend *Jarass*, NVwZ 2000, S. 1089 (1090); *von Münch/Mager* (Fn. 12), Rn. 395; *Pieroth* (Fn. 4), Art. 70 Rn. 12; *Rengeling* (Fn. 5), § 135 Rn. 74; *Starck*, in: Geis/Lorenz, FS Maurer, S. 281 (285); *Stern* (Fn. 12), S. 611; *Zippelius/Würtenberger* (Fn. 2), § 45 Rn. 43. Jedenfalls handelt es sich bei beiden ungeschriebenen Bundeskompetenzen um einander ähnelnde Konstellationen (vgl. *Kunig* (Fn. 5), Art. 70 Rn. 26). *Rozek* bejaht zwar die Auffassung, dass die Annexkompetenz ein Unterfall der Kompetenz kraft Sachzusammenhangs sei, jedoch stimmt er zugleich der Meinung zu, dass die Annexkompetenz – anders als die Kompetenz kraft Sachzusammenhangs – nicht in die „Breite", sondern in die „Tiefe" gehe (vgl. *Rozek* (Fn. 10), Art. 70 Rn. 44).

20 BVerfGE 3, 407 (433); 8, 143 (150); *Degenhart* (Fn. 5), Art. 70 Rn. 39; *Götz* (Fn. 1), § 1 Rn. 13; *Haratsch* (Fn. 5), Art. 70 Rn. 18; *Ipsen* (Fn. 8), Rn. 595; *Kunig* (Fn. 5), Art. 70 Rn. 25; *Maurer* (Fn. 8), § 10 Rn. 29; *Pieroth* (Fn. 4), Art. 70 Rn. 12; *Rozek* (Fn. 10), Art. 70 Rn. 48; *Stettner* (Fn. 5), Art. 70 Rn. 77; *Zippelius/Würtenberger* (Fn. 2), § 45 Rn. 43.

21 Auch die Literatur, die dem terminologischen Unterschied zwischen der Annexkompetenz und der Kompetenz kraft Sachzusammenhangs zustimmt, erkennt an, dass die Abgrenzung der beiden ungeschriebenen Bundeskompetenz letztlich unscharf ist (vgl. *Degenhart* (Fn. 5), Art. 70 Rn. 43; *Stettner* (Fn. 8), S. 432).

22 Siehe oben Fn. 20.

uferloses Übergreifen in den Kompetenzbereich der Länder erfolgen darf[23]. Durch die Annexkompetenz kann der Bund kein allgemeines Gefahrenabwehrrecht, sondern nur spezielles Ordnungs- und Polizeirecht in dem entsprechenden Sachgebiet regeln[24]. Insoweit erließ der Bund nach seiner Annexkompetenz, die für die Vorbereitung und Durchführung der geschriebenen Bundeskompetenz erforderlich ist, eine Reihe von polizeirechtlichen Vorschriften wie etwa das Passgesetz (Art. 74 Abs. 1 Nr. 3 GG), das Jugendschutzgesetz (Art. 74 Abs. 1 Nr. 7 GG), das Straßenverkehrsgesetz (Art. 74 Abs. 1 Nr. 22 GG) etc[25].

Die Konsequenz, dass der Bund durch seine Annexkompetenz spezielles Ordnungs- und Polizeirecht im entsprechenden Sachgebiet regeln kann, begründet keine an Art. 73 Abs. 1 Nr. 7 GG knüpfende Gesetzgebungskompetenz des Bundes für präventiv-polizeiliche Telekommunikationsüberwachung. Wird eine Annexkompetenz des Bundes für die Gefahrenabwehr im Sachgebiete der Art. 73 Abs. 1 Nr. 7 GG anerkannt, so bleibt die Reichweite des Art. 73 Abs. 1 Nr. 7 GG zu beachten. Von diesem Standpunkt aus erschöpft sich die an Art. 73 Abs. 1 Nr. 7 GG knüpfende Annexkompetenz des Bundes für das Polizeirecht in der Abwehr der von der technischen Seite der Telekommunikation herrührenden Gefahren (z. B. Elektrosmog)[26]. Demgegenüber handelt es sich bei der präventiv-polizeilichen Telekommunikationsüberwachung jedoch um die Gefahren, die durch Inhalte der Telekommunikation verursacht werden. Demzufolge hat der Bund keine an Art. 73 Abs. 1 Nr. 7 GG knüpfende Annexkompetenz für die präventiv-polizeiliche Telekommunikationsüberwachung[27].

3. Gesetzgebungskompetenz des Bundes nach Art. 73 Abs. 1 Nr. 9a GG?

a) Neue Bundeskompetenz für die Bekämpfung des internationalen Terrorismus

Bemerkenswert ist, dass der Bund gemäß Art. 73 Abs. 1 Nr. 9a GG, der im Rahmen der Föderalismusreform 2006[28] geschaffen wurde, die ausschließliche Kompetenz für die Abwehr von Gefahren des internationalen Terrorismus[29] durch das Bundeskriminalpolizeiamt besitzt. Die neue Kompetenz

23 Vgl. *Degenhart* (Fn. 5), Art. 70 Rn. 38; *Rozek* (Fn. 10), Art. 70 Rn. 48.

24 Vgl. BVerfGE 3, 407 (433); 8, 143 (150); *Götz* (Fn. 1), § 1 Rn. 13; *Kunig* (Fn. 5), Art. 70 Rn. 25; *Maurer* (Fn. 8), § 10 Rn. 29; *Pieroth* (Fn. 4), Art. 70 Rn. 12; *Rozek* (Fn. 10), Art. 70 Rn. 48; *Stettner* (Fn. 5), Art. 70 Rn. 77; *Zippelius/Würtenberger* (Fn. 2), § 45 Rn. 43.

25 *W.-R. Schenke*, PolR, Rn. 25 ff.

26 *Heintzen* (Fn. 5), Art. 73 Rn. 75 f.; *Schenke* (Fn. 4), S. 1 (9).

27 *Gusy* (Fn. 1), S. 61 (62); *Schenke* (Fn. 4), S. 1 (9).

28 Zur Föderalismusreform 2006 *Degenhart*, NVwZ 2006, S. 1209 ff.; *J. Ipsen*, NJW 2006, S. 2801 ff.; *Papier*, NJW 2007, S. 2145 ff.

29 Der Begriff des internationalen Terrorismus ist durch das internationalen und nationalen Normen zugrunde liegende Verständnis vorgeprägt, aber zugleich für künftige Entwicklung offen

des Bundes nach Art. 73 Abs. 1 Nr. 9a GG, also die Abwehr von Gefahren des internationalen Terrorismus, erstreckt sich nicht auf die repressive, sondern auf die präventive Aufgabe der Polizei[30]. Dies lässt sich auch daraus herleiten, dass die Kompetenz zur Abwehr von Gefahren des internationalen Terrorismus nicht in den Bereich der internationalen Verbrechensbekämpfung (Art. 73 Abs. 1 Nr. 10 GG) fällt[31]. Insoweit stellt Art. 73 Abs. 1 Nr. 9a GG ausnahmsweise eine ausdrücklich normierte Gesetzgebungskompetenz des Bundes für die Gefahrenabwehr dar[32]. Zu beachten ist allerdings, dass die Bundesgesetzgebungskompetenz zur Abwehr von Gefahren des internationalen Terrorismus subsidiär gegenüber der Landesgesetzgebungszuständigkeit für die Gefahrenabwehr ist[33]. Denn gemäß Art. 73 Abs. 1 Nr. 9a GG besitzt der Bund die Kompetenz zur Abwehr von Gefahren des internationalen Terrorismus nur in Fällen, in denen eine länderübergreifende Gefahr vorliegt, die Zuständigkeit einer Landespolizeibehörde nicht erkennbar ist oder die oberste Landesbehörde um eine Übernahme ersucht. Aufgrund dieser Restriktionen lässt die neue Bundesgesetzgebungskompetenz nach Art. 73 Abs. 1 Nr. 9a GG die Gesetzgebungskompetenzen der Länder zur Gefahrenabwehr im Grundsatz unberührt. Dadurch bleibt die Landeskompetenz für die Gefahrenabwehr bestehen[34], was im Folgenden weiter zu begründen ist.

b) Keine ausschließliche Bundeskompetenz für präventiv-polizeiliche Telekommunikationsüberwachung nach Art. 73 Abs. 1 Nr. 9a GG

Die territorialen Grenzen spielen keine Rolle für den E-Mail-Verkehr oder andere moderne Telekommunikationsformen. Wird eine gefährliche Information durch eine E-Mail übertragen, kann eine solche Gefahr länderübergreifend sein. In diesem Zusammenhang stellt sich die Frage, ob das Bundesgesetz nach Art. 73 Abs. 1 Nr. 9a GG die präventiv-polizeiliche Telekommunikationsüberwachung regeln kann. Die Antwort auf diese Frage hängt davon ab, ob die Befugnis für die präventiv-polizeiliche Telekommunikationsüberwachung nur der Bekämpfung des internationalen Terrorismus dient.

Zunächst ist festzuhalten, dass sich eine Bundeskompetenz für die präventive Telekommunikationsüberwachung, die den Zweck der Bekämpfung

(BT-Drs. 16/813, S. 12). Vgl. *Degenhart* (Fn. 5), Art. 73 Rn. 47; *Kluth*, in: Kluth, Föderalismusreformgesetz, Art. 73 Rn. 8; *Schnapauff* (Fn. 5), Art. 73 Rn. 14; *Stettner* (Fn. 5), Art. 73 Rn. 53.

30 Vgl. BT-Drs. 16/813, S. 12; *Degenhart* (Fn. 5), Art. 73 Rn. 48; *Heintzen*, in: Starck, Föderalismusreform, Rn. 98; *Pieroth* (Fn. 4), Art. 73 Rn. 30; *Rengeling* (Fn. 5), § 135 Rn. 126; *Schnapauff* (Fn. 5), Art. 73 Rn. 14; *Stettner* (Fn. 5), Art. 73 Rn. 51.

31 Vgl. *Heintzen* (Fn. 30), Rn. 92; *Stettner* (Fn. 5), Art. 73 Rn. 52.

32 *Stettner* (Fn. 5), Art. 73 Rn. 51.

33 *Heintzen* (Fn. 30), Rn. 98.

34 BT-Drs. 16/813, S. 12; *Heintzen* (Fn. 30), Rn. 101; *Rengeling* (Fn. 5), § 135 Rn. 127; *Schnapauff* (Fn. 5), Art. 73 Rn. 14; *Stettner* (Fn. 5), Art. 73 Rn. 51.

des nationalen Terrorismus verfolgt, nicht aus Art. 73 Abs. 1 Nr. 9a GG ergeben kann, da der nationale Terrorismus nicht von Art. 73 Abs. 1 Nr. 9a GG erfasst wird[35]. Zwar sind der nationale und internationale Terrorismus in der Tat schwer zu trennen[36], jedoch darf man die Eingrenzungswirkung, die das Kriterium der Internationalität in Art. 73 Abs. 1 Nr. 9a GG besitzt, nicht übergehen: Ein Bundesgesetz, das nach der Begründung der Gesetzgebung ausdrücklich (nur) zur Bekämpfung des nationalen Terrorismus erlassen wird, kann seine verfassungsrechtliche Grundlage nicht in Art. 73 Abs. 1 Nr. 9a GG finden.

Wegen der Kompetenz für die Gefahrenabwehr nach Art. 73 Abs. 1 Nr. 9a GG kann der Bundesgesetzgeber die präventive Telekommunikationsüberwachung zur Bekämpfung des internationalen Terrorismus regeln. Zu beachten ist jedoch, dass die Bundeskompetenz für die Gefahrenabwehr (Bekämpfung des internationalen Terrorismus) nach Art. 73 Abs. 1 Nr. 9a GG nur das Bundeskriminalpolizeiamt (Bundeskriminalamt, BKA) erfasst[37]. Dies führt dazu, dass der Bundesgesetzgeber nur dem BKA die Befugnis zur präventiven Telekommunikationsüberwachung einräumen darf. Nach § 20 l BKAG (Gesetz über das Bundeskriminalamt und die Zusammenarbeit des Bundes und der Länder in kriminalpolizeilichen Angelegenheiten[38]), der durch Art. 1 Terrorismusabwehr-G vom 25. 12. 2008[39] eingefügt wurde, besitzt das BKA eine Befugnis für die präventive Telekommunikationsüberwachung.

Obwohl der Bundesgesetzgeber durch § 20 l BKAG die Befugnis für präventive Telekommunikationsüberwachung regelt, ist zu betonen, dass diese neue Regelung des BKAG nicht die polizei- und ordnungsgesetzlichen Vorschriften der Länder zur präventiv-polizeilichen Telekommunikationsüberwachung verdrängt. Da § 20 l BKAG seine verfassungsrechtliche Grundlage in Art. 73 Abs. 1 Nr. 9a GG findet, kann die Befugnis des BKA für präventive Telekommunikationsüberwachung nur im Rahmen der Bekämpfung des internationalen Terrorismus geregelt und ausgeübt werden[40]. Der Bund darf nicht die Grenze zur allgemeinen Gefahrenabwehr überschreiten. Angesichts dieser Grenze gibt es auch keine an Art. 73 Abs. 1 Nr. 9a GG anknüpfende Bundeskompetenz kraft Sachzusammenhangs oder Annexes für die zur allgemeinen Gefahrenabwehr dienende Telekommunikationsüberwachung. Folglich verdrängt Art. 73 Abs. 1 Nr. 9a GG nicht die geltenden polizei- und ordnungsgesetzlichen Vorschriften der Länder zur Tele-

35 Vgl. BT-Drs. 16/813, S. 12; *Degenhart* (Fn. 5), Art. 73 Rn. 47; *Haratsch* (Fn. 5), Art. 73 Rn. 19; *Heintzen* (Fn. 30), Rn. 92; *Pieroth* (Fn. 4), Art. 73 Rn. 30; *Stettner* (Fn. 5), Art. 73 Rn. 53.

36 *Heintzen* (Fn. 30), Rn. 97; *Stettner* (Fn. 5), Art. 73 Rn. 53.

37 *Heintzen* (Fn. 30), Rn. 99, 101; *Sannwald* (Fn. 5), Art. 73 Rn. 122d.

38 BGBl. 1997 I, S. 1650.

39 BGBl. 2008 I, S. 3083.

40 Vgl. § 4a Abs. 1 S. 1 i.V.m § 20a Abs. 1 BKAG.

kommunikationsüberwachung, die nicht (nur) auf die Bekämpfung des internationalen Terrorismus, sondern auf allgemeine Gefahrenabwehr abzielen, nicht außer Kraft.

4. Gesetzgebungskompetenz des Bundes kraft Natur der Sache?

a) Bundeskompetenz kraft Natur der Sache als begriffsnotwendig ungeschriebene Bundeskompetenz

Da sich die ausschließliche Gesetzgebungskompetenz des Bundes für die präventiv-polizeiliche Telekommunikationsüberwachung weder aus der geschriebenen Bundeskompetenz noch aus der an eine im Grundgesetz normierte Bundeskompetenz anknüpfenden ungeschriebenen Bundeskompetenz ergibt, ist zum Schluss noch zu überprüfen, ob eine Gesetzgebungskompetenz des Bundes kraft Natur der Sache für die präventiv-polizeiliche Telekommunikationsüberwachung besteht. Im Gegensatz zur ungeschriebenen Bundeskompetenz kraft Sachzusammenhangs oder Annexes hat die ungeschriebene Bundeskompetenz kraft Natur der Sache keine Anknüpfung an die geschriebene Bundeskompetenz[41]. Eine Bundeskompetenz kraft Natur der Sache kann nach der Auffassung des Bundesverfassungsgerichts und der Literatur angenommen werden, wenn „gewisse Sachgebiete, weil sie ihrer Natur nach eine eigenste, der partikularen Gesetzgebungszuständigkeit a priori entrückte Angelegenheit des Bundes darstellen, vom Bund und nur von ihm geregelt werden können“[42]. Insoweit müsse die Anerkennung einer Bundeskompetenz kraft Natur der Sache begriffsnotwendig sein[43]. Diese Begriffsnotwendigkeit sei nicht an einer einzelnen bestimmten Kompetenzvorschrift des Grundgesetzes angebunden. Vielmehr leite sie sich aus einer systematischen Auslegung, die die gesamte Verfassung umfasse, her[44]. Dadurch würden die im Verfassungstext belassenen Lücken geschlossen[45]. Eine solche begriffsnotwendig ungeschriebene Bundeskompetenz werde als eine ausschließliche Kompetenz des Bundes angesehen[46].

41 *Degenhart* (Fn. 5), Art. 70 Rn. 30; *Ipsen* (Fn. 8), Rn. 596; *Kunig* (Fn. 5), Art. 70 Rn. 23; *von Münch/Mager* (Fn. 12), Rn. 398; *Rozek* (Fn. 10), Art. 70 Rn. 39; a. A. *Ehlers* (Fn. 10), S. 323 (325); *Stern* (Fn. 12), S. 612.

42 BVerfGE, 22, 180 (217); 26, 246 (257).

43 Vgl. BVerfGE, 11, 89 (99); 22, 180 (217); *Degenhart* (Fn. 5), Art. 70 Rn. 32; *Kunig* (Fn. 5), Art. 70 Rn. 27; *Rengeling* (Fn. 5), § 135 Rn. 78; *Sannwald* (Fn. 5), Vorb. v. Art. 70 Rn. 23; *Zippelius/Würtenberger* (Fn. 2), § 45 Rn. 46.

44 *Pieroth* (Fn. 4), Art. 70 Rn. 13; *Rengeling* (Fn. 5), § 135 Rn. 79; *Rozek* (Fn. 10), Art. 70 Rn. 41.

45 *Kunig* (Fn. 5), Art. 70 Rn. 27; wohl auch *Rengeling* (Fn. 5), § 135 Rn. 79: Analogie zu einzelnen Kompetenzartikeln.

46 *Ehlers* (Fn. 10), S. 323 (325); *Kunig* (Fn. 5), Art. 70 Rn. 27; *von Münch/Mager* (Fn. 12), Rn. 398; *Pieroth* (Fn. 4), Art. 70 Rn. 13; *Rozek* (Fn. 10), Art. 70 Rn. 40; *Sannwald* (Fn. 5), Vorb. v. Art. 70 Rn. 23.

b) Keine Bundeskompetenz kraft Natur der Sache für präventiv-polizeiliche Telekommunikationsüberwachung

Ob das oben genannte Argument für die Anerkennung einer Bundeskompetenz kraft Natur der Sache überzeugend ist, ist sehr problematisch[47]. Auf den ersten Blick lässt sich der Begriff der Begriffsnotwendigkeit als ein Kriterium, dem man nicht widersprechen kann, ansehen. Bei näherer Betrachtung erweist sich, dass der Begriff der Begriffsnotwendigkeit nichts begründet. Vielmehr stellt er nur eine inhaltslose Formel dar. Beispielsweise wird die Bestimmung der Bundessymbole in der Rechtsprechung und Literatur als eine auf der Begriffsnotwendigkeit basierende Bundeskompetenz kraft Natur der Sache betrachtet[48]. Schwer zu verstehen ist aber, warum die „Bestimmung der Bundessymbole durch ein Zusammenwirken von Bund und Ländern" nicht begriffsnotwendig oder nicht möglich ist. Zu dieser Frage gibt die Lehre der Bundeskompetenz kraft Natur der Sache keine Antwort. Zwar wird vertreten, dass die Begriffsnotwendigkeit durch eine die gesamte Verfassung umfassende systematische Auslegung (oder Analogie) festgelegt werden könne[49], jedoch ist diese Meinung, die mit Verfassungsauslegung oder Analogie argumentiert, methodisch zweifelhaft. Die Analogie, durch die man Rechtslücken schließen kann, setzt eine Rechtslücke voraus. Falls keine Rechtslücke vorliegt, ist eine Analogie sowohl praktisch unnötig als auch logisch unmöglich. Berücksichtigt man die ausdrückliche Regelung des Art. 70 Abs. 1 GG, kann sich nur eine Folgerung aus dieser grundgesetzlichen Vorschrift ergeben: Art. 70 Abs. 1 GG beseitigt deutlich die Möglichkeit der Rechtslücke im Bereich der Gesetzgebungskompetenzverteilung. Da Art. 73 Abs. 1 GG eine Ordnung der Kompetenzverteilung, in der keine Rechtslücke besteht, bildet, ist es schwer nachzuvollziehen, warum man aus der Analogie eine Bundeskompetenz kraft Natur der Sache herleiten kann. Zudem ist der Versuch, dass man aus einer die gesamte Verfassung umfassenden systematischen Auslegung die Bundeskompetenz kraft Natur der Sache ableitet, ebenfalls misslungen. Denn eine durch Verfassungsauslegung abgeleitete ungeschriebene Bundeskompetenz kann nicht die Grenze, die Art. 70 GG absteckt, überschreiten.

Die durch Art. 70 Abs. 1 GG normierte lückenlose Ordnung der Kompetenzverteilung und die durch Art. 70 Abs. 2 GG abgesteckte Grenze für den Umfang der Bundeskompetenz führen dazu, dass die Bundeskompetenz kraft Natur der Sache keine verfassungsrechtliche Grundlage hat. Zu vermeiden ist deswegen, dass man eine solche aus Sicht der Verfassung sehr problematische ungeschriebene Bundeskompetenz anerkennt. Ausgehend davon lässt sich auch keine Bundeskompetenz kraft Natur der

47 Dazu kritisch *Maurer* (Fn. 8), § 10 Rn. 31.

48 So BVerfGE 3, 407 (422); *Degenhart* (Fn. 5), Art. 70 Rn. 31; *Ehlers* (Fn. 10), S. 323 (325); *Pieroth* (Fn. 4), Art. 70 Rn. 14; *Sannwald* (Fn. 5), Vorb. v. Art. 70 Rn. 24.

49 Siehe oben Fn. 44, 45.

Sache für die präventiv-polizeiliche Telekommunikationsüberwachung begründen.

5. Formelle Verfassungsmäßigkeit der geltenden polizei- und ordnungsgesetzlichen Vorschriften zur präventiv-polizeilichen Telekommunikationsüberwachung

Nach der obigen Erörterung lässt sich festhalten, dass die Länder aufgrund ihrer Kompetenz für die allgemeine Gefahrenabwehr die präventiv-polizeiliche Telekommunikationsüberwachung regeln können. Obwohl der Bund gemäß Art. 73 Abs. 1 Nr. 7 GG eine Gesetzgebungskompetenz für die Telekommunikation besitzt, stellt diese grundgesetzliche Vorschrift keine verfassungsrechtliche Grundlage der Bundesgesetzgebungskompetenz für die Telekommunikationsüberwachung dar. Da keine Bundeskompetenz die Landesgesetzgebungskompetenz für die präventiv-polizeiliche Telekommunikationsüberwachung zur Gefahrenabwehr verdrängt, sind die geltenden polizei- und ordnungsgesetzlichen Ermächtigungsvorschriften zur präventiv-polizeilichen Telekommunikationsüberwachung, die als die ausdrücklichen Rechtsgrundlagen des präventiv-polizeilichen Zugriffs auf die E-Mail-Kommunikation angesehen werden, formell verfassungsmäßig. Zwar kann der Bundesgesetzgeber wegen der neuen Bundeskompetenz für die Bekämpfung des internationalen Terrorismus auch ein Gesetz zur präventiven Telekommunikationsüberwachung erlassen, jedoch beschränkt sich eine solche bundesgesetzliche Regelung zur präventiven Telekommunikationsüberwachung auf den Sachbereich der Bekämpfung des internationalen Terrorismus. Demzufolge hat die neue Bundeskompetenz für die präventive Bekämpfung des internationalen Terrorismus nach Art. 73 Abs. 1 Nr. 9a GG keine Sperrwirkung für die im Sachbereich der allgemeinen Gefahrenabwehr bestehende Kompetenz der Länder. Die formelle Verfassungsmäßigkeit der polizei- und ordnungsgesetzlichen Ermächtigungsvorschriften zur präventiv-polizeilichen Telekommunikationsüberwachung ist nicht durch Art. 73 Abs. 1 Nr. 9a GG ausgeschlossen.

II. Grundsatz des Gesetzesvorbehalts

Nachdem festgestellt wurde, dass die Bundesländer aufgrund ihrer Gesetzgebungskompetenz für die allgemeine Gefahrenabwehr die präventiv-polizeiliche Telekommunikationsüberwachung regeln können, ist im Folgenden zu untersuchen, ob die Durchführung einer präventiv-polizeilichen E-Mail-Überwachung in den Polizei- und Ordnungsgesetzen, die die Landesgesetzgeber im Rahmen ihrer Gesetzgebungskompetenz für die allgemeine Gefahrenabwehr erlassen, eine Rechtsgrundlage finden kann. Wie im 4. Kapitel ausgeführt wurde, greift die präventiv-polizeiliche E-Mail-Überwachung in das Fernmeldegeheimnis der betroffenen Kommunikati-

onsteilnehmer, das ein Grundrecht mit einfachem Gesetzesvorbehalt (Art. 10 Abs. 2 GG) darstellt, ein[50]. Berücksichtigt man, dass die E-Mail-Provider bei der Durchführung einer präventiv-polizeilichen Überwachung eine Mitwirkungspflicht haben, führt die Durchführung der E-Mail-Überwachung auch zum Eingriff in die Berufsausübungsfreiheit der E-Mail-Provider, für die der einfache Gesetzesvorbehalt gemäß Art. 12 Abs. 1 S. 2 GG gilt. Deswegen ist eine gesetzliche Vorschrift, die der Polizei die Befugnis für den Zugriff auf die E-Mail-Kommunikation einräumt, bei der präventiv-polizeilichen Überwachung eines E-Mail-Verkehrs notwendig. Die Polizei darf eine Maßnahme der präventiven E-Mail-Überwachung also nur ergreifen[51], wenn eine solche Rechtsgrundlage besteht.

1. Dreistufige Subsidiarität der polizeirechtlichen Ermächtigungsgrundlagen

Unter der gesetzlichen Ermächtigungsgrundlage der polizeilichen Tätigkeit versteht man nicht die polizeiliche Aufgabenzuweisungsnorm[52], sondern die polizeiliche Befugnisnorm[53]. Während die polizeiliche Aufgabenzuweisungsnorm[54] regelt, *was* die Polizei tut, zeigt die polizeiliche Befugnisnorm, *ob* und *wie* die Polizei ihre Aufgaben erfüllen darf[55]. Aufgrund des (grundrechtlichen) Gesetzesvorbehalts, der im Bereich des Grundrechtsschutzes als eine spezielle Ausprägung des (rechtsstaatlichen) Vorbehalts des Gesetzes angesehen wird, muss jede polizeiliche grundrechtsbeeinträchtigende Maßnahme eine gesetzliche Ermächtigungsgrundlage haben. Da die polizeirechtlichen Aufgabenzuweisungsnormen die Gefahrenabwehr dem Aufgabenkreis der Polizei zuordnen, sind sie Zuständigkeitsvorschriften im Sinne des Verwaltungsorganisationsrechts. Allerdings regeln sie keinen

50 Siehe 4. Kapitel A I 3.

51 Da sich der Grundsatz des Gesetzesvorbehalts aus dem Demokratieprinzip und dem Rechtsstaatsprinzip ergibt (vgl. *Jarass*, in: Jarass/Pieroth, GG, Art. 20 Rn. 46; *Maurer* (Fn. 8), § 8 Rn. 20; *Schulze-Fielitz*, in: Dreier, GG, Bd. 2, Art. 20 (Rechtsstaat) Rn. 105), besteht die Bedeutung des grundrechtlichen Gesetzesvorbehalts bei der präventiv-polizeilichen E-Mail-Überwachung darin, dass er einerseits die demokratische Legitimität der präventiv-polizeilichen E-Mail-Überwachung begründet. Andererseits macht er die präventiv-polizeiliche E-Mail-Überwachung voraussehbar und dient damit der Rechtssicherheit.

52 Nur soweit die polizeiliche Tätigkeit nicht in Grundrechte eingreift, kann die polizeiliche Aufgabenzuweisungsnorm als ihre ausreichende Rechtsgrundlage angesehen werden (vgl. *Götz* (Fn. 1), § 7 Rn. 7; *Pieroth/Schlink/Kniesel*, PolR, § 2 Rn. 45; *Schenke* (Fn. 25), Rn. 36; *Würtenberger/Heckmann*, PolR BW, Rn. 160).

53 Vgl. *Schenke* (Fn. 25), Rn. 36 ff.; *Schoch*, in: Schmidt-Aßmann/Schoch, BesVerwR, 2. Kapitel, Rn. 32 f.; *Würtenberger/Heckmann* (Fn. 52), Rn. 160 f. Die Trennung der polizeilichen Aufgabenzuweisungsnorm von der polizeilichen Befugnisnorm schließt jedoch nicht aus, dass sie aus dem gesetzestechnischen Grund zugleich in einer Vorschrift zusammengefasst werden (vgl. *Schenke* (Fn. 25), Rn. 37).

54 Nachweise bei *Pieroth/Schlink/Kniesel* (Fn. 52), § 5 Rn. 1 mit Fn. 1, 2, 3.

55 *Gusy*, PolR, Rn. 165.

Tatbestand und keine Rechtsfolge der polizeilichen Eingriffstätigkeit. Berücksichtigt man das rechtsstaatliche Bestimmtheitsgebot, darf die polizeirechtliche Aufgabenzuweisungsnorm nicht als eine hinreichende Ermächtigungsgrundlage der in Grundrechte eingreifenden polizeilichen Maßnahmen betrachtet werden[56]. Insoweit bedarf die polizeiliche Eingriffstätigkeit noch einer Befugnisnorm, die die Polizei zu konkreten grundrechtseingreifenden Maßnahmen zur Gefahrenabwehr ermächtigt[57].

Die gesetzlichen Ermächtigungsgrundlagen der polizeilichen Eingriffsbefugnis können Vorschriften der Spezialbefugnisse im Sondergesetz, Regelungen der Standardmaßnahmen in allgemeinen Polizei- und Ordnungsgesetzen und die polizeirechtliche Generalklausel sein[58]. Heute lassen sich die polizeilichen Spezialbefugnisse im Bauordnungsrecht, Wasserrecht, Umweltrecht, Ausländerrecht und Versammlungsrecht usw. finden[59]. Durch die in Sondergesetzen bestehenden Vorschriften der polizeilichen Spezialbefugnisse werden Voraussetzungen des polizeilichen Eingriffs und besondere polizeiliche Maßnahmen zur Gefahrenabwehr in speziellen Sachbereichen geregelt. Die Regelungen der Standardmaßnahmen in allgemeinen Polizei- und Ordnungsgesetzen stellen dagegen im Bereich der allgemeinen Gefahrenabwehr die polizeilichen speziellen Befugnisnormen für bestimmte Gefährdungslagen dar. Im Vergleich dazu legt die polizeirechtliche Generalklausel fest, dass die Polizei allgemein zur Gefahrenabwehr notwendige Maßnahmen treffen kann. Hierbei ist die Rangordnung der unterschiedlichen gesetzlichen Ermächtigungsgrundlagen zu beachten. Nach dem Grundsatz „lex specialis derogat legi generali“ besitzen die Vorschriften der Spezialbefugnisse in Sondergesetzen einen Anwendungsvorrang gegenüber den in allgemeinen Polizei- und Ordnungsgesetzen bestehenden Ermächtigungsvorschriften zu grundrechtseingreifenden Maßnahmen[60]. Hinsichtlich des Verhältnisses zwischen beiden Ermächtigungsgrundlagen in allgemeinen Polizei- und Ordnungsgesetzen ist die Regelung der Standardmaßnahmen – auch aufgrund des Grundsatzes „lex specialis derogat legi generali“ – vorrangig gegenüber der Generalklausel[61]. Insoweit

56 *Schoch* (Fn. 53), Rn. 32; *Würtenberger/Heckmann* (Fn. 52), Rn. 161.

57 *Götz* (Fn. 1), § 7 Rn. 8; *Gusy* (Fn. 55), Rn. 171; *Knemeyer*, PolR, Rn. 141; *Pieroth/Schlink/Kniesel* (Fn. 52), § 2 Rn. 47.

58 *Knemeyer* (Fn. 57), Rn. 148; *Schoch* (Fn. 53), Rn. 33; *Würtenberger/Heckmann* (Fn. 52), Rn. 161.

59 Zur einzelnen Spezialermächtigung *Würtenberger/Heckmann* (Fn. 52), Rn. 257 ff.

60 *Gusy* (Fn. 55), Rn. 170; *Knemeyer* (Fn. 57), Rn. 148.

61 *Götz* (Fn. 1), § 8 Rn. 5; *Gusy* (Fn. 55), Rn. 313; *Knemeyer* (Fn. 57), Rn. 157; *Lambiris*, Klassische Standardbefugnisse, S. 43; *Schenke* (Fn. 25), Rn. 38; *Schoch* (Fn. 53), Rn. 53; *Würtenberger/Heckmann* (Fn. 52), Rn. 250.

gibt es eine dreistufige Subsidiarität der Ermächtigungsgrundlagen im Bereich des Polizeirechts[62].

Da es bisher keine Vorschriften zur präventiv-polizeilichen E-Mail-Überwachung in einem Sondergesetz (insbesondere: im Bereich des Medienrechts) gibt[63], beschränkt sich die folgende Diskussion der gesetzlichen Ermächtigungsgrundlage für die präventiv-polizeiliche E-Mail-Überwachung auf die Vorschriften des allgemeinen Polizei- und Ordnungsgesetzes.

2. Regelungen der Standardmaßnahmen als gesetzliche Grundlagen der präventiv-polizeilichen E-Mail-Überwachung

Berücksichtigt man die Subsidiarität der polizeirechtlichen Generalklausel und die größere Klarheit der polizei- und ordnungsgesetzlichen Vorschriften zu Standardmaßnahmen, ist zunächst zu prüfen, ob der präventiv-polizeiliche Zugriff auf die E-Mail-Kommunikation in den vorhandenen Regelungen der Standardmaßnahmen seine Rechtsgrundlage finden kann.

a) Rechtsstaatliche Bedeutung der polizeilichen Standardmaßnahmen

Durch die vom Gesetzgeber im allgemeinen Polizei- und Ordnungsgesetz normierten Standardmaßnahmen werden bestimmte häufig wiederkehrende polizeirechtliche Gefährdungslagen typisiert[64]. In diesen typisierten Gefahrensituationen kann die Polizei nur nach den Tatbestandsvoraussetzungen und Rechtsfolgen, die in den Vorschriften der Standardmaßnahmen geregelt werden, handeln. Unter dem Aspekt des Rechtsstaatsprinzips besteht die Bedeutung der polizeirechtlichen Standardmaßnahmen darin, dass die polizeilichen Eingriffsbefugnisse dadurch standardisiert sind[65]. Denn die abzuwehrenden Gefahrensituationen und die zu schützenden Rechtsgüter, die die Tatbestandvoraussetzungen des polizeilichen Eingriffs darstellen, werden durch die Standardmaßnahmen konkreter und klarer gefasst. In Grundrechte darf zur Beseitigung bestimmter Gefahrensituationen nur eingegriffen werden, wenn die in Vorschriften der Standardmaßnahmen vorgeschriebenen Tatbestände erfüllt werden. Davon ausgehend dienen Standardmaßnahmen der Übersichtlichkeit und Rechtklarheit[66]. Zudem haben die Standardmaßnahmen auch eine Bedeutung für den Verhältnismäßigkeitsgrundsatz[67]. Im Gegensatz zur umfassenden Rechtsfolge der Generalklausel (notwendige Maßnahmen) darf die Polizei zur Abwehr

62 *Würtenberger/Heckmann* (Fn. 52), Rn. 250.

63 Wie bereits im 2. Kapitel dargelegt wurde, kann § 59 RStV nicht als die Rechtsgrundlage der präventiv-polizeilichen E-Mail-Überwachung betrachtet werden (siehe 2. Kapitel C. II 3).

64 *Götz* (Fn. 1), § 8 Rn. 11; *Knemeyer* (Fn. 57), Rn. 149; *Schoch* (Fn. 53), Rn. 191; *Tettinger/Erbguth/Mann*, BesVerwR, Rn. 565; *Würtenberger/Heckmann* (Fn. 52), Rn. 305.

65 Vgl. *Schoch* (Fn. 53), Rn. 191; *Würtenberger/Heckmann* (Fn. 52), Rn. 305.

66 *Schoch* (Fn. 53), Rn. 191; *Würtenberger/Heckmann* (Fn. 52), Rn. 305.

67 Vgl. *Schoch* (Fn. 53), Rn. 191; *Würtenberger/Heckmann* (Fn. 52), Rn. 314.

bestimmter Gefahrensituationen, die in Vorschriften zu Standardmaßnahmen umschrieben werden, nur bestimmte Maßnahmen ergreifen[68]. Die Reduzierung des polizeilichen Auswahlermessens auf bestimmte Maßnahmen lässt sich als die Konsequenz der vom Gesetzgeber vorweggenommenen Güterabwägung ansehen[69]. Insoweit konkretisieren die Standardmaßnahmen den Verhältnismäßigkeitsgrundsatz[70] und vermeiden ein übermäßiges polizeiliches Auswahlermessen[71].

b) Polizei- und ordnungsgesetzliche Vorschriften zur Telekommunikationsüberwachung als Ermächtigungsgrundlage der präventiv-polizeilichen E-Mail-Überwachung

Es wurde ausgeführt, dass in Baden-Württemberg, Bayern, Brandenburg, Hamburg, Hessen, Mecklenburg-Vorpommern, Niedersachsen, Rheinland-Pfalz, Saarland, Schleswig-Holstein und Thüringen spezielle Ermächtigungsvorschriften zur Telekommunikationsüberwachung in den allgemeinen Polizei- und Ordnungsgesetzen bestehen[72]. Systematisch gehört diese neue polizeiliche Befugnis zu den informationellen Standardmaßnahmen[73]. Da ein E-Mail-Verkehr eine Telekommunikation ist, können diese polizei- und ordnungsgesetzlichen Ermächtigungsvorschriften zur Telekommunikationsüberwachung als Rechtsgrundlage der präventiv-polizeilichen E-Mail-Überwachung angesehen werden.

c) Polizei- und ordnungsgesetzliche Vorschriften zum verdeckten Einsatz technischer Mittel als Ermächtigungsgrundlage der präventiv-polizeilichen E-Mail-Überwachung?

Da die präventiv-polizeiliche E-Mail-Überwachung heimlich erfolgt, stellt sich die Frage, ob die Polizei in den Bundesländern, in denen eine aus-

68 *Götz* (Fn. 1), § 8 Rn. 11; *Pieroth/Schlink/Kniesel* (Fn. 52), § 12 Rn. 4.

69 *Würtenberger/Heckmann* (Fn. 52), Rn. 314. Insoweit legt der Gesetzgeber selbst durch die Vorschriften der Standardmaßnahmen die Voraussetzungen und die Grenzen des polizeilichen Eingriffshandelns fest (vgl. *Butzer*, VerwArch 93 (2002), S. 506 (523)).

70 *Würtenberger/Heckmann* (Fn. 52), Rn. 314.

71 Dies bedeutet jedoch nicht, dass die Vorschriften der Standardmaßnahmen eine Garantie der Verhältnismäßigkeit sind.

72 Siehe 2. Kapitel C II 1.

73 Im bwPolG: dritter Unterabschnitt (des zweiten Abschnitts) Datenerhebung; im bayPAG: dritter Abschnitt Datenerhebung und -verarbeitung; im bbgPolG: zweiter Abschnitt Datenverarbeitung; im hambGDatPol: zweiter Abschnitt Besondere Befugnisse zur Datenerhebung; im mvSOG: erster Unterabschnitt (des dritten Abschnitts) Datenerhebung; im ndsSOG: zweiter Abschnitt Befugnisse zur Datenverarbeitung; im shLVwG: Abschnitt 3 Unterabschnitt 2 II 2. Datenerhebung; im saarlPolG: zweiter Unterabschnitt (des zweiten Abschnitts) Befugnisse zur Informationsverarbeitung; im thürPAG: zweiter Unterabschnitt (des zweiten Abschnitts) Datenerhebung und -verarbeitung. Im hessSOG und rpPOG besteht keine systematische Gliederung der polizeilichen Standardmaßnahmen.

drückliche polizei- und ordnungsgesetzliche Ermächtigungsvorschrift zur Telekommunikationsüberwachung fehlt, die polizei- und ordnungsgesetzlichen Vorschriften über den verdeckten Einsatz technischer Mittel bzw. über die Datenerhebung in oder aus Wohnungen[74] als Rechtsgrundlage der präventiv-polizeilichen E-Mail-Überwachung heranziehen kann[75]. Berücksichtigt man nur den Wortlaut einer solchen Vorschrift, könnte ein präventiv-polizeilicher Zugriff auf die E-Mail-Kommunikation in ihren Regelungsbereich fallen. Jedoch ist darüber hinaus zu beachten, dass die Polizei- und Ordnungsgesetze dieser Bundesländer, die keine ausdrückliche Regelung zur Telekommunikationsüberwachung enthalten, das Fernmeldegeheimnis des Art. 10 Abs. 1 GG nicht unter den einschränkbaren Grundrechten nennen[76]. Dementsprechend scheitert der verdeckte Einsatz technischer Mittel bzw. die Datenerhebung in oder aus Wohnungen am Zitiergebot des Art. 19 Abs. 1 Satz 2 GG[77]. Daher stellen diese Vorschriften keine Rechtsgrundlage für eine präventiv-polizeilichen E-Mail-Überwachung dar[78].

d) Polizei- und ordnungsgesetzliche Vorschriften zur Durchsuchung von Sachen und zur Beschlagnahme als Ermächtigungsgrundlage der präventiv-polizeilichen E-Mail-Überwachung?

Alle Polizei- und Ordnungsgesetze enthalten Regelungen zur Durchsuchung von Sachen und zu deren Beschlagnahme[79]. Systematisch kann die Durchsuchung einer Sache als eine Standardmaßnahme zur Gefahrenaufklärung angesehen werden[80]. Zudem wird in der strafprozessualen Literatur teilweise vertreten, dass § 94 StPO (Beschlagnahme) die Rechtsgrundlage des Zugriffs auf die E-Mail, die sich in der 2. Phase der E-Mail-Übertragung befinde[81], darstellen könne[82]. Insoweit ist zu prüfen, ob poli-

74 § 25 Abs. 1 S. 1 Nr. 2 berlASOG; § 33 bremPolG; § 17 nwPolG; § 39 sächsPolG; § 17 saSOG.

75 Dafür: *Pieroth/Schlink/Kniesel* (Fn. 52), § 14 Rn. 130; dagegen: *Kugelmann*, PolR, 5. Kapitel Rn. 149; *Schenke* (Fn. 25), Rn. 197a; *Tischer* (Fn. 4), S. 477; *Würtenberger/Heckmann* (Fn. 52), Rn. 620.

76 Vgl. § 66 berlASOG; § 9 bremPolG; § 7 nwPolG; § 79 sächsPolG; § 11 saSOG.

77 *Tischer* (Fn. 4), S. 477. Zwar bejahen *Pieroth/Schlink/Kniesel* die Anwendung der Bestimmungen über den verdeckten Einsatz technischer Mittel, jedoch erkennen sie zugleich an, dass die Verletzung des Zitiergebots ein gewichtiger Grund für die Gegenmeinung ist (*Pieroth/Schlink/Kniesel* (Fn. 52), § 14 Rn. 132).

78 Vgl. *Kugelmann* (Fn. 75), 5. Kapitel Rn. 149; *Schenke* (Fn. 25), Rn. 197a; *Würtenberger/Heckmann* (Fn. 52), Rn. 620.

79 Nachweise bei *Schenke* (Fn. 25), Rn. 151 mit Fn. 356, Rn. 158 mit Fn. 382.

80 *Gusy* (Fn. 55), Rn. 180, 251 ff.

81 D. h., die E-Mail ruht im Mailserver und wird noch nicht abgerufen.

82 So *Bär*, MMR 2000, S. 472 (474 f.); *Nack*, in: Hannich, StPO, § 100a Rn. 22; a. A. LG Hanau NJW 1999, S. 3647; *Beulke*, Strafprozessrecht, Rn. 253; *Kindhäuser*, Strafprozessrecht, § 8 Rn. 82; *Meyer-Goßner*, StPO, § 100a Rn. 6; *Murmann*, in: Heghmanns/Scheffler, Handbuch zum Strafverfahren, III. Kapitel Rn. 193; *Schäfer*, in: Rieß, StPO, § 100a Rn. 58.

zei- und ordnungsgesetzliche Vorschriften zur Durchsuchung von Sachen und zur Beschlagnahme zur präventiv-polizeilichen E-Mail-Überwachung ermächtigen können.

Die Möglichkeit, dass die präventiv-polizeiliche E-Mail-Überwachung ihre Rechtsgrundlage in polizei- und ordnungsgesetzlichen Vorschriften zur Durchsuchung von Sachen und zur Beschlagnahme finden kann, ist aus zwei Gründen zu verneinen. Zunächst erfolgen sowohl die Durchsuchung einer Sache als auch die Beschlagnahme grundsätzlich offen[83]. Dies ist bei der präventiv-polizeilichen E-Mail-Überwachung, die eine heimliche polizeiliche Tätigkeit zur Informationserhebung ist, nicht der Fall. Ferner ist der Telekommunikationsvorgang noch nicht abgeschlossen, bevor der Empfänger die auf dem Mailserver der Provider ruhende E-Mail abgerufen hat. Davon ausgehend wird die E-Mail vor dem Abruf durch den Empfänger (auch in der 2. Phase des Übertragungsvorgangs) durch das Fernmeldegeheimnis geschützt. Dies gilt auch für den Fall der Webmail, in dem die E-Mail in der Mailbox auf dem Webmail-Server ruht und noch nicht abgerufen wurde[84]. Soweit das Fernmeldegeheimnis des Art. 10 Abs. 1 GG im Anwendungsbereich des Polizei- und Ordnungsgesetzes nicht durch die Klarstellung des Gesetzgebers als ein einschränkbares Grundrecht angesehen wird, können die polizei- und ordnungsgesetzlichen Ermächtigungsvorschriften zur Durchsuchung von Sachen und zur Beschlagnahme nicht den präventiv-polizeilichen Zugriff auf eine im Mailserver der Provider zwischengespeicherte E-Mail begründen. Ansonsten führte dies zu einer Verletzung des Art. 19 Abs. 1 Satz 2 GG.

e) Generalklausel der Informationserhebung als Ermächtigungsgrundlage der präventiv-polizeilichen E-Mail-Überwachung?

Zu erwägen ist weiter, ob sich eine polizeiliche Befugnis zur präventiven E-Mail-Überwachung aus der Generalklausel der Informationserhebung im Polizei- und Ordnungsgesetz ergeben kann. Heute gibt es in allen Polizei- und Ordnungsgesetzen der Länder eine Generalklausel der Informationserhebung[85]. Dadurch besitzt die polizeiliche Maßnahme zur Informationserhebung eine allgemeine Ermächtigungsgrundlage in den Polizei- und Ordnungsgesetzen. Falls die Anwendung der polizei- und ordnungsgesetzlichen Vorschriften, die der Spezialbefugnis der Informationserhebung dienen, unmöglich ist, lässt sich daran denken, die allgemeine Ermächtigungsvorschrift der Informationserhebung aufgrund ihrer Auffangwirkung heranzuziehen[86].

83 *Schenke* (Fn. 25), Rn. 151, 159.

84 Vgl. dazu 4. Kapitel A I 3 c).

85 Nachweise bei *Schenke* (Fn. 25), Rn. 181 mit Fn. 444.

86 *Pieroth/Schlink/Kniesel* (Fn. 52), § 13 Rn. 24; *Schenke* (Fn. 25), Rn. 181.

Im Schrifttum wird vertreten, dass der Anwendungsbereich für die polizei- und ordnungsgesetzliche Generalklausel der Informationserhebung auf die offene Beschaffung der Informationen begrenzt sei, da die verdeckte Informationserhebung in den Standardmaßnahmen geregelt sei[87]. Aus diesem Grund stütze die Generalklausel der Informationserhebung keine verdeckte polizeiliche Maßnahme zur Informationserhebung. Ob diese Auffassung zutreffend ist, ist jedoch zweifelhaft. Zunächst findet diese Begrenzung des Anwendungsbereichs keine Anhaltspunkte im positiven Recht. Jedenfalls bildet die geltende Generalklausel der Informationserhebung nach ihrem Wortlaut eine solche Anwendungsgrenze nicht[88].

Obwohl verdeckte polizeiliche Maßnahmen zur Informationsbeschaffung von der Generalklausel der Informationserhebung umfasst werden können, lässt sich die Generalklausel der Informationserhebung in den Bundesländern, deren Polizei- und Ordnungsgesetze keine speziellen Ermächtigungsvorschriften zur Telekommunikationsüberwachung enthalten, nicht als Rechtsgrundlage der präventiv-polizeilichen E-Mail-Überwachung betrachten. Der Grund besteht darin, dass das Fernmeldegeheimnis des Art. 10 Abs. 1 GG in Polizei- und Ordnungsgesetzen dieser Bundesländer nicht als ein einschränkbares Grundrecht genannt wird[89]. Im Hinblick auf Art. 19 Abs. 1 Satz 2 GG, ist eine dem Zugriff auf die E-Mail-Kommunikation dienende und damit in das Fernmeldegeheimnis eingreifende Anwendung der Generalklausel der Informationserhebung verfassungsrechtlich unzulässig[90].

Diese Folgerung lässt sich auch aus dem rechtsstaatlichen Gebot der Bestimmtheit der Norm[91] ableiten[92]. Bei der Ermächtigung zu Überwachungsmaßnahmen, die zu einem schweren Grundrechtseingriff führen, muss sich die Anforderung an die Bestimmtheit der Norm erhöhen[93]. Da die Generalklausel der Informationserhebung keine höhere Bestimmtheit hat, kann sie nicht die Ermächtigungsgrundlage der präventiv-polizeilichen Telekommunikationsüberwachung darstellen.

87 So *Koch*, Datenerhebung, S. 94.

88 Zur Zulässigkeit der verdeckten Informationserhebung nach der geltenden Generalklausel der Informationserhebung in Polizei- und Ordnungsgesetzen *Pieroth/Schlink/Kniesel* (Fn. 52), § 13 Rn. 21 mit Fn. 24.

89 Nachweise siehe oben Fn. 76.

90 *Schenke* (Fn. 25), Rn. 197a.

91 Zur Bestimmtheit der polizei- und ordnungsgesetzlichen Ermächtigungsgrundlagen zur Telekommunikationsüberwachung siehe unten B I 3.

92 *Koch* (Fn. 87), S. 95; wohl auch *Petri*, in: Lisken/Denninger, HPolR, H Rn. 173; *Pieroth/Schlink/Kniesel* (Fn. 52), § 13 Rn. 24.

93 BVerfGE 113, 348 (376).

f) Polizeirechtliche Generalklausel als Ermächtigungsgrundlage der präventiv-polizeilichen E-Mail-Überwachung?

Aufgrund ihrer Subsidiarität kommt die polizeirechtliche Generalklausel, die die allgemeine gesetzliche Ermächtigungsgrundlage der zur Gefahrenabwehr notwendigen Maßnahmen darstellt[94], in Betracht, soweit keine polizei- und ordnungsgesetzlichen Regelungen der Standardmaßnahmen angewendet werden können. Erörterungsbedürftig ist deswegen, ob die polizeirechtliche Generalklausel die Ermächtigungsgrundlage der präventiv-polizeilichen E-Mail-Überwachung sein kann.

D. Kugelmann verneint dies, weil der „spezifische Eingriff" vielfache Verfahrensanforderungen und erhöhte Eingriffsschwellen benötige[95]. Zwar ist dieser Folgerung zuzustimmen, allerdings ist die Begründung kritikwürdig. *D. Kugelmann* klärt nicht, warum die präventiv-polizeiliche Telekommunikationsüberwachung einen „spezifischen Eingriff" darstellen soll. Seine Begründung basiert einerseits wohl darauf, dass das Fernmeldegeheimnis, in das durch die präventiv-polizeiliche Telekommunikationsüberwachung eingegriffen wird, eine spezifische Position gegenüber anderen Grundrechten besitze. Andererseits dürfte seine Begründung auch davon ausgehen, dass eine verdeckte Informationserhebung zu einem relativ starken Grundrechtseingriff führe. Ob sich das Ergebnis, dass die präventiv-polizeiliche Telekommunikationsüberwachung nicht in der polizeirechtlichen Generalklausel ihre Rechtsgrundlage findet, aus diesen beiden Ausgangspunkten ergeben kann, ist aber zweifelhaft.

Der Ausgangspunkt, dass das durch Art. 10 GG geschützte Fernmeldegeheimnis eine höhere Eingriffsschwelle fordere, ist problematisch. Warum der Eingriff in das Fernmeldegeheimnis – im Vergleich zum Eingriff in andere Grundrechte – einen spezifischen Eingriff darstellt, ist kaum zu begründen. Jedenfalls ergibt sich aus dem Grundgesetz eine solche Sonderstellung des Fernmeldegeheimnisses gegenüber anderen Grundrechten nicht. Das Grundgesetz bestimmt auch nicht, dass die Eingriffsschwellen des Fernmeldegeheimnisses höher als bei Eingriffen in andere Grundrechte sein müssen. Insoweit ist die von „spezifischer Position des Fernmeldegeheimnisses" ausgehende Begründung nicht überzeugend. Darüber hinaus kann die zweite Prämisse, dass die verdeckte polizeiliche Informationserhebung zu einem schweren Grundrechtseingriff führe, nicht das Ergebnis, dass die polizeirechtliche Generalklausel keine Rechtsgrundlage der präventiv-polizeilichen Telekommunikationsüberwachung darstellen kann, begründen. Denn hinsichtlich des Verhältnisses zwischen den speziellen Ermächtigungen (Standardmaßnahmen) und der polizeirechtlichen Generalklausel spielt es keine Rolle, ob die Standardmaßnahmen schwerere

94 Nachweise bei *Pieroth/Schlink/Kniesel* (Fn. 52), § 7 Rn. 1 mit Fn. 1.
95 *Kugelmann* (Fn. 75), 5. Kapitel Rn. 149.

bzw. intensivere Grundrechtseingriffe regeln. Maßgeblich ist vielmehr, dass die Regelungen der Standardmaßnahmen zu den typischen Grundrechtseingriffen berechtigen[96]. Eine neue polizeiliche Maßnahme, die stark in das Grundrecht eingreift und noch keine speziellen Ermächtigungsgrundlagen besitzt, kann – zumindest für eine Übergangszeit – auch auf die polizeirechtliche Generalklausel gestützt werden[97]. Deswegen kann alleine die Schwere eines Grundrechtseingriffes kein zutreffendes Argument für die Ablehnung der Anwendung der polizeilichen Generalklausel sein.

Die überzeugendere (wohl auch einzige) Begründung für die Konsequenz, dass die polizeirechtliche Generalklausel in den Bundesländern, deren Polizei- und Ordnungsgesetze noch keine speziellen Ermächtigungsvorschriften zur Telekommunikationsüberwachung enthalten, den präventiv-polizeilichen Zugriff auf die E-Mail-Kommunikation nicht stützen kann, ist wiederum das Zitiergebot des Art. 19 Abs. 1 Satz 2 GG. Da der Gesetzgeber dieser Bundesländer im Anwendungsbereich des Polizei- und Ordnungsgesetzes das Fernmeldegeheimnis des Art. 10 Abs. 1 GG nicht als ein einschränkbares Grundrecht betrachtet[98], stellt die polizeirechtliche Generalklausel keine gesetzliche Ermächtigungsgrundlage der präventiv-polizeilichen Telekommunikationsüberwachung dar[99]. Die Folgerung, dass die polizeirechtliche Generalklausel nicht als eine Ermächtigungsgrundlage der präventiv-polizeilichen Telekommunikationsüberwachung angesehen werden kann, lässt sich, wie bereits dargelegt wurde[100], zudem aus der erhöhten Anforderung an die Bestimmtheit der Norm herleiten.

B. Materielle Verfassungsmäßigkeit der geltenden polizei- und ordnungsgesetzlichen Ermächtigungsvorschriften zur Telekommunikationsüberwachung

Nach der obigen Erörterung lässt sich feststellen, dass die präventiv-polizeiliche E-Mail-Überwachung (nur) in den Bundesländern, in denen eine polizei- und ordnungsgesetzliche Ermächtigungsvorschrift zur Telekommunikationsüberwachung besteht, ihre Rechtsgrundlage finden kann. Zu

96 Vgl. *Götz* (Fn. 1), § 8 Rn. 11; *Gusy* (Fn. 55), Rn. 179; *Lambiris* (Fn. 61), S. 37; *Pieroth/Schlink/Kniesel* (Fn. 52), § 7 Rn. 20; *Schoch* (Fn. 53), Rn. 56, 191; *Würtenberger/Heckmann* (Fn. 52), Rn. 305; a. A. BVerwGE 129, 142 (149 f.); *Rachor*, in: Lisken/Denninger, HPolR, F Rn. 502, 789; *Schenke* (Fn. 25), Rn. 49.

97 *Pieroth/Schlink/Kniesel* (Fn. 52), § 7 Rn. 20; *Schoch* (Fn. 53), Rn. 56, 191; a. A. *Schenke* (Fn. 25), Rn. 49.

98 Nachweise siehe oben Fn. 76.

99 *Gusy*, in: von Mangoldt/Klein/Starck, GG, Bd. 1, Art. 10 Rn. 70; *Hufen* (Fn. 2), § 17 Rn. 13; *Jarass* (Fn. 51), Art. 10 Rn. 17; *Löwer* (Fn. 4), Art. 10 Rn. 29; *Schenke* (Fn. 25), Rn. 197a; *C. Sievers*, Telekommunikationsüberwachung, S. 62; *Würtenberger/Heckmann* (Fn. 52), Rn. 625a.

100 Siehe oben e).

prüfen ist weiter, ob die Rechtsgrundlagen präventiv-polizeilicher E-Mail-Überwachung, also die polizei- und ordnungsgesetzlichen Ermächtigungsvorschriften zur Telekommunikationsüberwachung, materiell verfassungsmäßig sind. Bei der Prüfung der materiellen Verfassungsmäßigkeit geht es um vielfältige verfassungsrechtliche Schranken des Grundrechtseingriffs. Die polizei- und ordnungsgesetzlichen Regelungen zur präventiven Telekommunikationsüberwachung können materiell mit der Verfassung in Einklang nur stehen, wenn sie diesen allgemeinen verfassungsrechtlichen Anforderungen genügen.

I. Anforderung an die Bestimmtheit der Gesetze

1. Bestimmtheit der Gesetze als rechtsstaatliche Anforderung

Zunächst lässt sich untersuchen, ob die geltenden polizei- und ordnungsgesetzlichen Ermächtigungsvorschriften zur Telekommunikationsüberwachung dem Bestimmtheitsgebot[101] entsprechen. Während der Bestimmtheitsgrundsatz des Art. 103 Abs. 2 GG nur für Strafgesetze gilt, ergibt sich der allgemeine Bestimmtheitsgrundsatz aus dem Rechtsstaatsprinzip (Art. 20 Abs. 3 GG)[102]. Dieser lässt sich sowohl als Präzisierung des Gesetzesvorbehaltes[103] als auch als Konkretisierung des Gebots der Rechtssicherheit[104] ansehen. Nach dieser rechtstaatlichen Anforderung müssen die Tatbestände der Gesetze hinreichend bestimmt sein[105]. Vor allem ist das Gebot der Bestimmtheit des Gesetzes erhöht, soweit das Gesetz eine Ermächti-

101 Der Begriff der Gesetzesbestimmtheit überschneidet sich mit dem Begriff der Gesetzesklarheit. Sie lassen sich als Synonyme ansehen (vgl. BVerfGE 93, 213 (238); 113, 348 (375 f.); *Degenhart*, Staatsorganisationsrecht, Rn. 356; *Jarass* (Fn. 51), Art. 20 Rn. 63; *Kunig*, Rechtsstaatsprinzip, S. 396 ff.; *Maurer* (Fn. 8), § 8 Rn. 47; *Sodan* in: Sodan, GG, Art. 20 Rn. 55; *Sommermann*, in: von Mangoldt/Klein/Starck, GG, Bd. 2, Art. 20 Rn. 289; *Zippelius/Würtenberger* (Fn. 2), § 7 Rn. 56; wohl auch *Sachs* in: Sachs, GG, Art. 20 Rn. 126: Von inhaltlicher Klarheit nicht eindeutig abzugrenzen ist die Bestimmtheit; a. A. *Jehke*, Bestimmtheit und Klarheit, S. 178 ff.; *Schmidt-Aßmann*, Ordnungsidee, Kapitel 4 Rn. 27 f.; *Schulze-Fielitz* (Fn. 51), Art. 20 (Rechtsstaat) Rn. 141: Das Gebot der (äußeren) Klarheit ist von dem Gebot der (inneren) Bestimmtheit zu unterscheiden).

102 Vgl. BVerfGE 86, 288 (311); *Degenhart* (Fn. 101), Rn. 356; *Jarass* (Fn. 51), Art. 20 Rn. 57; *Kunig* (Fn. 101), S. 396; *Maurer* (Fn. 8), § 8 Rn. 46; *von Münch/Mager* (Fn. 12), Rn. 659; *Sachs* (Fn. 101), Art. 20 Rn. 126; *Schmidt-Aßmann* (Fn. 101), Kapitel 4 Rn. 28; *Schnapp*, in: von Münch/Kunig, GG, Bd. 2, Art. 20 Rn. 29; *Sommermann* (Fn. 101), Art. 20 Rn. 287 ff.; *Schulze-Fielitz* (Fn. 51), Art. 20 (Rechtsstaat) Rn. 129.

103 BVerfGE 80, 137 (161); *Degenhart* (Rn. 101), Rn. 356; *Hofmann*, in: Schmidt-Bleibtreu/Hofmann/Hopfauf, GG, Art. 20 Rn. 85; *Jarass* (Fn. 51), Art. 20 Rn. 54; *Kunig* (Fn. 101), S. 400; *Schmidt-Aßmann* (Fn. 101), Kapitel 4 Rn. 28; *Sommermann* (Fn. 101), Art. 20 Rn. 290.

104 *Degenhart* (Rn. 101), Rn. 356; *Jarass* (Fn. 51), Art. 20 Rn. 57; *Kunig* (Fn. 101), S. 396; *Maurer* (Fn. 8), § 8 Rn. 46; *Sachs* (Fn. 101), Art. 20 Rn. 122; *Schmidt-Aßmann* (Fn. 101), Kapitel 4 Rn. 26; *Schulze-Fielitz* (Fn. 51), Art. 20 (Rechtsstaat) Rn. 129; *Sommermann* (Fn. 101), Art. 20 Rn. 289; *Zippelius/Würtenberger* (Fn. 2), § 12 Rn. 62.

105 Vgl. BVerfGE 57, 295 (320 f.).

gungsgrundlage für einen Grundrechtseingriff darstellt[106]. In diesem Punkt sind der Anlass, der Zweck und die Grenzen des Grundrechtseingriffs in der Ermächtigung bereichsspezifisch, präzise und normenklar festzulegen[107].

Durch die Bestimmtheit der Gesetze lässt sich sicherstellen, dass der Betroffene die Rechtslage erkennen und sich auf mögliche belastende Maßnahmen einstellen kann[108]. Der Bürger muss erkennen können, wie weit der Kreis der Gesetzesadressaten ist und unter welchen gesetzlichen Voraussetzungen die Grundrechte eingeschränkt werden können. Die möglichen Eingriffsmaßnahmen müssen in ihren gesetzlichen Ermächtigungsgrundlagen vorhersehbar sein. Insoweit besteht die Bedeutung der Gesetzesbestimmtheit für die Betroffenen darin, dass der Gesetzesadressat aufgrund hinreichend bestimmter Gesetzesinhalte die Rechtsfolge seines Verhaltens kalkulieren kann.

Zudem hat das Bestimmtheitsgebot auch eine Begrenzungsfunktion für die Verwaltung. So muss die gesetzliche Ermächtigung zur (belastenden) Tätigkeit der Verwaltung nach Inhalt, Zweck und Ausmaß so bestimmt sein, dass das Verwaltungshandeln messbar und voraussehbar ist[109]. Obwohl sich ein Handlungsspielraum der Exekutive – im Rahmen der nichtgebundenen Verwaltung[110] – nach der Lehre des Ermessens allgemein anerkennen lässt (Entschließungsermessen und Auswahlermessen der Behörde)[111],

106 Vgl. BVerfGE 5, 104 (114); 86, 288 (311); 108, 52 (75); 117, 71 (111); *Degenhart* (Rn. 101), Rn. 329, 358; *Hofmann* (Fn. 103), Art. 20 Rn. 85; *Maurer* (Fn. 8), § 8 Rn. 47; *Sachs* (Fn. 101), Art. 20 Rn. 128; *Schulze-Fielitz* (Fn. 51), Art. 20 (Rechtsstaat) Rn. 136; *Zippelius/Würtenberger* (Fn. 2), § 12 Rn. 63. Das Gebot der Gesetzesbestimmtheit gilt auch für die Ausführung staatlicher Leistungsaufgaben (vgl. BVerfGE 108, 52 (75); *Zippelius/Würtenberger* (Fn. 2), § 12 Rn. 63; wohl auch *Maurer* (Fn. 8), § 8 Rn. 47).

107 BVerfGE 110, 33 (53); 113, 348 (375); vgl. auch *Degenhart* (Rn. 101), Rn. 325; *Hofmann* (Fn. 103), Art. 20 Rn. 85; *Jarass* (Fn. 51), Art. 20 Rn. 61; *Schulze-Fielitz* (Fn. 51), Art. 20 (Rechtsstaat) Rn. 136; *Zippelius/Würtenberger* (Fn. 2), § 12 Rn. 63.

108 BVerfGE 83, 130 (145); 110, 33 (53); 113, 348 (375 f.); 120, 274 (316); *Degenhart* (Rn. 101), Rn. 356; *Maurer* (Fn. 8), § 8 Rn. 47; *Sachs* (Fn. 101), Art. 20 Rn. 129; *Schulze-Fielitz* (Fn. 51), Art. 20 (Rechtsstaat) Rn. 129.

109 BVerfGE 69, 1 (41); 110, 33 (54); 113, 348 (376); *Jarass* (Fn. 51), Art. 20 Rn. 61; *Schulze-Fielitz* (Fn. 51), Art. 20 (Rechtsstaat) Rn. 136; *Zippelius/Würtenberger* (Fn. 2), § 12 Rn. 63.

110 Zur Differenzierung zwischen gebundener Verwaltung und nichtgebundener Verwaltung (Ermessensverwaltung) *Detterbeck*, AllgVerwR, Rn. 304 ff.; *Maurer*, AllgVerwR, § 1 Rn. 24; *Peine*, AllgVerwR, Rn. 200 f.; *Sachs*, in: Stelkens/Bonk/Sachs, VwVfG, § 40 Rn. 12 f.; kritisch dazu aber *Jestaedt*, in: Erichsen/Ehlers, AllgVerwR, § 10 Rn. 17. Zu beachten ist, dass die nichtgebundene Verwaltung (Ermessensverwaltung), die einer gesetzlichen Ermessensgrundlage bedarf, keine gesetzesfreie Verwaltung, die ohne gesetzliche Ermächtigungsgrundlage ausgeführt wird, ist (vgl. *Detterbeck*, AllgVerwR, Rn. 308; *Maurer*, AllgVerwR, § 1 Rn. 25).

111 Dazu *Detterbeck* (Fn. 110), Rn. 311 ff.; *Jestaedt* (Fn. 110), § 10 Rn. 55 ff.; *Maurer* (Fn. 110), § 7 Rn. 7 ff.; *Peine* (Fn. 110), Rn. 204 ff.; *Sachs* (Fn. 110), § 40 Rn. 21 ff.; *Schoch*, JURA 2004, S. 462 ff.

darf dies zu keinem Verlust an Rechtssicherheit führen. Aus diesem Grund dürfen Grundrechte unter dem Gesichtspunkt des Rechtsstaatsprinzips nicht einseitig durch Ermessensentscheidungen der Verwaltung begrenzt werden[112]. Vielmehr sind die Entscheidungen der Verwaltungsbehörde durch hinreichend bestimmte gesetzliche Tatbestände, die der Verwaltung einen Ermessensspielraum einräumen, zu begrenzen. Je bestimmter die Maßstäbe gesetzlicher Ermächtigung sind, desto voraussehbarer ist das Verhalten der Exekutive. Um die Verwaltung zu binden und damit die Grundrechte der Bürger zu schützen, muss der Gesetzgeber die Anforderung an die Bestimmtheit der Gesetze beachten.

Ferner spielt das Gebot der Bestimmtheit der Gesetze auch eine große Rolle für die Judikative. Denn die gerichtliche Kontrolle der Verwaltungstätigkeit setzt voraus, dass ein hinreichend bestimmter rechtlicher Maßstab vorliegt[113]. Soweit die Gesetze, die die Prüfungsmaßstäbe darstellen, nicht ausreichend bestimmt sind, wird die gerichtliche Rechtskontrolle erschwert.

2. Besondere Bedeutung des Bestimmtheitsgebots für die präventiv-polizeiliche Telekommunikationsüberwachung

Bei heimlichen Überwachungsmaßnahmen sind die Anforderungen an die Bestimmtheit der Gesetze besonderes wichtig[114]. Der Grund hierfür besteht darin, dass der Betroffene von der versteckten Überwachungsmaßnahme nichts weiß und daher „keine Möglichkeit hat, in einem vorgeschalten Verfahren Einfluss auf das eingreifende Verhalten der Verwaltung zu nehmen“[115]. Da der Betroffene wegen der Heimlichkeit der Überwachungsmaßnahmen nicht unverzüglich vom derzeitigen Eingriff in seine Grundrechte erfährt, muss die gesetzliche Ermächtigung jedenfalls so hinreichend bestimmt sein, dass er erkennen kann, bei welchen Anlässen und unter welchen Voraussetzungen ein Risiko der Überwachung für ihn vorliegt[116].

Soweit die präventiv-polizeiliche Telekommunikationsüberwachung in einigen Bundesländern auch der Gefahrenabwehr im Vorfeld der Gefahr (Verhütung von Straftaten) dient[117], sind besondere Anforderungen an das

112 Vgl. BVerfGE 21, 73 (79 f.); 78, 214 (226); 113, 348 (376); *Sachs* (Fn. 110), § 40 Rn. 17; *Schmidt-Aßmann* (Fn. 101), Kapitel 4 Rn. 49; *Schulze-Fielitz* (Fn. 51), Art. 20 (Rechtsstaat) Rn. 136 ff.; *Sommermann* (Fn. 101), Art. 20 Rn. 289.

113 Vgl. BVerfGE 31, 255 (264); 110, 33 (54); 113, 348 (376 f.); *Sachs* (Fn. 101), Art. 20 Rn. 126; *Schulze-Fielitz* (Fn. 51), Art. 20 (Rechtsstaat) Rn. 133; *Sodan* (Fn. 101), Art. 20 Rn. 55; *Sommermann* (Fn. 101), Art. 20 Rn. 289.

114 BVerfGE 113, 348 (376); *Schulze-Fielitz* (Fn. 51), Art. 20 (Rechtsstaat) Rn. 136; *Son*, Heimliche polizeiliche Eingriffe, S. 240.

115 BVerfGE 113, 348 (376).

116 BVerfGE 113, 348 (376); *Puschke/Singelnstein*, NJW 2005, S. 3534 (3535).

117 Dazu siehe 3. Kapitel B.

Bestimmtheitsgebot zu beachten[118]. Die Gefahrenabwehr im Vorfeld stützt sich auf Anhaltspunkte der möglichen Begehung einer künftigen Straftat. Obwohl die Frage, ob Personen in Zukunft Straftaten begehen werden, noch sehr unklar ist, kann die Polizei durch die Telekommunikationsüberwachung den Sachverhalt aufklären und die Frage nach dem Aufkommen einer Gefahr beurteilen[119]. Bloß vage Anhaltspunkte entsprechen der hinreichenden Wahrscheinlichkeit des Schadenseintritts, die für die Telekommunikationsüberwachung zu fordern ist, jedoch nicht[120]. Darüber hinaus hat diese Vorverlagerung des polizeilichen Eingriffs auch zur Folge, dass sich das Risiko einer Fehlprognose erhöht. Aus diesem Grund sind die Anforderungen an die Bestimmtheit der Gesetze bei der Ermächtigung zur präventiv-polizeilichen Telekommunikationsüberwachung besonders zu beachten. Durch hinreichend bestimmte gesetzliche Ermächtigungsgrundlagen können verfassungsrechtliche Bedenken gegen das besonders hohe Risiko der Fehlprognose in gewissem Maße zerstreut werden. Deswegen stellt das Bestimmtheitsgebot keine Grenze für die präventive Telekommunikationsüberwachung dar[121]. Vielmehr verhält es sich gerade umgekehrt: Die Ungewissheit der Bedrohungslage im Vorfeld der Gefahr kann durch erhöhte Anforderungen an die Bestimmtheit der Ermächtigungsgrundlagen kompensiert werden.

In Bezug auf die Bedeutung des Bestimmtheitsgebots für die Prävention im Vorfeld der Gefahr steht das Bundesverfassungsgericht auf dem Standpunkt, dass das im Bereich der Vorfeldermittlung bestehende besonders hohe Risiko einer Fehlprognose durch die Beachtung des Bestimmtheitsgebots gleichwohl verfassungsrechtlich noch hinnehmbar sei[122]. Die Bedeutung des Bestimmtheitsgebots bestehe darin, dass die ausreichend be-

118 Vgl. BVerfGE 113, 348 (377 f.); *Puschke/Singelnstein* (Fn. 116), S. 3534 (3535 f.); *Trute*, Die Verwaltung 42 (2009), S. 85 (90 ff.).

119 Vgl. *Trute*, in: Erbguth/Müller/Neumann, GS Jeand'Heur, S. 403 (408). Es wird vertreten, dass die polizeiliche Vorfeldaktivität nur zulässig sei, wenn sie auf Grundlage einer hinreichend sicheren Faktenlage getroffen werde (so *Schenke* (Fn. 4), S. 1 (14)) oder auf einem erheblichen steigenden Wahrscheinlichkeitsgrad basiere (so *Roggan/Bergemann*, NJW 2007, S. 876 (877)). Folgt man dieser Ansicht, kann eine verfassungsmäßige polizeiliche Tätigkeit im Vorfeldbereich unmöglich werden. Denn gerade die noch unklare Tatsachenlage und die Erosion der Gefahrenschwelle stellen die Kennzeichnung des Gefahrenvorfeldes dar (vgl. *Trute*, in: Erbguth/Müller/Neumann, GS Jeand'Heur, S. 403 (406 ff.)). Begrifflich ist die polizeiliche Maßnahme, die auf einer hinreichend sicheren Faktenlage beruht, keine polizeiliche Tätigkeit im Vorfeld der Gefahren, sondern eine Maßnahme zur (klassischen) Gefahrenabwehr. Die Frage, ob die „Erosion der Gefahrenschwelle" besagt, dass die Person, deren E-Mail-Kommunikation im Vorfeld der Gefahr zu überwachen ist, als Störer im Sinne des Polizeirechts angesehen werden kann, wird im 6. Kapitel behandelt (dazu siehe 6. Kapitel A I 3 b)).

120 *Trute* (Fn. 119), S. 403 (407).

121 *Trute* (Fn. 118), S. 85 (91 ff.).

122 BVerfGE 113, 348 (377).

stimmte gesetzliche Ermächtigung zur verfassungsrechtlichen Hinnehmbarkeit des besonders hohen Risikos der Fehlprognose führe. Diese vom Bundesverfassungsgericht vertretene Auffassung überzeugt nur auf den ersten Blick. Bei näherer Betrachtung stellt sich jedoch heraus, dass sie problematisch ist, da sie die Funktion des Bestimmtheitsgebots mit der Funktion des Verhältnismäßigkeitsgrundsatzes vermengt[123]. Ob ein besonders hohes Risiko der Fehlprognose verfassungsrechtlich hingenommen werden kann, ist anhand des Verhältnismäßigkeitsgrundsatzes zu überprüfen. Im Unterschied dazu liegt die Bedeutung der Bestimmtheit darin, dass sie das Risiko einer exekutiven Fehlprognose reduziert[124]. Dies wiederum trägt dazu bei, dass eine solche Überwachungsmaßnahme die Prüfung der Verhältnismäßigkeit bestehen kann.

3. Bestimmtheit der polizei- und ordnungsgesetzlichen Ermächtigungsgrundlagen zur Telekommunikationsüberwachung

a) Urteil des Bundesverfassungsgerichts vom 27. 7. 2005

Das Bundesverfassungsgericht erklärte durch sein Urteil vom 27. 7. 2005[125] § 33a Abs. 1 Nr. 2 und 3 ndsSOG a. F. für nichtig. Einer der Gründe war, dass die genannten niedersächsischen Ermächtigungsvorschriften zur präventiv-polizeilichen Telekommunikationsüberwachung gegen die Bestimmtheitsanforderung verstießen[126]. Da das Bundesverfassungsgericht in diesem Urteil detailliert zeigte, warum die angegriffenen niedersächsischen Regelungen nicht mit dem rechtsstaatlichen Gebot der Normenbestimmtheit vereinbar waren, ist es ein Grundsatzurteil für die Frage der Verfassungsmäßigkeit der gesetzlichen Ermächtigungsgrundlagen zur präventivpolizeilichen Überwachung der Telekommunikation auch in anderen Bundesländern. In diesem Zusammenhang ist dieses Grundsatzurteil zunächst vorzustellen, bevor untersucht wird, ob die derzeitigen polizei- und ordnungsgesetzlichen Regelungen, durch die der Gesetzgeber (des Bundeslandes) der Polizei die Befugnis zur präventiven Telekommunikationsüberwachung gibt, den Anforderungen des Bestimmtheitsgebots entsprechen.

Gemäß § 33a Abs. 1 Nr. 2 ndsSOG a. F. konnte die Polizei durch eine Telekommunikationsüberwachung personenbezogene Daten erheben, soweit

123 Jedenfalls garantiert das Gebot der Bestimmtheit der Gesetze gegenüber dem Verhältnismäßigkeitsgrundsatz eine schlechtere Balance von Freiheit und Sicherheit *Trute* (Fn. 118), S. 85 (96)). Zwar haben das Bestimmtheitsgebot und der Verhältnismäßigkeitsgrundsatz unterschiedliche Funktionen bei der Prüfung der materiellen Verfassungsmäßigkeit eines Gesetzes, jedoch bedeutet dies nicht, dass das Bestimmtheitsdefizit des zu prüfenden Gesetzes keine Auswirkung auf die Verhältnismäßigkeitsprüfung hat (dazu siehe unten B II 2).

124 So zutreffend *Puschke/Singelnstein* (Fn. 116), S. 3534 (3535).

125 BVerfGE 113, 348 ff.

126 BVerfGE 113, 348 (375 ff.).

Tatsachen vorlagen, die die Annahme rechtfertigten, dass Personen Straftaten von erheblicher Bedeutung begehen werden. Hinsichtlich des persönlichen Tatbestandes können – wenn unerlässlich – auch Kontakt- und Begleitpersonen Überwachungsadressaten sein (§ 33a Abs. 1 Nr. 3 ndsSOG a. F.). Das Bundesverfassungsgericht rügte, dass diese gesetzliche Ermächtigung nicht mit dem Bestimmtheitsgebot in Einklang stehe[127]. Zwar verlange der niedersächsische Gesetzgeber, dass die präventiv-polizeiliche Telekommunikationsüberwachung einer richterlichen Anordnung bedürfe (§ 33a Abs. 3 ndsSOG a. F.), jedoch könnten die Bestimmtheitsdefizite dadurch nicht beseitigt werden[128].

Dem ersten Anschein nach führt die Verwendung des Begriffs der „Tatsache" dazu, dass bloße Vermutungen und allgemeine Erfahrungssätze nicht ausreichend für die Durchführung einer präventiv-polizeilichen Telekommunikationsüberwachung seien. Insoweit lässt sich der Begriff der „Tatsache" isoliert betrachtet als hinreichend bestimmt ansehen. Bei genauerer Überlegung genügt dieses Tatbestandsmerkmal in seiner Bezugnahme auf eine künftige Straftatenbegehung allerdings den Bestimmtheitsanforderungen nicht. Der Begriff der „Tatsache" bezieht sich auf einen hypothetischen Kausalverlauf, nach dem die Polizei eine zukünftig mögliche Straftatenbegehung aufklärt und verhindert. Jedoch wird die Frage, mit welchem Indikator und Wahrscheinlichkeitsgrad die Polizei erst festlegen könne, dass der potenzielle Täter in Zukunft diesen hypothetischen Kausalverlauf verwirklichen werde, nach Ansicht des Bundesverfassungsgerichts nicht vom niedersächsischen Gesetzgeber beantwortet. Dies habe zur Folge, dass der Zeitpunkt für die Durchführung einer präventiv-polizeilichen Telekommunikationsüberwachung völlig vom unvoraussehbaren Ermessen der Polizei abhänge[129]. Ferner lässt sich nach Ansicht des Bundesverfassungsgerichts ein Bestimmtheitsdefizit auch aus dem Begriff der „Straftat von erheblicher Bedeutung" herleiten. Der niedersächsische Gesetzgeber definiere den Begriff der „Straftat von erheblicher Bedeutung" einerseits in § 2 Nr. 10 ndsSOG a. F. durch eine Reihe von ausdrücklich aufgezählten Straftatbeständen. Andererseits sehe er zugleich ein Vergehen, das nach dem geschützten Rechtsgut und der Strafandrohung mit einem der bereits ausdrücklich in dieser Regelung genannten Straftatbestände vergleichbar sei, auch als eine Straftat von erheblicher Bedeutung an (§ 2 Nr. 10 Buchstabe b ndsSOG a. F.). Die Antwort auf die Frage, wie sich die Erheblichkeit der ungenannten Straftaten durch die sehr unscharfe Vergleichbarkeit ergebe, sei aber nicht deutlich[130]. Auch wenn man diese problematische zusätzliche Einbeziehung ignoriert, ist dem Bestimmtheitsgebot nicht genügt. Denn

127 BVerfGE 113, 348 (378 ff.).
128 BVerfGE 113, 348 (381).
129 BVerfGE 113, 348 (378 f.).
130 BVerfGE 113, 348 (379 f.).

durch den Begriff der „Straftat von erheblicher Bedeutung“ kann man nicht genau wissen, wann ein Verhalten auf die künftige Begehung solcher Straftaten hindeute[131].

Das obige Bestimmtheitsdefizit des § 33a Abs. 1 Nr. 2 ndsSOG a. F. führt nach Ansicht des Bundesverfassungsgerichts in der Folge auch zur Unbestimmtheit des § 33a Abs. 1 Nr. 3 ndsSOG a. F.[132]. Unter dem in § 33a Abs. 1 Nr. 3 ndsSOG a. F. verwendeten Begriff der „Kontakt- und Begleitperson“ versteht man aufgrund der Legaldefinition in § 2 Nr. 11 ndsSOG a. F. die Person, die mit einer anderen Person, von der Tatsachen die Annahme rechtfertigen, dass diese eine Straftat von erheblicher Bedeutung begehen wird, in einer Weise in Verbindung steht, die erwarten lässt, dass durch sie Hinweise auf die angenommene Straftat gewonnen werden können. Ausgehend davon knüpft der Begriff der „Kontakt- und Begleitperson“, die auch Adressaten präventiv-polizeilicher Telekommunikationsüberwachung sein können, an den potenziellen Straftäter, der in Zukunft eine mögliche Straftat von erheblicher Bedeutung begehen wird, an. Da die Frage, wer der potenzielle Straftäter ist, wegen der dargelegten Unbestimmtheit in § 33a Abs. 1 Nr. 2 ndsSOG a. F. nicht eindeutig beantwortet werden kann, lässt sich auch sehr schwer feststellen, wer dem Begriff der „Kontakt- und Begleitperson“ in § 33a Abs. 1 Nr. 3 ndsSOG a. F. entspricht[133]. Dies hat nach Meinung des Bundesverfassungsgerichts zur Konsequenz, dass es an einem handhabbaren Maßstab für die Prüfung der Unerlässlichkeit, die in § 33a Abs. 1 Nr. 3 ndsSOG a. F. gefordert wurde, fehle. Der Versuch, den Begriff der „Kontakt- und Begleitperson“ durch eine nähere Qualifizierung des Kontakts zwischen dem Straftäter und der anderen Person zu konkretisieren und damit restriktiv auszulegen, ist zudem nicht zielführend. Denn ein solcher Versuch basiert auf dem Gedanken, dass eine unbestimmte Eingriffsermächtigung durch die Auslegung der Polizei, deren Tätigkeit gerade begrenzt werden solle, in freiheitsschützender Weise eingeengt werden könne. Dies ist jedoch, wie das Bundesverfassungsgericht hervorhebt, aus rechtsstaatlicher Sicht fragwürdig[134].

b) Novellierung des ndsSOG als gesetzgeberische Reaktion auf das Urteil des Bundesverfassungsgerichts

Angesichts der Bestimmtheitsdefizite in § 33a Abs. 1 Nr. 2 und 3 ndsSOG a. F., die das Bundesverfassungsgericht durch obiges Urteil rügte, änderte der Gesetzgeber das ndsSOG. Nach § 33a Abs. 1 ndsSOG n. F. darf die präventiv-polizeiliche Telekommunikationsüberwachung nunmehr nur der Abwehr einer gegenwärtigen Gefahr dienen. Die Durchführung einer prä-

131 BVerfGE 113, 348 (379).
132 BVerfGE 113, 348 (380 f.).
133 BVerfGE 113, 348 (380).
134 BVerfGE 113, 348 (381).

ventiv-polizeilichen Telekommunikationsüberwachung im Vorfeld der Gefahr ist nun in Niedersachsen nicht mehr zulässig. Der niedersächsische Gesetzgeber verzichtet in § 33a ndsSOG n. F. darauf, den Begriff der „Tatsache", der Grundlage für einen hypothetischen Kausalverlauf der zukünftigen Straftatenbegehung ist, zu verwenden. Auch der zu vage bleibende Begriff der „Kontakt- und Begleitperson", der an potenzielle Straftäter anknüpft, wurde in § 33a Abs. 1 ndsSOG n. F. gestrichen. Da sich der Adressatenbereich präventiv-polizeilicher Telekommunikationsüberwachung deutlich auf die in §§ 6, 7 und 8 ndsSOG genannten Personen (Störer und Nichtstörer im Sinne des klassischen Gefahrenabwehrrechts) begrenzt[135], kann der Bürger voraussehen, ob ein Überwachungsrisiko für sein Telekommunikationsverhalten vorliegt.

Grundsätzlich lässt sich feststellen, dass die Novellierung des ndsSOG eine gelungene Reaktion auf das Urteil des Bundesverfassungsgerichts darstellt. Unbefriedigend ist jedoch, dass sich diese Novelle nur auf § 33a ndsSOG n. F. beschränkt. Die polizeiliche Befugnis der Informationserhebung zur Straftatenverhütung nach § 31 Abs. 2 ndsSOG n. F. wurde nicht aufgehoben. Personen, bei denen Tatsachen die Annahme rechtfertigen, dass sie künftig Straftaten begehen werden, können Adressat der polizeilichen Informationserhebung sein. In § 31 Abs. 2 Nr. 1 ndsSOG n. F. fehlen jedoch bestimmte Vorgaben über die Indikatoren und den Wahrscheinlichkeitsgrad dieses hypothetischen Kausalverlaufs. Deswegen ist der Kreis der in § 31 Abs. 2 Nr. 1 ndsSOG genannten potenziellen Straftäter unbestimmt. Darüber hinaus wird der Begriff der Kontakt- oder Begleitperson in § 31 Abs. 2 Nr. 2 ndsSOG n. F. verwendet. Obwohl der niedersächsische Gesetzgeber durch § 2 Nr. 12 ndsSOG n. F. die Qualifizierung des Kontakts näher konkretisiert, setzt die Festlegung der Kontakt- oder Begleitperson immer voraus, dass der Kontaktadressat, also der potenzielle Straftäter, bestimmt werden kann. Wegen der in § 31 Abs. 2 Nr. 1 ndsSOG n. F. bestehenden Unbestimmtheit dürfte diese Festlegung schwerlich möglich sein. Aus diesem Grund sind die verfassungsrechtlichen Bedenken gegen die Bestimmtheit der § 31 Abs. 2 ndsSOG n. F. nicht beseitigt. Jedoch ist zu beachten, dass die Bestimmtheitsdefizite in § 31 Abs. 2 ndsSOG n. F. nicht zur Unbestimmtheit der Rechtsgrundlage der präventiv-polizeilichen Telekommunikationsüberwachung in Niedersachsen führen. Denn § 33a ndsSOG, der eine Spezialermächtigung zur Informationserhebung (Telekommunikationsüberwachung) darstellt, besitzt einen Anwendungsvorrang und eine Sperrwirkung für den als die Generalklausel der Informationserhebung betrachteten[136] § 31 ndsSOG n. F. Bei der Durchführung einer präventiv-polizeilichen Telekommunikationsüberwachung kann die gesetzliche Grund-

135 § 33a Abs. 1 Nr. 1 und 2 ndsSOG n. F.
136 *Schenke* (Fn. 25), Rn. 181 mit Fn. 444.

lage nur § 33a ndsSOG n. F. sein. Ein Rückgriff auf § 31 ndsSOG ist unzulässig.

c) Bestimmtheit der polizei- und ordnungsgesetzlichen Ermächtigungsvorschriften zur Telekommunikationsüberwachung in anderen Bundesländern

Nach der Erörterung der durch das bundesverfassungsgerichtliche Urteil vom 27. 7. 2005 entwickelten Kriterien für die Bestimmtheit der Gesetze ist im Folgenden zu untersuchen, ob die polizei- und ordnungsgesetzlichen Ermächtigungsvorschriften zur Telekommunikationsüberwachung in anderen Bundesländern dem rechtsstaatlichen Bestimmtheitsgebot entsprechen.

aa) Bestimmtheit der baden-württembergischen Ermächtigungsvorschrift

Gemäß § 23a Abs. 1 Satz 1 Nr. 1 bwPolG kann die Polizei verdeckt Verkehrsdaten der Telekommunikation erheben, soweit dies zur Abwehr einer unmittelbar bevorstehenden Gefahr für den Bestand oder die Sicherheit des Bundes oder eines Landes oder für Leben, Gesundheit oder Freiheit einer Person erforderlich ist. Diese Vorschrift regelt deutlich, dass sich Adressaten der präventiv-polizeilichen Telekommunikationsüberwachung auf Störer im Sinne des Polizeirechts (§§ 6 und 7 bwPolG) beschränken. Wenn ein polizeilicher Notstand besteht, kann die Polizei die Telekommunikation eines Nichtstörers (§ 9 bwPolG) überwachen. Da die sachlichen und persönlichen Tatbestände hinreichend bestimmt sind, steht die Ermächtigungsvorschrift zur präventiv-polizeilichen Telekommunikationsüberwachung im Bereich der klassischen Gefahrenabwehr mit dem Gebot der Bestimmtheit in Einklang.

Der baden-württembergische Gesetzgeber erlaubt auch die präventiv-polizeiliche Telekommunikationsüberwachung im Vorfeld der Gefahr. Nach § 23a Abs. 1 Satz 1 Nr. 2 Buchstabe a bwPolG kann sich die Maßnahme präventiv-polizeilicher Telekommunikationsüberwachung gegen Personen richten, wenn konkrete Planungen oder Vorbereitungshandlungen für sich oder zusammen mit weiteren Tatsachen die Annahme rechtfertigen, dass sie schwerwiegende Straftaten begehen werden. Die Anwendung des Begriffs „Tatsache“ muss auf einer „konkreten Planung oder Vorbereitungshandlung“ basieren. Diese Indikatoren des hypothetischen Kausalverlaufs tragen zur Bestimmtheit des § 23a Abs. 1 Satz 1 Nr. 2 Buchstabe a bwPolG bei. Zeitlich darf die Polizei im Vorfeld der Gefahr eine Maßnahme der Telekommunikationsüberwachung nur ergreifen, wenn eine konkrete Planung oder Vorbereitungshandlung bezüglich einer schwerwiegenden Straftat vorliegt. Insoweit stellt das Bestehen einer konkreten Planung oder Vorbereitungshandlung die zeitliche Schwelle für den polizeilichen Zugriff auf die Telekommunikation dar. Zudem definiert der baden-württembergische

Gesetzgeber durch § 23a Abs. 2 bwPolG ausdrücklich den Begriff der „schwerwiegenden Straftaten". Deswegen ist § 23a Abs. 1 Satz 1 Nr. 2 Buchstabe a bwPolG mit dem Bestimmtheitsgebot vereinbar.

Nach § 23a Abs. 1 Satz 1 Nr. 2 Buchstabe b und c bwPolG kann die Polizei die Telekommunikation der Kontakt- und Begleitpersonen überwachen, wenn Tatsachen die Annahme rechtfertigen, dass sie in die Planung oder Vorbereitung von schwerwiegenden Straftaten eines in § 23a Abs. 1 Satz 1 Nr. 2 Buchstabe a bwPolG genannten potenziellen Straftäters ganz oder teilweise eingeweiht sind oder wenn Tatsachen die Annahme rechtfertigen, dass sie (Kontakt- und Begleitpersonen) Mitteilungen entgegennehmen, die für einen potenziellen Straftäter oder eine Kontakt- und Begleitperson bestimmt sind oder von ihr herrühren, oder dass ihre Kommunikationseinrichtung von einer solchen Person benutzt wird. Die baden-württembergische Ermächtigungsvorschrift zur präventiv-polizeilichen Telekommunikationsüberwachung von Kontakt- und Begleitpersonen erfüllt die rechtsstaatlichen Anforderungen an die Bestimmtheit. Denn in § 23a Abs. 1 Satz 1 Nr. 2 Buchstabe b und c bwPolG werden bestimmte Indikatoren (Kontakttätigkeiten) genannt. Liegt eine dieser Kontakttätigkeiten vor, kann die Polizeibehörde die Telekommunikation der Kontakt- und Begleitpersonen überwachen. Deswegen ist die zeitliche Schwelle für die Durchführung einer präventiv-polizeilichen Telekommunikation hinreichend bestimmt. Die Bestimmtheit des § 23a Abs. 1 Satz 1 Nr. 2 Buchstabe b und c bwPolG ist damit zu bejahen.

bb) Bestimmtheit der bayerischen Ermächtigungsvorschrift

Der bayerische Gesetzgeber ermächtigt durch Art. 34a Abs. 1 Satz 1 Nr. 1 bayPAG die Polizei dazu, die präventive Telekommunikationsüberwachung durchzuführen, soweit dies zur Abwehr einer dringenden Gefahr für den Bestand oder die Sicherheit des Bundes oder eines Landes oder für Leib, Leben oder Freiheit einer Person oder für Sachen, soweit eine gemeine Gefahr besteht, erforderlich ist. Adressaten polizeilicher Maßnahmen nach Art. 34a Abs. 1 Satz 1 Nr. 1 bayPAG sind die für eine Gefahr Verantwortlichen. Jedoch fragt sich, ob die Verwendung des Begriffs der „dringenden Gefahr" in Art. 34a Abs. 1 Satz 1 Nr. 1 bayPAG vereinbar mit dem rechtsstaatlichen Gebot der Bestimmtheit ist. Die Frage, welche Gefährdungslage einer dringenden Gefahr entspricht, wird in der Literatur nicht einheitlich beantwortet. Nach der (wohl herrschenden) Meinung besagt die dringende Gefahr eine Gefährdung eines bedeutsamen Rechtsguts[137]. Dagegen bedeutet die dringende Gefahr nach anderer Auffassung aus der Sicht der zeitli-

137 *Käß*, BayVBl. 2008, S. 225 (228 f.); *Götz* (Fn. 1), § 6 Rn. 27; *Hermes*, in: Dreier, GG, Bd. 1, Art. 13 Rn. 115; *Jarass* (Fn. 51), Art. 13 Rn. 37; *Knemeyer* (Fn. 57), Rn. 94; *Kugelmann* (Fn. 75), 4. Kapitel Rn. 135; *Kunig*, in: von Münch/Kunig, GG, Bd. 1, Art. 13 Rn. 67; *Rachor* (Fn. 96), F Rn. 711; *Schoch* (Fn. 53), Rn. 100; *Sodan* (Fn. 101), Art. 13 Rn. 15.

chen Dringlichkeit eine erhöhte Wahrscheinlichkeit des Schadenseintritts[138]. Folgt man der dritten Ansicht, stellt die dringende Gefahr sowohl eine Gefährdung eines hochrangigen Rechtsguts als auch eine zeitliche Nähe des Schadenseintritts dar[139]. Trotz dieses in der Literatur bestehenden Meinungsstreits, der sich aus der Unklarheit des Wortlauts der dringenden Gefahr ergibt, kann das Fazit, dass Art. 34a Abs. 1 Satz 1 Nr. 1 bayPAG wegen Verletzung des Bestimmtheitsgebots verfassungswidrig ist, nicht gezogen werden. Denn nur eine der oben genannten Auffassungen ist überzeugend für die Auslegung des Begriffs der dringenden Gefahr in Art. 34a Abs. 1 Satz 1 Nr. 1 bayPAG: Die in Art. 34a Abs. 1 Satz 1 Nr. 1 bayPAG vorgeschriebene dringende Gefahr ist unter dem Aspekt der zeitlichen Dringlichkeit auszulegen. Da in Art. 34a Abs. 1 Satz 1 Nr. 1 bayPAG bereits eine Aufzählung der bedeutsamen Rechtsgüter[140] vorliegt, besagt die dringende Gefahr in Art. 34a Abs. 1 Satz 1 Nr. 1 bayPAG nicht die Gefährdung wichtiger Rechtsgüter; denn sonst ist der Begriff der dringenden Gefahr in dieser Vorschrift nicht konsequent verwendet. Durch diese Klarstellung können die Bedenken hinsichtlich des Bestimmtheitsdefizits des Begriffs der dringenden Gefahr beseitigt werden.

Nach Art. 34a Abs. 1 Satz 1 Nr. 2 bayPAG kann die Polizei im Vorfeld der Gefahr eine Telekommunikationsüberwachung durchführen, soweit konkrete Vorbereitungshandlungen für sich oder zusammen mit weiteren bestimmten Tatsachen die begründete Annahme rechtfertigen, dass Personen eine schwerwiegende Straftat begehen werden. Die Anwendung des Begriffs „Tatsache“ basiert – wie im Fall des § 23a Abs. 1 Satz 1 Nr. 2 Buchstabe a bwPolG – auf einer „konkreten Vorbereitungshandlung“. Ohne Bestehen einer konkreten Vorbereitungshandlung der schwerwiegenden Straftaten darf die Polizei nicht im Vorfeld der Gefahr eine Maßnahme der Telekommunikationsüberwachung ergreifen. In diesem Punkt lässt sich „konkrete Vorbereitungshandlung“ als ein (hinreichend bestimmtes) handlungsbegrenzendes Tatbestandselement ansehen[141]. Außerdem gibt es in Art. 30 Abs. 5 Satz 1 bayPAG eine hinreichend bestimmte Legaldefinition der schwerwiegenden Straftat. Insoweit lässt sich festhalten, dass Art. 34a Abs. 1 Satz 1 Nr. 2 bayPAG hinreichend bestimmt ist.

Gemäß Art. 34a Abs. 1 Satz 1 Nr. 3 bayPAG können Kontakt- und Begleitpersonen Adressaten präventiv-polizeilicher Telekommunikationsüberwachung sein, soweit bestimmte Tatsachen die begründete Annahme recht-

138 *Gornig*, in: von Mangoldt/Klein/Starck, GG, Bd. 1, Art. 13 Rn. 127; *Gusy* (Fn. 55), Rn. 128; *Schenke* (Fn. 25), Rn. 78 mit Fn. 135; *Stern*, in: Stern, Staatsrecht, Bd. IV/1, S. 278.

139 *Denninger*, in: Lisken/Denninger, HPolR, E Rn. 63; dazu *Götz* (Fn. 1), § 6 Rn. 27; *Pieroth/Schlink/Kniesel* (Fn. 52), § 4 Rn. 19.

140 Der Bestand oder die Sicherheit des Bundes oder eines Landes oder der Leib, das Leben oder die Freiheit einer Person oder der Bestand der Sachen, soweit eine gemeine Gefahr besteht.

141 *Sievers* (Fn. 99), S. 88.

fertigen, dass sie für den in Art. 34a Abs. 1 Satz 1 Nr. 2 bayPAG genannten potenziellen Straftäter bestimmte oder von diesen herrührende Mitteilungen entgegennehmen, ohne insoweit das Recht zur Verweigerung des Zeugnisses nach §§ 53, 53a StPO zu haben, oder weitergeben oder die in Art. 34a Abs. 1 Satz 1 Nr. 2 bayPAG genannten potenziellen Straftäter ihre Kommunikationseinrichtungen benutzen werden. Da der bayerische Gesetzgeber in Art. 34a Abs. 1 Satz 1 Nr. 3 bayPAG das Kontaktverhalten der Kontakt- und Begleitpersonen deutlich auf die Entgegennahme von Mitteilungen oder die Benutzung der Kommunikationseinrichtungen beschränkt, sind der Kreis der Kontakt- und Begleitpersonen und die zeitliche Eingriffsschwelle deutlich bestimmt. Insoweit entspricht Art. 34a Abs. 1 Satz 1 Nr. 3 bayPAG dem Bestimmtheitsgebot.

cc) Bestimmtheit der brandenburgischen Ermächtigungsvorschrift

Mit § 33b Abs. 1 in Verbindung mit § 33a Abs. 1 Nr. 1 bbgPolG gibt der brandenburgischen Gesetzgeber der Polizei die Befugnis, die präventive Telekommunikationsüberwachung durchzuführen, soweit dies zur Abwehr einer dringenden Gefahr für Leib, Leben oder Freiheit einer Person unerlässlich ist. Hinsichtlich der Richtung der Maßnahme regelt § 33b Abs. 2 S. 1 bbgPolG deutlich, dass sowohl Störer wie auch Nichtstörer Adressaten des Eingriffs sein können. In Bezug auf die sachlichen Voraussetzungen verwendet der brandenburgische Gesetzgeber den Begriff der „dringenden Gefahr", dessen Bedeutung umstritten ist. Da § 33a Abs. 1 Nr. 1 bbgPolG die gewichtigen Rechtsgüter aufzählt[142], ist festzustellen, dass der Begriff der dringenden Gefahr nur die zeitliche Nähe zur Schädigung bedeuten kann[143]. Die Verwendung des Begriffs der dringenden Gefahr führt nicht zu einer Verletzung des Bestimmtheitsgebots.

Nach § 33b Abs. 1 und Abs. 2 Satz 2 in Verbindung mit § 33a Abs. 1 Nr. 2 bbgPolG kann eine präventiv-polizeiliche Telekommunikationsüberwachung auch im Vorfeld der Gefahr durchgeführt werden, wenn bestimmte Tatsachen die Annahme rechtfertigen, dass aufgrund tatsächlicher Anhaltspunkte, insbesondere aufgrund konkreter Informationen über Planungs- und Vorbereitungshandlungen, anzunehmen ist, dass die in § 33a Abs. 1 Nr. 2 Buchstaben a bis g bbgPolG genannten Straftaten organisiert begangen werden sollen, die drohende Rechtsgutsverletzung auch im Einzelfall schwer wiegt und die Datenerhebung zur Abwehr der mit diesen Straftaten verbundenen dringenden Gefahr erforderlich ist. Diese Ermächtigungsregelung erfüllt das rechtstaatliche Bestimmtheitsgebot nicht. Zwar ist der in § 33a Abs. 1 Nr. 2 bbgPolG geregelte Tatestand „konkrete Informationen über Planungs- und Vorbereitungshandlungen" ausreichend bestimmt, jedoch wird er nur als ein Beispiel für die „tatsächlichen Anhaltspunkte"

142 Der Leib, das Leben oder die Freiheit einer Person.

143 Siehe dazu die obigen Ausführungen zu Art. 34a Abs. 1 S. 1 Nr. 1 bayPAG.

angesehen[144]. Dies hat zur Folge, dass die Polizei ohne gesetzlich vorgegebene Kriterien beurteilen muss, ob ein tatsächlicher Anhaltspunkt für mögliche Straftaten vorliegt.

Ferner ist der Begriff der Kontakt- und Begleitpersonen (§ 33b Abs. 2 Satz 2 in Verbindung mit § 33a Abs. 2 Satz 3 bis 5 bbgPolG), die die Adressaten der präventiv-polizeilichen Telekommunikationsüberwachung darstellen können, nicht hinreichend bestimmt. Denn die Frage, wer als potenzieller Straftäter (= Kontaktadressat) in Betracht kommt, kann, wie bereits dargelegt wurde, nicht bestimmt beantwortet werden. Die brandenburgischen Ermächtigungsvorschriften zur präventiv-polizeilichen Telekommunikationsüberwachung im Vorfeld der Gefahr stehen also nicht mit dem rechtsstaatlichen Bestimmtheitsgebot in Einklang.

dd) Bestimmtheit der hamburgischen Ermächtigungsvorschrift

In Hamburg kann die Polizei zur erforderlichern Abwehr einer unmittelbar bevorstehenden Gefahr für Leib, Leben oder Freiheit einer Person eine präventive Telekommunikationsüberwachung durchführen (§ 10a Abs. 1 Satz 1 hambGDatPol). Eine Maßnahme der präventiv-polizeilichen Telekommunikationsüberwachung, die im Vorfeld der Gefahr ergriffen wird, ist unzulässig. Adressaten der präventiv-polizeilichen Telekommunikationsüberwachung sind nicht nur die für die Gefahr Verantwortlichen (Störer), sondern auch die in § 10 hambSOG genannt Personen (Nichtstörer). Da es in §§ 8–10 hambSOG eine ausreichend bestimmte Legaldefinition für die Adressaten der präventiv-polizeilichen Telekommunikationsüberwachung (Störer und Nichtstörer) gibt[145], können die Voraussetzungen präventiv-polizeilicher Telekommunikationsüberwachung in § 10a Abs. 1 Satz 1 hambGDatPol die Prüfung der Bestimmtheitsanforderungen bestehen.

ee) Bestimmtheit der hessischen Ermächtigungsvorschrift

Gemäß § 15a Abs. 1 hessSOG kann die präventiv-polizeiliche Telekommunikationsüberwachung nur der Abwehr einer gegenwärtigen Gefahr für Leib, Leben oder Freiheit einer Person dienen. Eine polizeiliche Befugnis zur im Vorfeld der Gefahr durchgeführten präventiven Telekommunikationsüberwachung wird nicht eingeräumt. In Bezug auf materiellrechtliche Voraussetzungen ist unstreitig, dass der Begriff der gegenwärtigen Gefahr die zeitliche Nähe und damit eine Steigerung der Schadenseintrittswahrscheinlichkeit beschreibt[146]. Hinsichtlich des persönlichen Tatbestands

144 Vgl. *Sievers* (Fn. 99), S. 100.

145 Gemäß § 1 Abs. 1 S. 1 hambGDatPol findet dieses Gesetz Anwendung, soweit die Polizei zur Erfüllung ihrer Aufgaben nach hambSOG Daten verarbeitet. Grundlage für die Festlegung der in 10a Abs. 1 S. 1 hambGDatPol genannten Adressaten ist deswegen die einschlägige Legaldefinition im hambSOG.

146 Vgl. *Denninger* (Fn. 139), E Rn. 53; *Götz* (Fn. 1), § 6 Rn. 25; *Gusy* (Fn. 55), Rn. 130; *Knemeyer* (Fn. 57), Rn. 94; *Kugelmann* (Fn. 75), 4. Kapitel Rn. 133; *Pieroth/Schlink/Kniesel* (Fn. 52),

regelt § 15a Abs. 1 hessSOG zwar keine Adressaten der Beobachtung, jedoch führt dies nicht zu einem Bestimmtheitsdefizit[147]. Mangels einer Regelung über den Kreis der Adressaten in § 15a Abs. 1 hessSOG sind die Vorschriften der allgemeinen Verantwortlichkeit (§§ 6, 7 und 9 hessSOG) zu berücksichtigen und anzuwenden[148]. § 9 hessSOG regelt, dass sich der polizeiliche Eingriff gegen den Nichtstörer richten kann, wenn ein polizeilicher Notstand vorliegt[149]. Insoweit können nicht nur Störer, sondern auch Nichtstörer die Adressaten der präventiv-polizeilichen Telekommunikationsüberwachung sein, soweit die Voraussetzungen des § 9 hessSOG erfüllt sind. Da diese Konsequenz vorhersehbar ist, verletzt § 15a Abs. 1 hessSOG das Bestimmtheitsgebot nicht.

ff) Bestimmtheit der mecklenburg-vorpommerischen Ermächtigungsvorschrift

Nach § 34a Abs. 1 Satz 1 mvSOG kann die Polizei eine präventive Telekommunikationsüberwachung durchführen, um eine im Einzelfall bevorstehende Gefahr für Leib, Leben oder Freiheit einer Person abzuwehren oder den Bestand oder die Sicherheit des Bundes oder eines Landes zu gewährleisten. Die präventiv-polizeiliche Telekommunikationsüberwachung zur Verhütung künftiger Straftaten ist nicht zulässig. In § 3 Abs. 3 Nr. 1 mvSOG gibt es eine hinreichend bestimmte Legaldefinition der im Einzelfall bevorstehenden Gefahr. Zu den Adressaten präventiv-polizeilicher Telekommunikationsüberwachung gehören die für eine Gefahr Verantwortlichen (§ 34a Abs. 1 Satz 1 Nr. 1 mvSOG) und die Personen, deren Leben oder Gesundheit gefährdet ist (§ 34a Abs. 1 S. 1 Nr. 2 mvSOG). Dadurch ist vorhersehbar, wer unter welchen Voraussetzungen die betroffene Person präventiv-polizeilicher Telekommunikationsüberwachung darstellt. Aufgrund seiner hinreichend bestimmten Tatbestände ist § 34a Abs. 1 mvSOG mit dem rechtsstaatlichen Bestimmtheitsgebot vereinbar.

gg) Bestimmtheit der rheinland-pfälzischen Ermächtigungsvorschrift

Durch § 31 Abs. 1 rpPOG ermächtigt der rheinland-pfälzische Gesetzgeber die Polizei dazu, eine präventive Telekommunikationsüberwachung zur Abwehr einer gegenwärtigen Gefahr für Leib oder Leben einer Person durchzuführen. Unzulässig ist die präventive Telekommunikationsüberwachung im Vorfeld einer Gefahr. Obwohl es im rpPOG keine Legaldefinition der gegenwärtigen Gefahr gibt, versteht man unter diesem Begriff eine

§ 4 Rn. 19; *Schenke* (Fn. 25), Rn. 78; *Schoch* (Fn. 53), Rn. 100; *Tettinger/Erbguth/Mann* (Fn. 64), Rn. 469; *Würtenberger/Heckmann* (Fn. 52), Rn. 415.

147 A. A. *Graulich*, NVwZ 2005, S. 271 (273).

148 *Schäfer*, Präventive Telekommunikationsüberwachung, S. 117; *Schenke* (Fn. 25), Rn. 197c.

149 *Götz* (Fn. 1), § 10 Rn. 1 ff.; *Gusy* (Fn. 55), Rn. 380 ff.; *Kugelmann* (Fn. 75), 6. Kapitel Rn. 81 ff.; *Pieroth/Schlink/Kniesel* (Fn. 52), § 9 Rn. 74; *Schenke* (Fn. 25), Rn. 312; *Schoch* (Fn. 53), Rn. 177 ff.

besondere zeitliche Nähe der Gefahrenrealisierung[150]. Die Adressaten der präventiv-polizeilichen Telekommunikationsüberwachung in § 31 rpPOG sind sowohl die in §§ 4 und 5 rpPOG genannte Verantwortlichen (Störer) wie auch die in § 7 genannten Personen (Nichtstörer). Durch diese bestimmten Tatbestände kann ein Bürger voraussehen, ob ein Risiko der präventiv-polizeilichen Telekommunikationsüberwachung für ihn vorliegt. Die Bestimmtheit des § 31 Abs. 1 rpPOG ist zu bejahen.

hh) Bestimmtheit der saarländischen Ermächtigungsvorschrift

Gemäß § 28b Abs. 1 S. 1 Nr. 1 saarlPolG kann die Polizei zur Abwehr einer gegenwärtigen Gefahr für Leib, Leben oder Freiheit einer Person eine präventive Telekommunikationsüberwachung durchführen. In Bezug auf die Richtung der Maßnahme regelt diese Vorschrift explizit, dass sowohl Störer (§§ 4 und 5 saarlPolG) als auch Nichtstörer (§ 6 saarlPolG) die Adressaten polizeilicher Telekommunikationsüberwachung zur Gefahrenabwehr sein können. Unter dem in § 28b Abs. 1 Satz 1 Nr. 1 saarlPolG verwendeten Begriff der gegenwärtigen Gefahr versteht man unstreitig die zeitliche Nähe des Schadenseintritts[151]. Insoweit ist § 28b Abs. 1 Satz 1 Nr. 1 saarlPolG hinreichend bestimmt.

Nach § 28b Abs. 1 Satz 1 Nr. 2 saarlPolG kann die präventiv-polizeiliche Telekommunikationsüberwachung auch im Vorfeld der Gefahr durchgeführt werden. Die Adressaten der durch diese Vorschrift vorgesehenen präventiv-polizeilichen Telekommunikationsüberwachung beschränken sich auf die potenziellen Straftäter, die die in § 100c StPO genannten Straftaten zukünftig begehen werden. Die Anwendung des in § 28b Abs. 1 Satz 1 Nr. 2 saarlPolG verwendeten Begriffs „Tatsache" basiert – wie in Art. 34a Abs. 1 Satz 1 Nr. 2 bayPAG – auf konkreten Vorbereitungshandlungen. Zeitlich darf die präventiv-polizeiliche Telekommunikationsüberwachung im Vorfeld der Gefahr nur durchgeführt werden, wenn eine konkrete Vorbereitungshandlung vorliegt. In diesem Zusammenhang stellt diese Vorschrift keine Blankettermächtigung dar. Die rechtsstaatlichen Anforderungen an die Bestimmtheit werden damit erfüllt.

ii) Bestimmtheit der schleswig-holsteinischen Ermächtigungsvorschrift

Gemäß § 185a Abs. 1 shLVwG kann eine präventiv-polizeiliche Telekommunikationsüberwachung zur Abwehr einer gegenwärtigen Gefahr für Leib, Leben oder Freiheit einer Person durchgeführt werden, wenn dieses zur Aufklärung des Sachverhalts unerlässlich ist. Diese Vorschrift erfüllt die Anforderungen an das Gebot rechtsstaatlicher Bestimmtheit. Wie bereits dargelegt wurde, besagt der hier verwendete Begriff der gegenwärtigen

150 Vgl. oben Fn. 146.
151 Vgl. oben Fn. 146.

Gefahr eine zeitliche Nähe des Schadenseintritts[152]. Nach § 185a Abs. 1 Satz 2 in Verbindung mit § 185 Abs. 2 Satz 2 shLVwG beschränkt sich der Adressatenkreis der präventiv-polizeilichen Telekommunikationsüberwachung deutlich auf Störer. § 185a Abs. 1 shLVwG ist damit eine hinreichend bestimmte Ermächtigungsregelung.

jj) Bestimmtheit der thüringischen Ermächtigungsvorschrift

Nach § 34a Abs. 1 Satz 1 Nr. 1 thürPAG a. F. konnte die Polizei durch die Mitwirkung der Diensteanbieter eine präventiv-polizeiliche Telekommunikationsüberwachung durchführen, soweit Tatsachen die Annahme rechtfertigten, dass Personen Straftaten im Sinne des § 100a StPO begehen wollten. Zu den Adressaten des Eingriffs gehörten auch Kontakt- oder Begleitpersonen (§ 34a Abs. 1 Satz 1 Nr. 1 thürPAG a. F.). Aufgrund ihres Bestimmtheitsdefizits stieß diese Vorschrift auf heftige Kritik[153]. Durch Art. 1 des Gesetzes zur Änderung sicherheits- und verfassungsschutzrechtlicher Vorschriften vom 16. 7. 2008[154] novellierte der thüringische Gesetzgeber § 34a thürPAG. Ob diese Novellierung die Bedenken gegen die Bestimmtheit des § 34a thürPAG völlig beseitigt, ist jedoch fraglich. Gemäß § 34a Abs. 1 und 2 thürPAG n. F. kann die Polizei unter Mitwirkung eines Diensteanbieters oder mit Hilfe von eigenen technischen Erfassungsanlagen die Telekommunikation überwachen. Die Maßnahme präventiv-polizeilicher Telekommunikationsüberwachung ist zunächst an den Störer adressiert, soweit dies zur Abwehr einer dringenden Gefahr für den Bestand oder die Sicherheit des Bundes oder eines Landes oder für Leib, Leben oder Freiheit einer Person oder für Sachen, soweit eine gemeine Gefahr besteht, zwingend erforderlich ist (§ 34a Abs. 3 Satz 1 Nr. 1 thürPAG n. F.). Wie bereits dargelegt wurde[155], steht die Verwendung des Begriffs der dringenden Gefahr, der in § 34a Abs. 3 Satz 1 Nr. 1 thürPAG n. F. die zeitliche Nähe der Schädigung meint, in Einklang mit dem Bestimmtheitsgebot. Zudem kann die präventiv-polizeiliche Telekommunikationsüberwachung auch im Vorfeld der Gefahr durchgeführt werden, soweit konkrete Planungs- und Vorbereitungshandlungen für sich oder zusammen mit weiteren bestimmten Tatsachen die begründete Annahme rechtfertigen, dass eine Straftat im Sinne des § 31 Abs. 5 thürPAG (besonders schwere Straftat) begangen werden soll (§ 34a Abs. 3 Satz 1 Nr. 2 thürPAG). § 34a Abs. 3 Satz 1 Nr. 2 thürPAG n. F. ist zu entnehmen, dass der Begriff der „Tatsache“[156] auf einer konkreten Planungs- und Vorbereitungshandlung basieren muss. Dies bedeutet,

152 Vgl. oben Fn. 146.

153 Vgl. *Sievers* (Fn. 99), S. 90 f.

154 GVBl. S. 245.

155 Vgl. oben bb).

156 In § 34a Abs. 3 S. 1 Nr. 2 Buchstaben a bis g thürPAG werden Beispiele für das Tatbestandselement „Tatsache“ genannt.

dass die präventiv-polizeiliche Telekommunikationsüberwachung im Vorfeld der Gefahr nur durchgeführt werden kann, wenn eine konkrete Planungs- und Vorbereitungshandlung vorliegt. Da der Zeitpunkt des Eingriffs im Anwendungsbereich des § 34a Abs. 3 Satz 1 Nr. 2 thürPAG n. F. vorhersehbar ist, ist das Bestimmtheitsgebot nicht verletzt.

Ferner können die Kontakt- und Begleitpersonen Adressaten der präventiv-polizeilichen Telekommunikationsüberwachung sein, soweit Tatsachen die Annahme rechtfertigen, dass sie für die in § 34a Abs. 3 Satz 1 Nr. 1 oder 2 thürPAG genannten verantwortlichen Personen bestimmte oder von diesen herrührende Mitteilungen entgegennehmen (§ 34a Abs. 3 Satz 1 Nr. 3 Buchstabe a thürPAG n. F.). Die präventiv-polizeiliche Telekommunikationsüberwachung, die sich gegen die Kontakt- und Begleitpersonen richtet, ist auch zulässig, soweit Tatsachen die Annahme rechtfertigen, dass die in § 34a Abs. 3 Satz 1 Nr. 1 oder 2 thürPAG genannten verantwortlichen Personen die Kommunikationseinrichtungen der Kontakt- und Begleitpersonen benutzen werden (§ 34a Abs. 3 Satz 1 Nr. 3 Buchstabe b thürPAG n. F.). Da die Kontakttätigkeiten, die als bestimmte Indikatoren des hypothetischen Kausalverlaufs angesehen werden, deutlich genannt werden, stellt § 34a Abs. 3 Satz 1 Nr. 3 thürPAG n. F. keine Blankettermächtigung dar. Das Gebot rechtsstaatlicher Bestimmtheit ist also gewahrt.

II. Anforderung der Verhältnismäßigkeit

Über die Anforderung an die Bestimmtheit der Gesetze hinaus ist zu prüfen, ob die polizei- und ordnungsrechtlichen Vorschriften, die die Polizei zur präventiven Telekommunikationsüberwachung ermächtigen und damit in Grundrechte eingreifen, in Einklang mit dem Verhältnismäßigkeitsgrundsatz, der ein wesentliches Element des Rechtsstaatsprinzips ist[157], stehen. Da die verfassungsrechtlichen Gesetzesvorbehalte praktisch Vorbehalte des verhältnismäßigen Gesetzes sind[158], bedarf es einer eingehenden Prüfung der Verhältnismäßigkeit gesetzlicher Eingriffsermächtigungen.

1. Zweistufige Prüfung der Verhältnismäßigkeit

Der Grundsatz der Verhältnismäßigkeit erfordert eine zweistufige Prüfung[159]. Zunächst ist zu prüfen, ob der Zweck, den das Gesetz verfolgt, legi-

157 BVerfGE 90, 145 (173); 111, 54 (82); *Degenhart* (Rn. 101), Rn. 398; *Jarass* (Fn. 51), Art. 20 Rn. 80; *Maurer* (Fn. 8), § 8 Rn. 55; *Sachs* (Fn. 101), Art. 20 Rn. 146; *Schulze-Fielitz* (Fn. 51), Art. 20 (Rechtsstaat) Rn. 179; *Sodan* (Fn. 101), Art. 20 Rn. 66; *Sommermann* (Fn. 101), Art. 20 Rn. 308; *Zippelius/Würtenberger* (Fn. 2), § 12 Rn. 84. Heute lässt sich der Verhältnismäßigkeitsgrundsatz nicht nur als ein verfassungsrechtliches Prinzip, sondern auch als ein Prinzip des Europarechts ansehen (vgl. *Degenhart* (Rn. 101), Rn. 413; *Sachs* (Fn. 101), Art. 20 Rn. 145; *Zippelius/Würtenberger* (Fn. 2), § 12 Rn. 84).

158 *Zippelius/Würtenberger* (Fn. 2), § 19 Rn. 84.

159 *Maurer* (Fn. 8), § 8 Rn. 56 f.

tim ist. Dann wird näher geprüft, ob das Mittel, das der Erreichung dieses Zwecks dient, geeignet, erforderlich und angemessen ist.

a) Erste Prüfungsstufe: Legitimität des verfolgten Zwecks

Da sich die erste Prüfungsstufe der Verhältnismäßigkeit auf die Legitimität des verfolgten Zwecks erstreckt, muss der verfolgte Zweck genau bestimmt sein[160]. Bei der Ermittlung des verfolgten Zwecks ist nicht nur der subjektive Wille des Gesetzgebers, sondern auch der objektiv erkennbare Zweck zu berücksichtigen[161]. Nach der Feststellung des verfolgten Zwecks lässt sich die Legitimität des Zwecks prüfen. Entspricht der verfolgte Zweck dem Grundgesetz, ist er legitim[162]. Falls die Legitimität des verfolgten Zwecks zu verneinen ist, ist die Verfassungswidrigkeit des Gesetzes bereits gegeben[163]. In diesem Fall kann die Prüfung der Verhältnismäßigkeit auf der ersten Stufe abgebrochen werden[164].

b) Zweite Prüfungsstufe: Geeignetheit, Erforderlichkeit und Angemessenheit

Soweit festgestellt wird, dass das Gesetz einen legitimen Zweck verfolgt, folgt die zweite Prüfungsstufe, die die Rationalität des Verhältnisses zwischen dem verfolgten legitimen Zweck und den der Erreichung dieses Zwecks dienenden Mittel betrifft. Die zweite Stufe der Verhältnismäßigkeitsprüfung lässt sich in drei Unterstufen aufgliedern: Prüfung der Geeignetheit, der Erforderlichkeit und der Angemessenheit (Verhältnismäßigkeit im engeren Sinne).

aa) Geeignetheit

Zunächst ist zu prüfen, ob das im Gesetz vorgesehene Mittel den verfolgten legitimen Zweck fördern kann. Die Geeignetheit verlangt allerdings nicht, dass das vom Gesetz zugelassene Mittel in jedem Einzelfall einen Erfolg erzielen muss[165]. Bei der Prüfung der Geeignetheit geht es nicht um eine Optimierung von Maßnahmen[166]. Aus diesem Grund hat der Gesetzgeber

160 *Jarass* (Fn. 51), Art. 20 Rn. 83; *Maurer* (Fn. 8), § 8 Rn. 56; *Schulze-Fielitz* (Fn. 51), Art. 20 (Rechtsstaat) Rn. 181.

161 *Cremer*, NVwZ 2004, S. 668 (670 ff.); *Epping*, Grundrechte, Rn. 49; *Jarass* (Fn. 51), Art. 20 Rn. 83; *Manssen*, Grundrechte, Rn. 165 f.; *Zippelius/Würtenberger* (Fn. 2), § 19 Rn. 84.

162 Vgl. *Degenhart* (Rn. 101), Rn. 399; *Zippelius/Würtenberger* (Fn. 2), § 19 Rn. 85. Ein legitimer Zweck muss aber nicht aus der Verfassung hergeleitet werden (vgl. *Hufen* (Fn. 2), § 9 Rn. 19).

163 *Maurer* (Fn. 8), § 8 Rn. 56.

164 Vgl. *Dreier* in: Dreier, GG, Bd. 1, Vorb. Rn. 146.

165 BVerfGE 67, 157 (175); 96, 10 (23); 113, 167 (234); *Jarass* (Fn. 51), Art. 20 Rn. 84; *Pieroth/Schlink* (Fn. 2), Rn. 293; *Sachs* (Fn. 101), Art. 20 Rn. 150; *Schulze-Fielitz* (Fn. 51), Art. 20 (Rechtsstaat) Rn. 182; *Stern*, Staatsrecht, Bd. III/2, S. 776.

166 BVerfGE 113, 167 (234); *Hufen* (Fn. 2), § 9 Rn. 20; *Jarass* (Fn. 51), Art. 20 Rn. 84; *Manssen* (Fn. 161), Rn. 167; *Sachs* (Fn. 101), Art. 20 Rn. 150; *Schulze-Fielitz* (Fn. 51), Art. 20 (Rechtsstaat) Rn. 182; *Sodan* (Fn. 101), Art. 20 Rn. 64.

für die Eignung des gewählten Mittels einen weiten Beurteilungs- und Prognosespielraum[167].

bb) Erforderlichkeit

Zudem muss die Erforderlichkeit des vom Gesetzgeber zugelassenen Mittels geprüft werden. Ein gewähltes Mittel ist nicht erforderlich, wenn es noch andere gleich geeignete Mittel, die weniger intensiv in Grundrechte eingreifen, gibt. Bei der Auswahl des Mittels hat die Maßnahme, die zum milderen Grundrechtseingriff führt, den Vorrang[168]. Zu beachten ist, dass ein Mittel auch nicht erforderlich ist, wenn der Adressat zwar weniger belastet wird, aber Dritte oder die Allgemeinheit intensiver beeinträchtigt werden[169]. Ein weiter Beurteilungs- und Prognosespielraum des Gesetzgebers wird – wie bei der Geeignetheit – für die Erforderlichkeit des Mittels anerkannt[170].

cc) Angemessenheit (Verhältnismäßigkeit im engeren Sinne)

Schließlich ist zu prüfen, ob das Verhältnis zwischen den durch die staatliche Maßnahme belasteten grundrechtlichen Rechtsgütern und dem durch die staatliche Maßnahme verfolgten Zweck angemessen ist. Bei der Prüfung der Angemessenheit geht es um eine Abwägung zwischen Rechtgütern[171]. Die Je-desto-Formel lässt sich als der Grundsatz der Abwägung ansehen: Je intensiver die staatliche Maßnahme in Grundrechte eingreift, desto gewichtiger muss das durch die staatliche Maßnahme geschützte Rechtsgut sein[172]. Eine solche Rechtsgüterabwägung ist nur möglich, wenn die Intensität des Grundrechtseingriffs und das Gewicht des geschützten Rechtsguts bestimmt sind[173].

---

167 BVerfGE 110, 117, (194); 110, 226 (262); *Degenhart* (Rn. 101), Rn. 401; *Epping* (Fn. 161), Rn. 52; *Hufen* (Fn. 2), § 9 Rn. 20; *Pieroth/Schlink* (Fn. 2), Rn. 292; *Sachs* (Fn. 101), Art. 20 Rn. 151; *Schulze-Fielitz* (Fn. 51), Art. 20 (Rechtsstaat) Rn. 182; *Sodan* (Fn. 101), Art. 20 Rn. 64; *Zippelius/Würtenberger* (Fn. 2), § 12 Rn. 87.

168 *Manssen* (Fn. 161), Rn. 169; *Sachs* (Fn. 101), Art. 20 Rn. 153; *Sodan* (Fn. 101), Art. 20 Rn. 65.

169 *Manssen* (Fn. 161), Rn. 170; *Schulze-Fielitz* (Fn. 51), Art. 20 (Rechtsstaat) Rn. 183; *Stern* (Fn. 165), S. 781.

170 BVerfGE 110, 226 (262); *Epping* (Fn. 161), Rn. 54; *Pieroth/Schlink* (Fn. 2), Rn. 292, 297; *Sachs* (Fn. 101), Art. 20 Rn. 153; *Schulze-Fielitz* (Fn. 51), Art. 20 (Rechtsstaat) Rn. 183.

171 BVerfGE 92, 277 (327); *Degenhart* (Rn. 101), Rn. 406; *Epping* (Fn. 161), Rn. 56; *Hufen* (Fn. 2), § 9 Rn. 24; *Jarass* (Fn. 51), Art. 20 Rn. 86; *Manssen* (Fn. 161), Rn. 172; *Maurer* (Fn. 8), § 8 Rn. 57; *Pieroth/Schlink* (Fn. 2), Rn. 299; *Sachs* (Fn. 101), Art. 20 Rn. 155; *Schulze-Fielitz* (Fn. 51), Art. 20 (Rechtsstaat) Rn. 184; *Sodan* (Fn. 101), Art. 20 Rn. 66; *Sommermann* (Fn. 101), Art. 20 Rn. 314; *Stern* (Fn. 165), S. 783; *Zippelius/Würtenberger* (Fn. 2), § 12 Rn. 89.

172 Vgl. *Alexy*, Theorie der Grundrechte, S. 146; *Epping* (Fn. 161), Rn. 56; *Sommermann* (Fn. 101), Art. 20 Rn. 314; *Zippelius/Würtenberger* (Fn. 2), § 12 Rn. 89.

173 Vgl. *Manssen* (Fn. 161), Rn. 172; *Zippelius/Würtenberger* (Fn. 2), § 12 Rn. 89.

2. Auswirkung des Bestimmtheitsdefizits auf die Prüfung der Verhältnismäßigkeit

In Bezug auf die Verhältnismäßigkeit präventiv-polizeilicher Telekommunikationsüberwachung zeigte das Urteil des Bundesverfassungsgerichts, durch das § 33a Abs. 1 Nr. 2 und 3 ndsSOG a. F. für nichtig erklärt wurde, dass ein Bestimmtheitsdefizit des Gesetzes zur Verletzung des Verhältnismäßigkeitsgrundsatzes führen kann[174]. Der Ausgangspunkt besteht darin, dass bei der Prüfung der Verhältnismäßigkeit im engeren Sinne, wie bereits ausgeführt wurde, die abzuwägenden Rechtsgüter (die durch die staatliche Maßnahme belasteten grundrechtlichen Rechtsgüter und die dadurch geschützten Rechtsgüter) bestimmt sein müssen.

a) Präventiv-polizeiliche Telekommunikationsüberwachung als schwerer Grundrechtseingriff

Das Bundesverfassungsgericht hatte mit Recht betont, dass die präventiv-polizeiliche Telekommunikationsüberwachung ein schwerer Grundrechtseingriff sei[175]. Diese Einschätzung beruhte auf folgenden Erwägungen.

Zunächst gehe es beim präventiv-polizeilichen Zugriff auf die Telekommunikation um personenbezogene Daten, die einen hohen Rang besitzen[176]. Der schwere Eingriff in Grundrechte beschränke sich nicht auf die Erhebung der Kommunikationsinhalte. Vielmehr könne ein besonders schwerer Grundrechtseingriff auch aus der Erhebung der Verbindungsdaten (Verkehrsdaten) und der Standortkennung resultieren. Denn Verbindungsdaten ließen erhebliche Rückschlüsse auf das Kommunikationsverhalten zu[177]. Durch die Erhebung der Standortkennung könne ein Bewegungsbild der betroffenen Personen erstellt werden[178].

Zudem treffe die präventiv-polizeiliche Telekommunikationsüberwachung eine große Zahl von Personen. Falls diese polizeiliche Maßnahme im Vorfeld der Gefahr durchgeführt werde, würden auch die Kontakt- und Begleitpersonen oder gänzlich unbeteiligte Dritte betroffen. Dementsprechend führe die präventiv-polizeiliche Telekommunikationsüberwachung zu einer großen Streubreite des Grundrechtseingriffs[179].

Ferner intensiviert die Ahnungslosigkeit der Betroffenen den Grundrechtseingriff, zu dem die präventiv-polizeiliche Telekommunikationsüber-

174 BVerfGE 113, 348 (385 ff.).
175 BVerfGE 113, 348 (382 ff.).
176 BVerfGE 113, 348 (382 f.). Zum hohen Rang des Schutzes von personenbezogenen Daten bzw. des Rechts auf informationelle Selbstbestimmung BVerfGE 118, 168 (197); *Bull*, ZRP 2008, S. 233 (234).
177 BVerfGE 113, 348 (383).
178 BVerfGE 113, 348 (383).
179 BVerfGE 113, 348 (383).

wachung führt[180]. Über die Durchführung präventiv-polizeilicher Telekommunikationsüberwachung wird erst später informiert. Dies habe zur Folge, dass ein effektiver Rechtsschutz erschwert ist. Dies wiederum erhöhe die Intensität des Eingriffs[181].

Schließlich werde die Eingriffsschwere präventiv-polizeilicher Telekommunikationsüberwachung dadurch verstärkt, dass die erhobenen Daten nicht nur zur Gefahrenabwehr, sondern auch zu weiteren Zwecken gespeichert, verändert und genutzt werden können[182]. Wird die präventiv-polizeiliche Telekommunikationsüberwachung im Vorfeld der Gefahr durchgeführt, könne der Grundsatz der Zweckbindung bei der weiteren Verwertung der erlangten Informationen praktisch kaum eingehalten werden. Da die Zwecke der Datenverwertung unbestimmt oder noch nicht bestimmt sind, erhöhe sich die Schwere des Grundrechtseingriffs bereits in der Phase der Informationserhebung[183].

Abgesehen von dem problematischen Argument, dass der unbestimmte Zweck der späteren Datenverwertung den Eingriffsgrad präventiv-polizeilicher Telekommunikationsüberwachung erhöhe[184], ist dem Ergebnis, dass die präventiv-polizeiliche Telekommunikationsüberwachung zu einem schweren Grundrechtseingriff führe, zuzustimmen. Diese Konsequenz gilt nicht nur für § 33a Abs. 1 Nr. 2 und 3 ndsSOG a. F., sondern auch für alle in anderen Bundesländern zugelassenen Maßnahmen der präventiv-polizeilichen Telekommunikationsüberwachung. Bei der Durchführung einer präventiv-polizeilichen Telekommunikationsüberwachung dürfen personenbezogene Daten erhoben werden. Jedenfalls sind E-Mail-Adressen (ggf. IP-Adressen), die sich als personenbezogene Daten ansehen lassen[185], erfasst, soweit die Polizei präventiv einen E-Mail-Verkehr überwacht. Auch die geltenden polizei- und ordnungsgesetzlichen Ermächtigungsvorschriften zum Zugriff auf die Telekommunikation zeigen, dass die präventiv-polizeiliche Telekommunikationsüberwachung der Erhebung personen-

180 BVerfGE 113, 348 (383 f.).
181 BVerfGE 113, 348 (384).
182 BVerfGE 113, 348 (384).
183 BVerfGE 113, 348 (384 f.).
184 Folgt man diesem vom Bundesverfassungsgericht entwickelten Argument, diffundiert der Unterschied zwischen der Informationserhebung und der Informationsverwertung. Richtiger ist, dass die Informationsverwertung einen selbstständigen Eingriff in Grundrechte gegenüber der Informationserhebung darstellt. In diesem Zusammenhang ist es schwer einzusehen, warum die unbestimmten Zwecke der Informationsverwertung, die (nur) für die Eingriffsschwere der Informationsverwertung wichtig sind, zur Eingriffsintensität der Informationserhebung führen.
185 AG Wuppertal, MMR 2008, S. 632; LG Berlin, MMR 2007, S. 799; *Czychowski/Nordemann*, NJW 2008, S. 3095 (3096); *Dammann*, in: Simitis, BDSG, § 3 Rn. 10; *Jandt*, MMR 2006, S. 652 (654); *Roßnagel*, NZV 2006, S. 281 (282); *Warg*, MMR 2006, S. 77 (80 f.).

bezogener Daten dient[186]. Ausgehend von der Sphärentheorie, nach der sich die Öffentlichkeitssphäre und die nur unter strikter Wahrung des Verhältnismäßigkeitsgrundsatzes einschränkbare Privatsphäre sowie die absolut unantastbare Intimsphäre voneinander unterscheiden lassen[187], können die personenbezogenen Daten mindestens der Privatsphäre zugerechnet werden[188]. Da die Gegenstände präventiv-polizeilicher Telekommunikationsüberwachung (= personenbezogene Daten) relevant für die Privatsphäre, ja sogar die Intimsphäre sind, lässt sich festhalten, dass diese polizeiliche Maßnahme intensiv in Grundrechte eingreift. Berücksichtigt man, dass alle in anderen Bundesländern verabschiedeten polizei- und ordnungsgesetzlichen Vorschriften, die der Polizei die präventive Telekommunikationsüberwachung erlauben, zu einem eine große Zahl von Personen treffenden und einen effektiven Rechtsschutz erschwerenden Grundrechtseingriff führen können, kann dies auch die Konsequenz haben, dass die präventiv-polizeiliche Telekommunikationsüberwachung den Grundrechtseingriff intensiviert.

b) Mangel an Anhaltspunkten für die Angemessenheitsprüfung

Da die präventiv-polizeiliche Telekommunikationsüberwachung tief in Grundrechte eingreift, muss das Gewicht der durch diese polizeiliche Maßnahme geschützten Rechtsgüter – nach der Je-desto-Formel – hinreichend groß sein, sonst kann sie die Prüfung der Verhältnismäßigkeit im engeren Sinne nicht bestehen. Wird die präventiv-polizeiliche Telekommunikationsüberwachung im Vorfeld einer Gefahr, wo sich der Wahrscheinlichkeitsgrad des Schadenseintritts reduziert, durchgeführt, ist die Anforderung an das große Gewicht der zu schützenden Rechtsgüter besonders zu betonen[189]. Denn im Bereich des Polizeirechts verlangt die Je-desto-Formel: Je gewichtiger das gefährdete Rechtsgut ist, desto geringere Anforderungen müssen an den Grad der Wahrscheinlichkeit gestellt werden[190].

Die Rechtsgutsabwägung, die bei der Angemessenheitsprüfung im Vordergrund steht, basiert darauf, dass die Tatbestände der polizei- und ordnungsgesetzlichen Ermächtigungsvorschriften zur Telekommunikations-

186 So deutlich Art. 34a Abs. 1 S. 1 bayPAG; § 33b Abs. 1 bbgPolG; § 10a Abs. 1 S. 1 hambGDatPol; § 34a Abs. 1 S. 1 mvSOG; § 33a Abs. 1 ndsSOG; § 31 Abs. 1 rpPOG; § 28b Abs. 1 S. 1 saarlPolG; § 185a Abs. 1 S. 1 shLVwG.

187 Vgl. dazu BVerfGE 27, 344 (350 f.); *Albers*, Informationelle Selbstbestimmung, S. 208 f.; *Dreier* (Fn. 164), Art. 2 I Rn. 87 f.; *Hufen* (Fn. 2), § 11 Rn. 4; *von Münch* (Fn. 2), Rn. 322; *Pieroth/Schlink* (Fn. 2), Rn. 396; *Schmitt Glaeser*, in: Isensee/Kirchhof, HStR, Bd. 6, 2. Aufl., § 129 Rn. 34 ff.; *Sodan* (Fn. 101), Art. 2 Rn. 17; *Stern* (Fn. 138), S. 264 ff.

188 Vgl. *Jarass* (Fn. 51), Art. 2 Rn. 61.

189 BVerfGE 113, 348 (386 f.).

190 BVerfGE 113, 348 (386); *Götz* (Fn. 1), § 6 Rn. 7; *Gusy* (Fn. 55), Rn. 115; *Kugelmann* (Fn. 75), 4. Kapitel Rn. 100; *Schenke* (Fn. 25), Rn. 77; *Schoch* (Fn. 53), Rn. 89; *Würtenberger/Heckmann* (Fn. 52), Rn. 417.

überwachung ausreichend bestimmt sind. Wenn die gesetzlichen Voraussetzungen der präventiv-polizeilichen Telekommunikationsüberwachung hinreichend bestimmt sind, lässt sich danach prüfen, ob bei der Durchführung der präventiv-polizeilichen Telekommunikationsüberwachung ein Rechtsgut, das ein großes Gewicht besitzt und damit den starken Grundrechtseingriff rechtfertigen kann, gefährdet wird. Falls eine solche Festlegung des gefährdeten Rechtsguts wegen des gesetzlichen Bestimmtheitsdefizits erschwert wird, ist die Prüfung der Angemessenheit unmöglich, weil in dieser Situation keine gesetzlichen Anhaltspunkte für die Abwägung der Rechtsgüter vorliegen[191]. Der Mangel an Anhaltspunkten für die Abwägung hat zur Folge, dass die polizei- und ordnungsgesetzlichen Ermächtigungsvorschriften zur präventiven Telekommunikationsüberwachung, die nicht ausreichend bestimmt sind, keine verhältnismäßigen Normen darstellen. Ausgehend davon können die polizei- und ordnungsgesetzlichen Ermächtigungsvorschriften zur präventiven Telekommunikationsüberwachung, die nicht hinreichend bestimmt sind, nicht dem Grundsatz der Verhältnismäßigkeit, der in der rechtlichen Vernunft verwurzelt ist[192], entsprechen. Aus diesem Grund stellte das Bundesverfassungsgericht fest, dass § 33a Abs. 1 Nr. 2 und 3 ndsSOG a. F. nicht verhältnismäßig war[193]. Diese Konsequenz soll auch für alle polizei- und ordnungsgesetzlichen Ermächtigungsvorschriften zur präventiven Telekommunikationsüberwachung gelten. Folglich lässt sich festhalten, dass die oben erwähnten brandenburgischen Ermächtigungsvorschriften zur im Vorfeld der Gefahr durchgeführten präventiv-polizeilichen Telekommunikationsüberwachung aufgrund des Bestimmtheitsdefizits nicht mit dem Grundsatz der Verhältnismäßigkeit vereinbar sind.

3. Verhältnismäßigkeit der polizei- und ordnungsgesetzlichen Ermächtigungsvorschriften zur Telekommunikationsüberwachung

Die polizei- und ordnungsgesetzlichen Ermächtigungsvorschriften zur Telekommunikationsüberwachung, die die Anforderungen an die Bestimmtheit erfüllen, können die Prüfung des Verhältnismäßigkeitsgrundsatzes bestehen. Diese Ermächtigungsvorschriften verfolgen den legitimen Zweck, eine gegenwärtige Gefahr für besonders hochrangige Rechtsgüter[194] abzuwehren. Da der Zugriff auf die Telekommunikation zu einem schweren Grundrechtseingriff führt, darf die präventiv-polizeiliche Telekommunikationsüberwachung nach diesen Ermächtigungsvorschriften nur zum Schutz besonders hochrangiger Rechtsgüter durchgeführt werden. Darüber hinaus

191 BVerfGE 113, 348 (388 f.); *Trute* (Fn. 118), S. 85 (96).
192 *Zippelius/Würtenberger* (Fn. 2), § 12 Rn. 85.
193 BVerfGE 113, 348 (382 ff.).
194 Z. B. Leib, Leben einer Person.

verlangen diese Ermächtigungsvorschriften eine erhöhte Wahrscheinlichkeit des Schadenseintritts. In diesem Zusammenhang lässt sich die Verhältnismäßigkeit dieser Ermächtigungsvorschriften bejahen.

Auch die hinreichend bestimmten Ermächtigungsvorschriften zur im Vorfeld der Gefahr durchgeführten präventiv-polizeilichen Telekommunikationsüberwachung sind verhältnismäßig, obwohl im Vorfeld der Gefahr nur eine geringe Wahrscheinlichkeit des Schadenseintritts besteht. Denn durch die in diesen Ermächtigungsvorschriften statuierten Schutzziele der zu verhindernden „schwerwiegenden Straftat" bzw. „besonders schweren Straftat" ist eine Begrenzung dieser Ermächtigungsvorschriften auf besonders hochrangige Rechtsgüter gewährleistet. Das überragende Gewicht der geschützten Rechtsgüter ist geeignet, den schweren Grundrechtseingriff zu rechtfertigen.

III. Schutz des Kernbereichs privater Lebensgestaltung

Über die Anforderung an die Bestimmtheit und die Verhältnismäßigkeit hinaus verlangt das Bundesverfassungsgericht, dass die Ermächtigungsvorschriften zur präventiv-polizeilichen Telekommunikationsüberwachung hinreichende Vorkehrungen dafür treffen, dass Eingriffe in den absolut geschützten Kernbereich privater Lebensgestaltung unterbleiben[195]. Bei der Durchführung präventiv-polizeilicher Telekommunikationsüberwachung können personenbezogene Daten, die sich auf den Kernbereich höchstpersönlicher Lebensgestaltung beziehen, betroffen sein[196]. Da Art. 10 Abs. 1 GG die freie Entfaltung der Persönlichkeit und die Menschenwürde schütze, sei eine präventiv-polizeiliche Telekommunikationsüberwachung nicht zu rechtfertigen und müsse unterbleiben, wenn diese Inhalte erfasse, die zum Kernbereich privater Lebensgestaltung gehören[197]. Berücksichtige man, dass bei der Durchführung präventiv-polizeilicher Telekommunikationsüberwachung nicht vorhersehbar sei, welche Inhalte die zu beobachtende Telekommunikation enthalte, liege ein Risiko vor, dass ein in den Kernbereich privater Lebensgestaltung fallender Telekommunikationsinhalt erfasst werde[198]. Dieses Risiko könne allenfalls bei einem besonders hohen Rang des gefährdeten Rechtsguts und einer durch konkrete Anhaltspunkte gekennzeichneten Lage, die auf einen unmittelbaren Bezug zur künftigen Begehung der Straftaten schließen lasse, hingenommen werden[199]. Zum Schutz der Daten, die zum Kernbereich privater Lebensgestaltung gehören, seien Vorkehrungen zu treffen, die sichern, dass die Kom-

195 BVerfGE 113, 348 (390 ff.).
196 BVerfGE 113, 348 (390 f.).
197 BVerfGE 113, 348 (391 f.).
198 BVerfGE 113, 348 (392).
199 BVerfGE 113, 348 (392).

munikationsinhalte des höchstpersönlichen Bereichs nicht gespeichert und verwertet werden, sondern unverzüglich gelöscht würden, wenn diese Daten ausnahmsweise erhoben worden wären[200].

Der Ausgangspunkt, dass die durch eine präventiv-polizeiliche Telekommunikationsüberwachung erfassten Daten, die in den Kernbereich privater Lebensgestaltung fallen, zu schützen sind, ist sicherlich zu begrüßen. Aus den im Folgenden zu entwickelnden Gründen ist allerdings fraglich, ob die vom Bundesverfassungsgericht angenommene Folgerung, dass die keine Vorkehrungen für den Schutz der Daten aus dem Kernbereich privater Lebensgestaltung enthaltenden Ermächtigungsvorschriften[201] zur präventiv-polizeilichen Telekommunikationsüberwachung (absolut) verfassungswidrig sind, zutreffend ist.

Der Schutzgrad des Kernbereichs privater Lebensgestaltung wird im Urteil des Bundesverfassungsgerichts widersprüchlich festgelegt. Das Bundesverfassungsgericht erklärte einerseits, dass der Kernbereich privater Lebensgestaltung absolut geschützt sei[202]. Falls die Telekommunikationsüberwachung Inhalte erfasse, die zu diesem Kernbereich zählen würden, sei sie nicht zu rechtfertigen und müsse unterbleiben[203]. Andererseits legte es dar, dass die Berührung des Kernbereichs ein hinzunehmendes Risiko sei. Bei der Durchführung einer Telekommunikationsüberwachung sei das Risiko nicht auszuschließen, dass die staatliche Beobachtungsmaßnahme eine Kommunikation aus dem Kernbereich privater Lebensgestaltung erfasse. Verfassungsrechtlich hinzunehmen sei dieses Risiko allenfalls bei einem besonders hohen Rang des gefährdeten Rechtsguts und einer durch konkrete Anhaltspunkte gekennzeichneten Lage, die auf einen unmittelbaren Bezug zur zukünftigen Begehung der Straftat schließen lasse[204]. Berücksicht man, dass der Schutz des unantastbaren Kernbereichs privater Lebensgestaltung – wie das Bundesverfassungsgericht durch sein Urteil betonte – absolut sein soll, ist es schwer einzusehen, warum das Bundesverfassungsgericht die Möglichkeit, dass der Kernbereich bei der Durchführung einer Telekommunikationsüberwachung berührt wird, als ein verfassungsrechtlich zu akzeptierendes Risiko betrachtet. Auf jeden Fall steht die

200 BVerfGE 113, 348 (392).

201 Im Gegensatz zu den meisten Bundesländern, in denen die präventiv-polizeiliche Telekommunikationsüberwachung gesetzlich zulässig ist, fehlen in den baden-württembergischen, hessischen und rheinland-pfälzischen Ermächtigungsvorschriften Regelungen zum Kernbereichschutz. Der Grund für die im bwPolG fehlende Regelung liegt wohl darin, dass der baden-württembergische Gesetzgeber die präventiv-polizeiliche Telekommunikationsüberwachung, die in Baden-Württemberg nicht die Überwachung der Telekommunikationsinhalte, sondern die Erhebung der Telekommunikationsverkehrsdaten betrifft, als einen minder schweren Eingriff ansieht (vgl. BW-LT-Drs. 14/3165, S. 58).

202 BVerfGE 113, 348 (390).

203 BVerfGE 113, 348 (391 f.).

204 BVerfGE 113, 348 (392).

nach dem Urteil des Bundesverfassungsgerichts zugelassene Abwägung zwischen dem oben genannten Risiko und der Informationserhebung, die der Verhinderung zukünftig möglicher Straftaten und dem Schutz der besonders hochrangigen gefährdeten Rechtsgüter dient, nicht in Einklang mit dem vom Bundesverfassungsgericht selbst statuierten absoluten Schutz des Kernbereichs privater Lebensgestaltung. Das Urteil des Bundesverfassungsgerichts ist insofern widersprüchlich.

Obwohl das Bundesverfassungsgericht auf dem Standpunkt stand, dass der Verwirklichung des oben genannten Risikos nachträglich durch Vorkehrungen zum Schutz des Kernbereichs (z. B. Abbruch der Überwachung und Verbot der Verwertung sowie Löschung der erhobenen Daten) abgeholfen werden könne[205], bewahrte es Schweigen zu der Frage, ob die präventiv-polizeiliche Telekommunikationsüberwachung, die Daten aus dem Kernbereich privater Lebensgestaltung erfasst hatte, bereits zur Verletzung des Kernbereichs, die aufgrund der Unantastbarkeit des Kernbereichs auf jeden Fall verfassungsrechtlich unzulässig ist, führt. Dieses Schweigen beweist sowohl die Widersprüchlichkeit des Urteils als auch den Zweifel an der Effektivität der Vorkehrungen, die nach dem Urteil des Bundesverfassungsgerichts den Kernbereich schützen können. Denn diese Vorkehrungen werden erst dann getroffen, wenn ein Eingriff in den Kernbereich bereits vorliegt. Ihre Funktion ist nicht die Verhinderung des Eingriffs in den Kernbereich, sondern nur die Minimierung der bereits realisierten Kernbereichsverletzung. Da die Kenntnisnahme der Kommunikationsinhalte aus dem Kernbereich nicht durch die oben genannten vom Bundesverfassungsgericht verlangten Vorkehrungen, die nur eine nachträgliche Abhilfefunktion haben, ungeschehen gemacht werden kann[206], ist es nicht möglich, dass die Verfassungswidrigkeit des bereits realisierten Eingriffs in den Kernbereich durch die oben genannten Vorkehrungen beseitigt wird. Insoweit ist es bedenklich, dass Vorkehrungen wie etwa das Verwertungsgebot einen effektiven Schutz des Kernbereichs darstellen sollen[207].

Damit ist festzuhalten, dass die präventiv-polizeiliche Telekommunikationsüberwachung, die Daten aus dem Kernbereich erfasst hatte, bereits zum Eingriff in den Kernbereich privater Lebensgestaltung führt. Wenn sich dieser Eingriff in den Kernbereich – wie das Bundesverfassungsgericht vertrat – nach der Abwägung mit dem Schutz eines besonders hochrangigen gefährdeten Rechtsguts als ein verfassungsrechtlich hinzunehmendes Risiko ansehen lässt, wird auch anerkannt, dass die Rechtfertigung dieses

205 BVerfGE 113, 348 (392).

206 So die abweichende Meinung der Richterinnen *R. Jaeger* und *C. Hohmann-Dennhardt* zum Lauschangriff-Urteil des Bundesverfassungsgerichts, BVerfGE 109, 279 (382); ebenso *Kutscha*, NJW 2005, S. 20 (21).

207 Zu den praktischen Schwierigkeiten der Umsetzung eines Konzepts von Schutzvorkehrungen *Kutscha* (Fn. 206), S. 20 (21); *Stephan*, VBlBW 2005, S. 410 (412 f.).

Eingriffs durch Abwägung erfolgen kann. Jedoch ist dieses Ergebnis nicht vereinbar mit der auch vom Bundesverfassungsgericht festgelegten Eigenart des Kernbereichsschutzes, die den Kernbereich absolut schützt und damit ein Eingriff in den Kernbereich nicht zu rechtfertigen ist. Aufgrund dieser Kontradiktion ist fraglich, ob bei der Durchführung einer präventiv-polizeilichen Telekommunikationsüberwachung der Schutz des Kernbereichs privater Lebensgestaltung eine absolut unantastbare Grenze oder nur ein abwägbares Interesse ist. Wenn er eine absolut unantastbare Grenze der präventiv-polizeilichen Telekommunikationsüberwachung ist, stellen die genannten vom Bundesverfassungsgericht verlangten Vorkehrungen, die erst nach der Verletzung des Kernbereichs getroffen werden, keine effektiven Schutzmaßnahmen dar. Lässt er sich umgekehrt als ein abwägbares Interesse betrachten, geht es nicht um Vorkehrungen zum Kernbereichsschutz, sondern um die Beachtung des Verhältnismäßigkeitsgrundsatzes. Der vom Bundesverfassungsgericht vorgebrachte Begriff des „Kernbereichs privater Lebensgestaltung" löst nur wenige der durch die präventiv-polizeiliche Telekommunikationsüberwachung verursachten Probleme.

IV. Zitiergebot

Gemäß Art. 19 Abs. 1 Satz 2 GG muss das in Grundrechte eingreifende Gesetz die eingeschränkten Grundrechte unter Angabe des Artikels nennen. Das in Art. 19 Abs. 1 Satz 2 GG normierte Zitiergebot hat die Funktion formeller Grundrechtssicherung[208]. Dadurch wird sichergestellt, dass sich der Gesetzgeber beim Erlass eines Gesetzes die dadurch erfolgende Beschränkung von Grundrechten bewusst macht[209]. Verstößt ein Gesetz gegen die Anforderungen des Art. 19 Abs. 1 Satz 2 GG, führt dies zur Nichtigkeit des Gesetzes[210].

Hinsichtlich des Eingriffs in das Fernmeldegeheimnis (Art. 10 Abs. 1 GG) erfüllen alle polizei- und ordnungsgesetzlichen Ermächtigungsregelungen zur präventiven Telekommunikation das Zitiergebot[211]. Wie bereits dargelegt wurde[212], führt die Durchführung der präventiv-polizeilichen Telekom-

208 *Dreier* (Fn. 164), Art. 19 I Rn. 18; *Huber*, in: von Mangoldt/Klein/Starck, GG, Bd. 1, Art. 19 Rn. 68; *Krebs*, in von Münch/Kunig, GG, Bd. 1, Art. 19 Rn. 14.

209 *Dreier* (Fn. 164), Art. 19 I Rn. 18; *Epping* (Fn. 161), Rn. 750; *Huber* (Fn. 208), Art. 19 Rn. 70; *Jarass* (Fn. 51), Art. 19 Rn. 3; *Krebs* (Fn. 208), Art. 19 Rn. 14; *Michael/Morlok*, Grundrechte, Rn. 580; *Pieroth/Schlink* (Fn. 2), Rn. 323; *Sachs* (Fn. 101), Art. 19 Rn. 25; *Zippelius/Würtenberger* (Fn. 2), § 19 Rn. 68.

210 BVerfGE 5, 13 (15 f.); *Bethge*, DVBl. 1972, S. 365; *Dreier* (Fn. 164), Art. 19 I Rn. 28; *Epping* (Fn. 161), Rn. 749; *Hofmann* (Fn. 103), Art. 19 Rn. 11; *Huber* (Fn. 208), Art. 19 Rn. 102; *Krebs* (Fn. 208), Art. 19 Rn. 18; *Sachs* (Fn. 101), Art. 19 Rn. 32; *Wuttke* (Fn. 5), S. 24 f.

211 Vgl. § 4 bwPolG; Art. 74 bayPAG; § 8 bbgPolG; § 28 hambGDatPol; § 10 hessSOG; § 78 mvSOG; § 10 ndsSOG; § 8 rpPOG; § 7 saarlPolG; § 227 shLVwG; § 11 thürPAG.

212 Siehe 4. Kapitel B.

munikationsüberwachung allerdings nicht nur zur Beschränkung des durch Art. 10 Abs. 1 GG geschützten Grundrechts. Da die Ermächtigungsvorschriften zur präventiv-polizeilichen Telekommunikationsüberwachung die Mitwirkungspflicht der Diensteanbieter regeln[213], ist auch die Berufsausübungsfreiheit (Art. 12 Abs. 1 GG) betroffen. In Polizei- und Ordnungsgesetzen, die die präventiv-polizeiliche Telekommunikationsüberwachung erlauben, fehlt es jedoch an einer Zitierklausel, die Art. 12 Abs. 1 GG nennt. Dies führt nicht zur Verfassungswidrigkeit der polizei- und ordnungsgesetzlichen Regelungen über die Mitwirkungspflichten der Diensteanbieter. Denn nach der Rechtsprechung des Bundesverfassungsgerichts gilt Art. 19 Abs. 1 Satz 2 GG nicht für Art. 12 Abs. 1 GG[214].

Durch sein Urteil erklärte das Bundesverfassungsgericht, dass Art. 19 Abs. 1 Satz 2 GG nur für die „Einschränkung der Grundrechte" gelte. Da die „Regelungen der Berufsausübung" nach Art. 12 Abs. 1 Satz 2 GG nicht als „Einschränkungen der Grundrechte" im Sinne des Art. 19 Abs. 1 GG betrachtet würden, falle die gesetzliche Regelung über die Berufsausübung nicht in den Anwendungsbereich des Zitiergebots[215]. Rechtsdogmatisch ist diese Auffassung jedoch zweifelhaft. Denn die Formulierung „regeln" in Art. 12 Abs. 1 Satz 2 GG eröffnet im Ergebnis „Eingriffsmöglichkeiten"[216]. Art. 12 Abs. 1 Satz 2 GG stellt eine typische verfassungsrechtliche Ermächtigung zur Grundrechtseinschränkung (Gesetzesvorbehalt) dar[217]. Sieht man Art. 12 Abs. 1 Satz 2 GG als eine Einschränkungsermächtigung an, kann die „Regelung" der Berufsausübung im Sinne des Art. 12 Abs. 1 Satz 2 GG nicht vom Anwendungsbereich des Art. 19 Abs. 1 Satz 2 GG ausgenommen werden, andernfalls liegt eine deutliche Inkonsequenz vor[218]. Ob der betroffene Grundrechtsartikel die Formulierung „einschränken" enthält, spielt nach der hier vertretenen Ansicht keine Rolle für den Anwendungsbereich des Zitiergebots. Die Auslegung der Reichweite des Zitiergebots kann nicht eng und starr nur an den formellen Ausdruck „einschränken"

213 Vgl. § 23a Abs. 5 bwPolG; Art. 34b bayPAG; § 33b Abs. 6 bbgPolG; § 10a Abs. 3 hambGDatPol; § 15a Abs. 1 hessSOG; § 34a Abs. 6 mvSOG; § 33a Abs. 7 ndsSOG; § 31 Abs. 6 rpPOG; § 28b Abs. 2 saarlPolG; § 185a Abs. 4 shLVwG; § 34a Abs. 1 thürPAG.

214 BVerfGE 64, 72 (80 f.); vgl. auch *Gubelt*, in: von Münch/Kunig, GG, Bd. 1, Art. 12 Rn. 42; *Jarass* (Fn. 51), Art. 12 Rn. 23; *Wuttke* (Fn. 5), S. 24 f. Das Bundesverfassungsgericht erkennt noch viele andere Ausnahmen von der Anwendung des Zitiergebots an (vgl. *Dreier* (Fn. 164), Art. 19 I Rn. 21 ff.). Dies hat zur Folge, dass Art. 19 Abs. 1 S. 2 GG weitgehend leerläuft (*Stern*, in: Badura/Dreier, FS BVerfG, S. 1 (29)).

215 BVerfGE 64, 72 (79 ff.).

216 *Gubelt* (Fn. 215), Art. 12 Rn. 42; *Manssen*, in: von Mangoldt/Klein/Starck, GG, Bd. 1, Art. 12 Rn. 102; *Wieland*, in: Dreier, GG, Bd. 1, Art. 12 Rn. 103.

217 *Manssen* (Fn. 216), Art. 12 Rn. 6, 102; *Pieroth/Schlink* (Fn. 2), Rn. 914; *Mann*, in: Sachs, GG, Art. 12 Rn. 106; *Wieland* (Fn. 216), Art. 12 Rn. 103; *Zippelius/Würtenberger* (Fn. 2), § 30 Rn. 19.

218 *Dreier* (Fn. 164), Art. 19 I Rn. 26; *Epping* (Fn. 161), Rn. 389.

des Art. 19 Abs. 1 GG anknüpfen[219]. Vielmehr gilt die Zitierpflicht für jedes Gesetz, das praktisch in Grundrechte eingreift. Mithin ist rechtsdogmatisch richtiger, dass das in die durch Art. 12 Abs. 1 GG geschützte Berufsausübungsfreiheit eingreifende Gesetz auch von Art. 19 Abs. 1 Satz 2 GG erfasst wird[220].

C. Zusammenfassung des 5. Kapitels

Die geltenden polizei- und ordnungsgesetzlichen Ermächtigungsvorschriften zur präventiv-polizeilichen Telekommunikationsüberwachung sind kompetenzgemäß. Der Grund hierfür liegt darin, dass diese Vorschriften der Gefahrenabwehr dienen und der Landesgesetzgeber gemäß Art. 70 Abs. 1 GG die Gesetzgebungsbefugnis für die Gefahrenabwehr hat. Zwar hat der Bund gemäß Art. 73 Abs. 1 Nr. 7 GG eine Gesetzgebungskompetenz für die technische Seite der Telekommunikation, jedoch folgt daraus keine Gesetzgebungskompetenz des Bundes für die Telekommunikationsüberwachung. Darüber hinaus kann auch keine ungeschriebene Bundeskompetenz für die Telekommunikationsüberwachung aus Art. 73 Abs. 1 Nr. 7 GG hergeleitet werden. Zudem ist die in Art. 73 Abs. 1 Nr. 9a GG vorgeschriebene neue Bundeskompetenz für die Gefahrenabwehr (Abwehr des internationalen Terrorismus) nur subsidiär gegenüber der Landesgesetzgebungszuständigkeit für die Gefahrenabwehr. Ferner ist eine Bundeskompetenz kraft Natur der Sache für die präventiv-polizeiliche Telekommunikationsüberwachung mangels verfassungsrechtlicher Grundlage zu verneinen. Deswegen gibt es keine Bundesgesetzgebungskompetenz, die die Landesgesetzgebungskompetenz für die präventiv-polizeiliche Telekommunikationsüberwachung verdrängt. Die polizei- und ordnungsgesetzlichen Ermächtigungsvorschriften zur Telekommunikationsüberwachung sind damit formell verfassungsgemäß. In den Bundesländern, in denen eine polizei- und ordnungsgesetzliche spezielle Ermächtigungsvorschrift zur Telekommunikationsüberwachung fehlt, kann der präventiv-polizeiliche Zugriff auf den E-Mail-Verkehr unter dem Gesichtspunkt des Gesetzesvorbehalts keine formelle Verfassungsmäßigkeit besitzen. Denn weder andere Vorschrift der polizeilichen Standardmaßnahmen noch die polizeirechtliche Generalklausel können als Rechtsgrundlage der präventiv-polizeilichen E-Mail-Überwachung betrachtet werden.

Hinsichtlich der materiellen Verfassungsmäßigkeit der polizei- und ordnungsgesetzlichen Ermächtigungsvorschriften zur Telekommunikationsüberwachung ist festzuhalten, dass dem rechtsstaatlichen Bestimmtheits-

219 Kritisch auch *Dreier* (Fn. 164), Art. 19 I Rn. 26; *Huber* (Fn. 208), Art. 19 Rn. 89 ff.; *Sachs* (Fn. 101), Art. 19 Rn. 17, 29.

220 *Dietlein*, in: Stern, Staatsrecht, Bd. IV/1, S. 1889 f.; *Dreier* (Fn. 164), Art. 19 I Rn. 26; *Huber* (Fn. 208), Art. 19 Rn. 95; *Manssen* (Fn. 216), Art. 12 Rn. 7; *Sachs* (Fn. 101), Art. 19 Rn. 29.

gebot in den meisten Ermächtigungsvorschriften entsprochen wird. Die polizei- und ordnungsgesetzlichen Ermächtigungsvorschriften zur Telekommunikationsüberwachung, die hinreichend bestimmt sind, erfüllen zudem die Anforderungen des Verhältnismäßigkeitsprinzips. Alleine die brandenburgischen Ermächtigungsvorschriften zur Telekommunikationsüberwachung sind aufgrund des Bestimmtheitsdefizits auch nicht mit dem Verhältnismäßigkeitsgrundsatz vereinbar.

Nach Ansicht des Bundesverfassungsgerichts müssen die Ermächtigungsvorschriften zur präventiv-polizeilichen Telekommunikationsüberwachung hinreichende Vorkehrungen zum Schutz des Kernbereichs privater Lebensgestaltung enthalten. Allerdings ist diese Forderung nicht unproblematisch. Denn es fragt sich, ob der vom Bundesverfassungsgericht betonte absolute Schutz des Kernbereichs privater Lebensgestaltung damit vereinbar ist, zum Schutz besonders hochrangiger Rechtsgüter das Risiko eines entsprechenden Eingriffes hinzunehmen. Ferner ist die Effektivität der Vorkehrungen zum Schutz des Kernbereichs privater Lebensgestaltung zweifelhaft. Denn sie greifen i. d. R. erst dann, wenn ein Eingriff in den Kernbereich bereits erfolgte. Ihre Funktion ist demnach nicht die Verhinderung des Eingriffs in den Kernbereich, sondern nur die Minimierung der bereits realisierten Kernbereichsverletzung.

Schließlich wird der Zitierklausel des Art. 19 Abs. 1 Satz 2 GG hinsichtlich Art. 12 Abs. 1 GG in den Polizei- und Ordnungsgesetzen, die die Mitwirkungspflicht der Diensteanbieter regeln, nicht entsprochen. Dies führt nicht zur Verfassungswidrigkeit der polizei- und ordnungsgesetzlichen Regelungen über die Mitwirkungspflicht der Diensteanbieter, weil das Zitiergebot nach der Rechtsprechung des Bundesverfassungsgerichts nicht für Art. 12 Abs. 1 GG gilt. Rechtsdogmatisch ist diese Ausnahme von der Anwendung des Zitiergebots jedoch zweifelhaft.

6. Kapitel: Dreiecksverhältnis bei Durchführung einer präventiv-polizeilichen E-Mail-Überwachung

In Bezug auf die technische Durchführung der E-Mail-Überwachung hat das Abfangen der digitalen Datenpakete auf dem Übertragungsweg mit Hilfe der Diensteanbieter die höchste Zuverlässigkeit[1]. Dabei geht es um die Kontrolle des E-Mail-Knotens[2], über den die „gefährlichen" E-Mail-Datenpakete[3] übertragen werden. Der Überwacher setzt im kontrollierten E-Mail-Knoten ein Überwachungsprogramm (E-Mail-Filter) ein, um über diesen E-Mail-Knoten übertragene E-Mail-Datenpakete abzufangen und zu analysieren sowie die „gefährlichen" E-Mails zu finden. Nach dem Abfangen der E-Mail-Datenpakete werden Kopien der gefundenen „gefährlichen E-Mails" durch eine gemäß § 100a TKG in Verbindung mit § 3 TKÜV zu installierende spezielle Hardware (sogenannte Sina-Box), auf der sich die Polizei einloggen kann, an den Rechner der Polizei weitergeleitet[4]. Da nicht nur die E-Mails, die von der Zielperson abgeschickt werden, sondern auch alle über den überwachten E-Mail-Knoten übermittelten E-Mail-Datenpakete abgegriffen werden können, kann jeder Nutzer der E-Mail-Dienste, dessen E-Mail über den kontrollierten E-Mail-Knoten transportiert wird, betroffen sein. Dies hängt nicht davon ab, ob der Nutzer der E-Mail-Dienste die Zielperson der Überwachung ist. Insoweit führt die Durchführung einer präventiv-polizeilichen E-Mail-Überwachung – im Vergleich zu anderen präventiv-polizeilichen Telekommunikationsüberwachungen wie etwa die Telefonüberwachung – zu einer größeren Zahl der betroffenen Nutzer der Telekommunikationsdienste. In diesem Zusammenhang stellt das Rechtsverhältnis zwischen der Polizeibehörde, die eine präventive E-Mail-Überwachung durchführt, und den betroffenen Nutzern der E-Mail-Dienste eine neue Problematik des Polizeirechts im Digitalzeitalter dar. In Anbetracht dessen, dass die polizei- und ordnungsgesetzlichen Ermächtigungsvorschriften zur präventiven Telekommunikationsüberwachung den Diensteanbietern eine Mitwirkungspflicht auferlegen und damit das durch Art. 10 Abs. 1 GG geschützte Fernmeldegeheimnis der betroffenen Dienstenutzer beeinträchtigt wird, knüpfen die überwachende Polizeibehörde

1 *Störing*, Strafprozessuale Zugriffsmöglichkeiten, S. 60.

2 Der Begriff des E-Mail-Knotens bezeichnet in der Regel einen E-Mail-Server, den ein E-Mail-Provider anbietet.

3 Die E-Mail wird in einzelne digitale „Datenpakete" zerlegt und versandt. Dazu siehe 2. Kapitel B I 2.

4 *Ermert*, c't 1/2006, S. 44; *Krempl*, c't 26/2004, S. 100 (101 f.).

und die betroffenen Dienstenutzer Rechtsbeziehungen mit Diensteanbietern an. In diesem Kapitel wird das sich aus der Durchführung der präventiv-polizeilichen E-Mail-Überwachung ergebende Dreiecksverhältnis zwischen der überwachenden Polizeibehörde, den betroffenen Nutzern der E-Mail-Dienste und den Anbietern der E-Mail-Dienste untersucht.

A. Rechtsverhältnis zwischen der überwachenden Polizeibehörde und den betroffenen Nutzern der E-Mail-Dienste

Zunächst wird das Rechtsverhältnis zwischen der überwachenden Polizeibehörde und den betroffenen Nutzern der E-Mail-Dienste diskutiert. Da, wie oben bereits ausgeführt wurde, auch Nichtzielpersonen die betroffenen Nutzer der E-Mail-Dienste darstellen können, unterscheidet die folgende Erörterung zwischen Zielpersonen und Nichtzielpersonen.

I. Rechtsverhältnis zwischen der überwachenden Polizeibehörde und den Zielpersonen

Die polizei- und ordnungsgesetzlichen Ermächtigungsvorschriften zur Telekommunikationsüberwachung erlauben nur eine Datenerhebung über bestimmte Personen[5]. Dies besagt, dass nur diese in den Ermächtigungsregelungen erwähnten bestimmten Zielpersonen die Adressaten der Überwachungsmaßnahme darstellen dürfen. Unzulässig ist, dass die Polizei zur Erhebung der personenbezogenen Daten dieser Zielpersonen den E-Mail-

5 Vgl. § 23a Abs. 1 S. 1 Nr. 1 und 2 bwPolG; Art. 34a Abs. 1 S. 1, Abs. 3 bayPAG; § 33b Abs. 2 S. 1 und 2 bbgPolG; § 10a Abs. 1 S. 1 hambGDatPol; § 34a Abs. 1 S. 1 mvSOG; § 33a Abs. 1 ndsSOG; § 31 Abs. 1 rpPOG; § 28b Abs. 1 S. 1 saarlPolG; § 34a Abs. 3 thürPAG. Obwohl die hessischen und schleswig-holsteinischen Ermächtigungsvorschriften zur präventiv-polizeilichen Telekommunikationsüberwachung die Adressaten des Eingriffs nicht ausdrücklich regeln, bedeutet dies nicht, dass eine Datenerhebung (durch präventiv-polizeiliche Telekommunikationsüberwachung) über unbestimmte Personen (Totalüberwachung) in diesen beiden Bundesländern zulässig wäre. Wenn die Ermächtigungsvorschriften der Standardmaßnahme den Adressaten nicht regeln, sind die allgemeinen Regelungen der Polizeiverantwortlichkeit anzuwenden (*Schäfer*, Präventive Telekommunikationsüberwachung, S. 117; *W.-R. Schenke*, PolR, Rn. 197c; *Schoch*, in: Schmidt-Aßmann/Schoch, BesVerwR, 2. Kapitel, Rn. 123). Deswegen beschränkt sich der Adressatenkreis präventiv-polizeilicher Telekommunikationsüberwachung in der Regel auf den Störer im Sinne des Polizeirechts. Die Überwachungsmaßnahme zur Gefahrenabwehr kann nur ausnahmsweise gegen den Nichtstörer gerichtet werden, wenn ein polizeilicher Notstand vorliegt. Eine unbestimmte Vielzahl von Bürgern oder anlasslose Datenerhebung (durch präventiv-polizeiliche Telekommunikationsüberwachung) ist in Hessen und Schleswig-Holstein nicht erlaubt. Diese Konsequenz ergibt sich nicht nur aus der Störerdogmatik des Polizeirechts, sondern auch aus positivrechtlichen Regelungen (§§ 6, 7 und 9 hessSOG; §§ 217–220 shLVwG).

Verkehr Dritter überwacht[6]. Technisch kann die Polizei im kontrollierten E-Mail-Knoten ein Überwachungsprogramm, das die mit einer bestimmten E-Mail-Adresse oder IP-Adresse zusammenhängende E-Mail filtern kann, einsetzen, um die E-Mail-Kommunikation der Zielperson zu beobachten. Dies entspricht den polizei- und ordnungsgesetzlichen Ermächtigungsvorschriften zur Telekommunikationsüberwachung, die nur den Zugriff auf den E-Mail-Verkehr bestimmter Personen erlauben. Technisch kann eine präventiv-polizeiliche E-Mail-Überwachung dadurch durchgeführt werden, dass die Polizei mittels eines im kontrollierten E-Mail-Knoten eingesetzten Überwachungsprogramms nach einem bestimmten Stichwort, das sich nicht auf bestimmte Personen bezieht[7], sucht und gefährliche E-Mails abfängt. Rechtlich ist eine solche Totalüberwachung der E-Mails, die sich nicht gegen bestimmte Personen, sondern gegen alle Nutzer der E-Mail-Dienste richtet, unzulässig.

1. Realakt als Entstehungsgrund des Rechtsverhältnisses

Aus der Durchführung einer präventiv-polizeilichen E-Mail-Überwachung, die in polizei- und ordnungsgesetzlichen Vorschriften ihre Rechtsgrundlagen finden kann, ergibt sich die rechtliche Beziehung zwischen der überwachenden Polizeibehörde und der Zielperson, deren E-Mail-Kommunikation zu überwachen ist. Zweifellos ist diese rechtliche Beziehung ein Verwaltungsrechtsverhältnis[8]. Es fragt sich jedoch, auf welcher staatlichen Tätigkeit dieses Verwaltungsrechtsverhältnis beruht. Zwar lässt der Gesetzgeber durch abstrakt-generelle Gesetze die präventiv-polizeiliche Telekommunikationsüberwachung zu, jedoch sind die polizei- und ordnungsgesetz-

6 Vgl. *Berner/Köhler*, PAG, Art. 34a Rn. 9. Diese Konsequenz entspricht dem Grundsatz der Unmittelbarkeit der Datenerhebung (zum Grundsatz der Unmittelbarkeit der Datenerhebung *Petri*, in: Lisken/Denninger, HPolR, H Rn. 158 ff.; *Tischer*, System der informationellen Befugnisse, S. 347 ff.). Obwohl die positiven Vorschriften auch Ausnahmefälle vom Unmittelbarkeitsgrundsatz anerkennen, sodass die personenbezogenen Daten der Zielpersonen auch bei Dritten erhoben werden können (vgl. § 19 Abs. 1 S. 2 bwPolG; Art. 30 Abs. 2 S. 2 bayPAG; § 29 Abs. 2 S. 2 bbgPolG; § 2 Abs. 2 S. 2 hambGDatPol; § 13 Abs. 6 S. 2 hessSOG; § 26 Abs. 1 S. 2 mvSOG; § 30 Abs. 1 S. 2 ndsSOG; § 26 Abs. 5 S. 2 rpPOG; § 25 Abs. 2 S. 2 saarlPolG; § 178 Abs. 1 S. 2 shLVwG; § 31 Abs. 2 S. 2 thürPAG), gelten diese Ausnahmen von der unmittelbaren Datenerhebung nur für den Fall, dass die Erhebung bei der betroffenen Person einen unverhältnismäßigen Aufwand erfordern würde oder die Erhebung bei der betroffenen Person die Erfüllung der polizeilichen Aufgaben gefährden oder wesentlich erschweren würde.

7 Z. B. das Stichwort „Bombenanschlag".

8 Zum Begriff des Verwaltungsrechtsverhältnisses *Bull/Mehde*, AllgVerwR, Rn. 287 ff.; *Detterbeck*, AllgVerwR, Rn. 413 ff.; *Gröschner*, Die Verwaltung 30 (1997), S. 301 ff.; *J. Ipsen*, AllgVerwR, Rn. 163 ff.; *Maurer*, AllgVerwR, § 8 Rn. 17 ff.; *Peine*, AllgVerwR, Rn. 264 ff.; *Pietzcker*, Die Verwaltung 30 (1997), S. 281 (282 ff.); *Remmert*, in: Erichsen/Ehlers, AllgVerwR, § 17 Rn. 1 ff.; zu Funktionen des Verwaltungsverhältnisses *von Danwitz*, Die Verwaltung 30 (1997), S. 339 ff.; *Schmidt-Aßmann*, Ordnungsidee, Kapitel 6 Rn. 42 ff.

lichen Ermächtigungsvorschriften zur präventiven Telekommunikationsüberwachung nicht als Entstehungsgrund des Rechtsverhältnisses zwischen der überwachenden Polizeibehörde und den Zielpersonen anzusehen. Denn wenngleich der Tatbestand dieser Ermächtigungsvorschriften erfüllt wird, führt dies nicht unbedingt zu einer Durchführung präventivpolizeilicher E-Mail-Überwachung. Aufgrund des im Polizeirecht beherrschenden Opportunitätsprinzips[9] bzw. des polizeilichen Ermessens kann sich die Polizei entscheiden, ob sie bei der Tatbestandserfüllung eine präventive E-Mail-Überwachung durchführt[10]. Das Rechtsverhältnis zwischen der überwachenden Polizeibehörde und den Zielpersonen wird nur begründet, wenn die Polizei nach ihrer Ermessensentscheidung einen E-Mail-Verkehr überwacht. Insoweit stellt nicht die gesetzliche Ermächtigungsvorschrift zur präventiv-polizeilichen Telekommunikationsüberwachung, sondern die exekutive Maßnahme der präventiv-polizeilichen E-Mail-Überwachung selbst den Entstehungsgrund des Rechtsverhältnisses dar.

Da das von Zielpersonen nicht gewünschte Rechtsverhältnis zur überwachenden Polizeibehörde die Folge eines in Grundrechte eingreifenden Verwaltungshandelns (genauer gesagt: die Folge der Maßnahme präventiv-polizeilicher E-Mail-Überwachung) ist, stellt sich mit Blick auf den Rechtsschutz die Frage nach der Rechtsnatur dieses Verwaltungshandelns (nämlich Rechtsnatur der Maßnahme präventiv-polizeilicher E-Mail-Überwachung). Im Schrifttum wird vertreten, dass polizeiliche Standardmaßnahmen in der Regel Verwaltungsakte darstellten[11]. Auch wenn diese These in aller Regel zutreffend ist, ist die Maßnahme präventiv-polizeilicher E-Mail-Überwachung als eine Ausnahme hiervon anzusehen. Zwar stellt die präventiv-polizeiliche E-Mail-Überwachung ein einseitiges hoheitliches Verwaltungshandeln, das das Merkmal „Einzelfall" erfüllt, dar, jedoch lässt sie sich nicht als Verwaltungsakt qualifizieren, weil es ihr an dem in § 35 S. 1 VwVfG vorgeschriebenen Merkmal „Regelung" fehlt. Das Merkmal „Regelung" im Sinne des § 35 Satz 1 VwVfG bedeutet eine behördliche Wil-

9 Dazu *Götz*, PolR, § 11 Rn. 1 ff.; *Gusy*, PolR, Rn. 391 ff.; *Knemeyer*, PolR, Rn. 125 ff.; *Kugelmann*, PolR, 8. Kapitel Rn. 3 ff.; *Pieroth/Schlink/Kniesel*, PolR, § 10 Rn. 32 ff.; *Schenke* (Fn. 5), Rn. 93 ff.; *Schoch* (Fn. 5), Rn. 101 ff.; *Tettinger/Erbguth/Mann*, BesVerwR, Rn. 531 ff.; *Würtenberger/Heckmann*, PolR BW, Rn. 494 ff.

10 Dabei geht es nicht nur um die Frage, ob die Polizei überhaupt eine präventive Telekommunikationsüberwachung durchführt, sondern auch um die Frage, welche Maßnahme präventiver Telekommunikationsüberwachung (z. B. Telefonüberwachung oder E-Mail-Überwachung) die Polizei ergreift.

11 So *Schenke* (Fn. 5), Rn. 115; a. A. *Gusy* (Fn. 9), Rn. 181; *Heintzen*, DÖV 2005, S. 1038 (1039 f.); *Hoffmann-Riem*, in: Hoffmann-Riem/Schmidt-Aßmann/Voßkuhle, GVwR, Bd. 2, § 33, Rn. 13, 15; *Kopp/Ramsauer*, VwVfG, § 35 Rn. 67a; *Pieroth/Schlink/Kniesel* (Fn. 9), § 12 Rn. 10 f.; *Ruffert*, in: Erichsen/Ehlers, AllgVerwR, § 20 Rn. 26; *Schoch* (Fn. 5), Rn. 193; *Stelkens*, in: Stelkens/Bonk/Sachs, VwVfG, § 35 Rn. 96; *Würtenberger/Heckmann* (Fn. 9), Rn. 315 f.

lenserklärung, die eine verbindliche Rechtsfolge anordnet[12]. Dadurch werden Rechte und/oder Pflichten begründet, geändert, aufgehoben, festgestellt oder verneint[13]. Im Gegensatz zu polizeilichen Standardmaßnahmen, die sich auf die Anordnung von Geboten oder Verboten erstrecken und damit dem Begriff des Verwaltungsakts entsprechen[14], ist die präventiv-polizeiliche E-Mail-Überwachung keine Willenserklärung, sondern nur eine tatsächliche Tätigkeit, durch die die Polizei heimlich im Internet Informationen erhebt. Da die Maßnahme präventiv-polizeilicher E-Mail-Überwachung in das durch Art. 10 Abs. 1 GG geschützte Fernmeldegeheimnis der Zielpersonen eingreift, wird dieser Grundrechtseingriff durch Verwaltungstathandeln verursacht[15]. Bei der Durchführung einer präventiv-polizeilichen E-Mail-Überwachung legt die Polizei den Zielpersonen keine Pflichten auf. Die Mails werden zwar (von der Polizei) mitgelesen, allerdings ist der E-Mail-Verkehr der Zielperson davon abgesehen nicht beeinträchtigt. In diesem Zusammenhang liegt keine Anordnung einer verbindlichen Rechtsfolge vor. Folglich ist die präventiv-polizeiliche E-Mail-Überwachung, die eine der polizeilichen Maßnahmen verdeckter Informationserhebung ist, als Realakt zu qualifizieren[16].

Gegenüber der hier vertretenen Meinung steht *H.-J. Meyer* auf dem Standpunkt, dass der Grundrechtseingriff durch polizeiliche verdeckte Informationserhebung unter dem Aspekt der Formen des Verwaltungshandelns aus einem konkludenten Verwaltungsakt und einem Realakt bestehe[17]. Die als Realakt zu qualifizierende polizeiliche Maßnahme heimlicher Informationserhebung stelle die Ausführung einer vorherigen konkludenten Behör-

12 Vgl. *Bull/Mehde* (Fn. 8), Rn. 689; *Bumke*, in: Hoffmann-Riem/Schmidt-Aßmann/Voßkuhle, GVwR, Bd. 2, § 35, Rn. 22; *Detterbeck* (Fn. 8), Rn. 445 ff.; *Henneke*, in: Knack/Henneke, VwVfG, § 35 Rn. 23; *Ipsen* (Fn. 8), Rn. 336; *Janßen*, in: Obermayer, VwVfG, § 35 Rn. 34 f.; *Kopp/Ramsauer* (Fn. 11), § 35 Rn. 47; *Maurer* (Fn. 8), § 9 Rn. 6; *Peine* (Fn. 8), Rn. 359; *Ruffert* (Fn. 11), § 20 Rn. 24; *Stelkens* (Fn. 11), § 35 Rn. 69, 142; *Ziekow*, VwVfG, § 35 Rn. 24.

13 BVerwGE 77, 268 (271); 80, 355 (364); *Bull/Mehde* (Fn. 8), Rn. 689; *Detterbeck* (Fn. 8), Rn. 447; *Henneke* (Fn. 12), § 35 Rn. 22; *Kopp/Ramsauer* (Fn. 12), § 35 Rn. 47; *Maurer* (Fn. 8), § 9 Rn. 6; *Peine* (Fn. 8), Rn. 360; *Ziekow* (Fn. 12), § 35 Rn. 24.

14 *Kopp/Ramsauer* (Fn. 12), § 35 Rn. 67a.

15 Allerdings sehen das Bundesverwaltungsgericht und das VG Bremen wegen des Eingriffscharakters die Überwachungsmaßnahme als einen Verwaltungsakt an (BVerwGE 87, 23 (25); VG Bremen NVwZ 1989, S. 895). Dem ist nicht zuzustimmen. Denn der Eingriffscharakter kann nicht mit der Verwaltungsaktsqualität gleichgesetzt werden. Nur der Eingriff, der die Voraussetzungen des § 35 VwVfG erfüllt, kann als ein Verwaltungsakt qualifiziert werden (*Alberts*, NVwZ 1989, S. 839 (840)).

16 Vgl. VGH BW, DVBl. 1995, S. 367; VG Freiburg, NVwZ-RR 2006, S. 322 (323); *Deutsch*, Erhebung von Informationen, S. 279 f.; *Kopp/Ramsauer* (Fn. 12), § 35 Rn. 67b; *Schäfer* (Fn. 5), S. 84; *Schenke* (Fn. 5), Rn. 188; *Sodan*, in: Sodan/Ziekow, VwGO, § 42 Rn. 247; *Son*, Heimliche polizeiliche Eingriffe, 2006, S. 96; *Stelkens* (Fn. 11), § 35 Rn. 96; *Vahle*, Aufklärungs- und Observationsmaßnahmen, S. 87; *Würtenberger/Heckmann* (Fn. 9), Rn. 686.

17 *Meyer*, Rechtsfragen, S. 106 f.

denentscheidung (Duldungsverfügung), die das Regelungsmerkmal erfülle, dar[18]. Da die auszuführende Behördenentscheidung konkludent festgesetzt werde, sei eine ausdrückliche Anordnung nicht erforderlich[19]. Obwohl die konkludente Behördenentscheidung, die durch polizeiliche Maßnahme verdeckter Informationserhebung ausgeführt werde, nicht gemäß § 41 VwVfG bekannt gegeben werde, wirke dies nicht hemmend auf die Verwaltungsaktsqualität der konkludenten Behördenentscheidung ein, weil die Bekanntgabe kein Begriffsmerkmal des Verwaltungsakts sei[20]. Die Richtigkeit dieser Gegenmeinung erscheint allerdings zweifelhaft. Zwar wird der „konkludente Verwaltungsakt", der in § 37 Abs. 2 Satz 1 VwVfG („in anderer Weise" im Gegensatz zu mündlich, schriftlich und elektronisch) eine positivrechtliche Grundlage finden kann[21], in Rechtsprechung und Literatur überwiegend anerkannt[22], allerdings ist die in jedem Realakt enthaltene konkludente Duldungsverfügung, die der Ausgangspunkt der Argumentation von *H.-J. Meyer* ist, zu verneinen. Denn sonst verliert der Realakt seine selbstständige Bedeutung als Form des Verwaltungshandelns[23]. Heutzutage stellt die sog. „stillschweigende in einem Realakt enthalten Duldungsverfügung" vielmehr nur ein Relikt aus der Zeit, als der Rechtsweg zu Verwaltungsgerichten nur für den Eingriff durch einen Verwaltungsakt eröffnet war, dar[24]. Auch wenn die „konkludente Duldungsverfügung", die von *H.-J. Meyer* als Verwaltungsakt eingestuft wird, angenommen werden kann, kann sie jedenfalls nicht für den Eingriff durch die präventiv-polizeiliche E-Mail-Überwachung gelten. Denn die Annahme, dass der polizeiliche Eingriff durch die heimliche Informationserhebung aus einem konkludenten Verwaltungsakt und einem diesen konkludenten Verwaltungsakt ausführenden Realakt bestehe[25], kann die Frage, zu welchem Verhalten die polizeiliche „stillschweigende Verfügung" die Zielpersonen verpflichtet, nicht klären. Falls – wie *H.-J. Meyer* behauptet – der „konkludente Verwaltungsakt" inhaltlich eine „stillschweigende Duldungsverfügung" ist und die Maßnahme der polizeilichen E-Mail-Überwachung einen Realakt, der eine vorherige Behördenentscheidung mit Regelungscharakter ausführt, darstellt[26], ist der Frage, ob die „stillschweigende Duldungsverfügung" und die „aus-

18 *Meyer* (Fn. 17), S. 107.

19 *Meyer* (Fn. 17), S. 107.

20 *Meyer* (Fn. 17), S. 107.

21 *Henneke* (Fn. 12), § 37 Rn. 20; *Janßen* (Fn. 12), § 37 Rn. 19; *Kopp/Ramsauer* (Fn. 12), § 37 Rn. 19; *Stelkens* (Fn. 11), § 37 Rn. 79; *Ziekow* (Fn. 12), § 37 Rn. 9.

22 Vgl. BVerwGE 26, 161 (164); VGH München NVwZ 1998, S. 1325 (1327); *Detterbeck* (Fn. 8), Rn. 442, 451; *Kopp/Ramsauer* (Fn. 12), § 35 Rn. 22a; *Peine* (Fn. 8), Rn. 345; *Ruffert* (Fn. 11), § 20 Rn. 16; *Stelkens* (Fn. 11), § 35 Rn. 81; *Ziekow* (Fn. 12), § 37 Rn. 9.

23 *Ziekow* (Fn. 12), § 35 Rn. 30.

24 *Deutsch* (Fn. 16), S. 280; *Rachor*, in: Lisken/Denninger, HPolR, F Rn. 46 f.

25 *Meyer* (Fn. 17), S. 106 f.

26 *Meyer* (Fn. 17), S. 107.

zuführende vorherige Behördenentscheidung mit Regelungscharakter" identisch sind, nicht auszuweichen. Wenn sich diese Frage bejahen lässt, ist sehr schwer nachzuvollziehen, wieso die Polizei durch eine Überwachungsmaßnahme die Duldungspflicht der Bürger, die der Regelungsinhalt der vorherigen Behördenentscheidung ist, durchsetzen kann[27]. Wenn sich diese Frage umkehrt verneinen lässt, ist die „stillschweigende Duldungsverfügung" unabhängig von der „vorherigen Behördenentscheidung mit Regelungscharakter". In dieser Situation ist schwer einzusehen, welchen Anordnungsinhalt die „vorherige Behördenentscheidung mit Regelungscharakter" hat. Insoweit ist das von *H.-J. Meyer* vorgebrachte Argument nicht überzeugend. Die Fragwürdigkeit der These von *H.-J. Meyer* besteht ferner darin, dass seine Auffassung die Bedeutung des § 41 VwVfG ignoriert[28]. Obwohl die Bekanntgabe kein Begriffsmerkmal des Verwaltungsakts ist, ist sie die Voraussetzung der rechtlichen Existenz eines Verwaltungsakts[29]. Das Verwaltungshandeln, das die Voraussetzungen des § 35 VwVfG erfüllt, ist (noch) kein extern wirksamer Verwaltungsakt, wenn es noch nicht bekannt gegeben wird[30]. Da bei der Durchführung einer präventiv-polizeilichen E-Mail-Überwachung die „konkludente Willenserklärung der Behörde", die nach *H.-J. Meyer* eine „stillschweigende Duldungsverfügung" ist, nicht bekannt gegeben wird, ist es sehr fraglich, ob eine durch einen „noch nicht existenten Verwaltungsakt" begründete Duldungspflicht der Zielpersonen aufgenommen werden darf. Unter rechtsstaatlichen Gesichtspunkten wird niemand durch einen noch nicht bekanntgegebenen Verwaltungsakt verpflichtet[31].

Nach der obigen Erörterung ist festzuhalten, dass die Rechtsnatur präventiv-polizeilicher E-Mail-Überwachung ein Realakt ist. Unzutreffend ist die Auffassung, dass der polizeiliche Überwachungseingriff aus einem konklu-

27 Es ist unmöglich, dass eine Duldungspflicht der Bürger durch eine polizeiliche Überwachungsmaßnahme durchgesetzt werden kann. Falls die Polizei die E-Mail-Überwachung als eine Maßnahme zur Durchsetzung einer (stillschweigenden) Duldungspflicht von Bürgern ansieht, ist der Verhältnismäßigkeitsgrundsatz verletzt, weil eine solche polizeiliche Maßnahme nicht geeignet ist.

28 Vgl. *Deutsch* (Fn. 16), S. 280; *Rachor* (Fn. 24), F Rn. 50; *Schenke* (Fn. 5), Rn. 188; *Sodan* (Fn. 16), § 42 Rn. 247.

29 *Bull/Mehde* (Fn. 8), Rn. 741; *Detterbeck* (Fn. 8), Rn. 537; *Henneke* (Fn. 12), § 41 Rn. 30; *Kopp/Ramsauer* (Fn. 12), § 41 Rn. 17; *Liebetanz*, in: Obermayer, VwVfG, § 41 Rn. 12; *Maurer* (Fn. 8), § 9 Rn. 65; *Peine* (Fn. 8), Rn. 539 f.; *Ruffert* (Fn. 11), § 21 Rn. 15; *Stelkens* (Fn. 11), § 41 Rn. 3; *Ziekow* (Fn. 12), § 41 Rn. 20.

30 *Maurer* (Fn. 8), § 9 Rn. 65; *Peine* (Fn. 8), Rn. 540. Ein solches Verwaltungshandeln ist kein nichtiger Verwaltungsakt, sondern ein „Nicht(verwaltungs)akt" (BVerwG NVwZ 1987, S. 330; VG Gera LKV 2003, S. 571 (573); VGH Mannheim NVwZ 1991, S. 1995 (1996); OVG Münster NJW 2004, S. 3730 (3731); *Detterbeck* (Fn. 8), Rn. 551; *Liebetanz* (Fn. 29), § 41 Rn. 74).

31 *Maurer* (Fn. 8), § 9 Rn. 65.

denten Verwaltungsakt und einem Realakt, der die Ausführung dieses konkludenten Verwaltungsakts darstelle, bestehe.

2. Aufenthaltsort und Wohnsitz der Zielpersonen als maßgebliche Faktoren für die Begründung des Rechtsverhältnisses zum Rechtsträger der überwachenden Polizeibehörde?

Ob sich die Zielpersonen im Landesgebiet, innerhalb dessen die überwachende Polizeibehörde die Gefahrenabwehraufgabe erfüllen muss, befinden, ist kein entscheidender Faktor für die Durchführung präventiv-polizeilicher E-Mail-Überwachung, durch die ein Rechtsverhältnis zwischen der überwachenden Polizeibehörde und den Zielpersonen begründet wird. Aus der Sicht der örtlichen Zuständigkeit[32] kann die Polizei- oder Ordnungsbehörde dann eine Maßnahme zur Gefahrenabwehr ergreifen, wenn eine Gefahr in ihrem Dienstbezirk auftritt[33]. Wo sich der Aufenthaltsort oder Wohnsitz der Person, die die abzuwehrende Gefahr verursacht, befindet, ist rechtlich nicht maßgebend[34]. Deswegen hängt die Frage, ob die Polizeibehörde zur Gefahrenabwehr auf die E-Mail-Kommunikation der Zielpersonen zugreifen kann, nicht davon ab, ob sich die Zielpersonen im Landesbereich aufhalten, wo die überwachende Polizeibehörde die Aufgabe der Gefahrenabwehr wahrnehmen muss, sondern davon, ob die abzuwehrende Gefahr, die die Zielpersonen verursacht, im Dienstbezirk der überwachenden Polizeibehörde auftritt, ab. In diesem Zusammenhang ist die Polizeibehörde auch zuständig dafür, den E-Mail-Verkehr von Zielpersonen, die sich in einem anderen Bundesland oder im Ausland befinden, aber polizeiliche Schutzgüter im Dienstbezirk der überwachenden Polizeibehörde verletzen[35], zu überwachen.

Ein weiterer Grund dafür, dass der Aufenthaltsort oder der Wohnsitz der Zielpersonen keine Rolle für die örtliche Zuständigkeit für die Durchführung einer präventiv-polizeilichen E-Mail-Überwachung spielt, besteht darin, dass nicht die Zielperson als solche, sondern die E-Mail-Kommuni-

32 Zur örtlichen Zuständigkeit der Polizeibehörde *Götz* (Fn. 9), § 12 Rn. 8; *Kugelmann* (Fn. 9), 2. Kapitel Rn. 56 f.; *Pieroth/Schlink/Kniesel* (Fn. 9), § 6 Rn. 12; *Schenke* (Fn. 5), Rn. 458 f.; *Schoch* (Fn. 5), Rn. 264; *Tettinger/Erbguth/Mann* (Fn. 9), Rn. 664 f.; *Würtenberger/Heckmann* (Fn. 9), Rn. 232 ff.

33 Vgl. § 68 Abs. 1 bwPolG; § 75 Abs. 1 bbgPolG; § 4 Abs. 1 bbgOBG; § 78 Abs. 1 bremPolG; §§ 100 Abs. 1, 101 Abs. 1 S. 2 hessSOG; § 5 Abs. 1 mvSOG; § 100 Abs. 1 ndsSOG; § 7 Abs. 1 nwPOG; § 4 Abs. 1 nwOBG; §§ 78 Abs. 1, 91 Abs. 1 rpPOG; § 81 Abs. 1 saarlPolG; § 70 Abs. 1 sächsPolG; § 88 Abs. 1 saSOG; § 166 Abs. 1 shLVwG; § 4 Abs. 3 thürOBG. Der Polizeivollzugsdienst kann im gesamten Gebiet eines Bundeslandes örtlich zuständig sein (vgl. § 75 S. 1 bwPolG; Art. 3 Abs. 1 bayPAG; § 6 berlASOG; § 101 Abs. 1 S. 1 hessSOG; § 8 Abs. 1 mvSOG; § 86 saarlPolG; § 76 sächsPolG; § 169 Abs. 1 shLVwG; § 3 Abs. 1 thürPOG).

34 Vgl. *Schoch* (Fn. 5), Rn. 264.

35 Beispielsweise verschwören sich landesexterne Terroristen durch die E-Mail-Kommunikation, im Dienstbezirk der überwachenden Polizeibehörde einen Terroranschlag zu verüben.

kation der Zielperson das Überwachungsobjekt darstellt. Auch wenn sich die Zielperson im Bezirk der überwachenden Polizeibehörde befindet, kann die örtliche Zuständigkeit problematisch sein. Dies ist der Fall, wenn die Zielperson, die sich im Dienstbezirk der überwachenden Polizeibehörde aufhält, die E-Mail-Dienste eines ausländischen oder landesfremden Providers, der keinen Firmensitz im örtlichen Zuständigkeitsgebiet der überwachenden Polizeibehörde hat, nutzt. Zwar wird der Internetanschluss, der sich als eine technische Voraussetzung eines E-Mail-Verkehrs ansehen lässt, von einem deutschen Anbieter des Internetzugangs, dessen Firmensitz im örtlichen Zuständigkeitsbereich der überwachenden Polizeibehörde liegt, angeboten, jedoch werden die E-Mails der Zielperson, die das Überwachungsobjekt darstellen, in dieser Konstellation nicht von diesem deutschen Anbieter des Internetzugangs, sondern von einem ausländischen oder landesfremden Provider der E-Mail-Dienste in der virtuellen Welt übertragen[36]. Dies bedeutet, dass die präventiv-polizeiliche E-Mail-Überwachung nur dann erfolgreich sein kann, wenn das Überwachungsprogramm (E-Mail-Filter) in einem E-Mail-Knoten, der sich im Ausland oder in einem anderen Bundesland befindet, eingesetzt wird. Infolgedessen hat die Antwort auf die Frage, ob der E-Mail-Provider, der den Zielpersonen die E-Mail-Dienste anbietet, einen Firmensitz im Bundesland, in dem die überwachende Polizeibehörde zuständig ist, hat, vielmehr – gegenüber der Frage nach dem Sitz der Zielperson – eine größere Bedeutung[37].

3. Rechtsposition der Zielpersonen gegenüber der überwachenden Polizeibehörde

Hinsichtlich seines Inhalts ist das Verwaltungsrechtsverhältnis zwischen der überwachenden Polizeibehörde und den Zielpersonen eine Informationsbeziehung zwischen Staat und Bürger. In dieser Informationsbeziehung werden die privaten Daten ohne oder gegen den Willen der Zielpersonen von der Polizei erhoben[38]. Insoweit befinden sich die Zielpersonen in einem asymmetrischen Rechtsverhältnis[39], in dem sie den polizeilichen Zugriff auf ihre E-Mail-Kommunikation dulden müssen. Dieses asymmetrische Rechtsverhältnis wird, wie bereits ausgeführt wurde, durch die als Realakt einzustufende Maßnahme präventiv-polizeilicher E-Mail-Über-

36 Ein Anbieter des Internetzugangs bietet oft auch E-Mail-Dienste an. Für eine zu überwachende E-Mail-Kommunikation können der Anbieter des Internetzugangs und der E-Mail-Dienste allerdings nicht identisch sein, wenn die Zielperson auf die Nutzung der E-Mail-Dienste, die der Provider des Internetzugangs anbietet, verzichtet.

37 Dazu siehe unten B II.

38 *Gusy*, in: Hoffmann-Riem/Schmidt-Aßmann/Voßkuhle, GVwR, Bd. 2, § 23, Rn. 75.

39 Zur Asymmetrie des Rechtsverhältnisses zwischen der überwachenden Polizeibehörde und den betroffenen Nutzern der E-Mail-Dienste siehe unten A III 1.

wachung begründet. Diese polizeiliche Maßnahme, die eine (asymmetrische) Informationsbeziehung zwischen Staat und Bürger begründet, darf durchgeführt werden, wenn die Voraussetzungen der polizei- und ordnungsgesetzlichen Ermächtigungsvorschriften zur Telekommunikationsüberwachung erfüllt werden. Zunächst muss eine Gefahr für die polizeilichen Schutzgüter vorliegen. Außerdem muss die Verantwortlichkeit der Zielpersonen bejaht werden, sonst stellt die Begründung des Rechtsverhältnisses zwischen der überwachenden Polizeibehörde und den Zielpersonen die Folge des polizeilichen Notstands dar. Die nachfolgend zu untersuchende Frage, ob die Zielpersonen für die Gefahr im Sinne des Polizeirechts verantwortlich sind, betrifft die Einordnung der Zielpersonen im polizeirechtlichen Zurechnungssystem.

a) Zielpersonen im Bereich klassischer Gefahrenabwehr als Störer und Nichtstörer

aa) Bedeutung der polizeirechtlichen Zurechnung

Das rechtsstaatliche Polizeirecht verlangt, dass sich die polizeiliche Maßnahme grundsätzlich gegen die Personen, die für die Gefahr verantwortlich sind, richten muss (Störer)[40]. Nur im Fall des polizeilichen Notstands[41] kann sich der polizeiliche Eingriff ausnahmsweise gegen die nichtverantwortlichen Personen (Nichtstörer) richten[42]. Störer im Sinne des Polizeirechts ist, wer eine Gefahr für die öffentliche Sicherheit oder Ordnung durch sein Verhalten (Handeln oder Unterlassen) oder durch den Zustand seiner Sachen verursacht. Insoweit umfasst der Begriff des Störers sowohl Verhaltensstörer wie auch Zustandsstörer[43]. Neben der konkreten Verantwortlichkeit im System polizeirechtlicher Gefahrzurechnung ist eine allgemeine Nichtstörungspflicht, nach der jede Person keine Gefahr durch ihr Verhalten oder durch den Zustand ihrer Sachen verursachen darf, anzuerkennen[44]. Diese allgemeine Nichtstörungspflicht, die für jeden Einzelnen

40 *Götz* (Fn. 9), § 9 Rn. 1; *Gusy* (Fn. 9), Rn. 329; *Knemeyer* (Fn. 9), Rn. 318; *Kugelmann* (Fn. 9), 6. Kapitel Rn. 1 f.; *Pieroth/Schlink/Kniesel* (Fn. 9), § 9 Rn. 2; *Schenke* (Fn. 5), Rn. 228; *Schoch* (Fn. 5), Rn. 117; *Würtenberger/Heckmann* (Fn. 9), Rn. 427.

41 Zu Voraussetzungen des polizeilichen Notstands *Götz* (Fn. 9), § 10 Rn. 4; *Gusy* (Fn. 9), Rn. 38 ff.; *Pieroth/Schlink/Kniesel* (Fn. 9), § 9 Rn. 74; *Schoch* (Fn. 5), Rn. 180 ff.

42 *Denninger*, in: Lisken/Denninger, HPolR, E Rn. 138; *Götz* (Fn. 9), § 10 Rn. 1 ff.; *Gusy* (Fn. 9), Rn. 380; *Knemeyer* (Fn. 9), Rn. 347; *Kugelmann* (Fn. 9), 6. Kapitel Rn. 81; *Pieroth/Schlink/Kniesel* (Fn. 9), § 9 Rn. 2, 74; *Schenke* (Fn. 5), Rn. 312; *Schoch* (Fn. 5), Rn. 117; *Würtenberger/Heckmann* (Fn. 9), Rn. 427.

43 *Denninger* (Fn. 42), E Rn. 70; *Gusy* (Fn. 9), Rn. 329; *Kugelmann* (Fn. 9), 6. Kapitel Rn. 6; *Pieroth/Schlink/Kniesel* (Fn. 9), § 9 Rn. 2; *Schenke* (Fn. 5), Rn. 229; *Schoch* (Fn. 5), Rn. 118; *Würtenberger/Heckmann* (Fn. 9), Rn. 427. Nach *M. Hollands* ist eine deutliche Trennung zwischen Verhaltensstörer wie auch Zustandsstörer unmöglich (*Hollands*, Gefahrenzurechnung, S. 65 ff.).

44 BVerwGE 125, 325 (332 f.); *Breuer*, NVwZ 1987, S. 751 (755); *Denninger* (Fn. 42), E Rn. 69; *Götz* (Fn. 9), § 9 Rn. 6; *Griesbeck*, Kostentragungspflicht, S. 82 ff.; *Hollands* (Fn. 43), S. 121 ff.;

gilt, wird durch die im Einzelfall durchgeführte polizeiliche Maßnahme, die sich gegen einen bestimmten Verantwortlichen richtet, konkretisiert[45]. Im Schrifttum wird die Gegenmeinung vertreten, dass eine allgemeine Nichtstörungspflicht nicht anzunehmen sei[46]. Eine solche Gegenauffassung überzeugt nicht. Der Grund dafür ist einfach: Wird die allgemeine Nichtstörungspflicht, die unabhängig von konkreten polizeilichen Maßnahmen ist, nicht akzeptiert, ist schwer einzusehen, wieso die Person, die nach der Gegenmeinung keine Nichtstörungspflicht hat, im Einzelfall für die Verursachung der Gefahr durch ihr Verhalten oder durch den Zustand ihrer Sachen verantwortlich ist und damit den Adressaten einer polizeilichen Maßnahme darstellen kann.

Die Wichtigkeit der polizeirechtlichen Gefahrzurechnung ist bei der Bestimmung der Eingriffsschwelle nicht zu übersehen. Liegt eine Gefahr für die öffentliche Sicherheit oder Ordnung vor, wird die sachliche Eingriffsschwelle erreicht. Dies bedeutet aber nicht, dass der polizeiliche Eingriff bereits wegen des Entstehens einer Gefahr völlig gerechtfertigt werden kann. Denn die polizeiliche Maßnahme darf in Grundrechte der betroffenen Personen nur eingreifen, wenn – abgesehen vom polizeilichen Notstand – ein hinreichender Zusammenhang bzw. eine besondere Nähebeziehung zwischen der Gefahr und dem Betroffenen besteht[47]. Falls es an diesem durch die polizeirechtliche Gefahrenzurechnung begründeten Zusammenhang fehlt, wird die Eingriffsschwelle aus personeller Sicht noch nicht vollständig erreicht.

bb) Verantwortlichkeit der Zielpersonen im Bereich klassischer Gefahrenabwehr

Nach den polizei- und ordnungsgesetzlichen Ermächtigungsvorschriften zur Telekommunikationsüberwachung kann sich die präventiv-polizeiliche E-Mail-Überwachung im Bereich der klassischen Gefahrenabwehr gegen die Personen, die für eine Gefahr verantwortlich sind, richten[48]. In diesem Anwendungskreis ist unstreitig, dass die Person, die eine Gefahr durch ihr Verhalten oder den Zustand ihrer Sachen verursacht und damit dem Störer im Sinne des Polizeirechts entspricht, den Adressaten der präventiv-poli-

---

Martensen, DVBl. 1996 S. 286 (287 f.); *Martensen*, NVwZ 1997, S. 442 (443); *Ossenbühl*, Altlasten, S. 57; *Peine*, DVBl. 1990, S. 733 (736); *Pietzcker*, DVBl. 1984, S. 457 (460); *Schenke* (Fn. 5), Rn. 228; *Schoch* (Fn. 5), Rn. 121.

45 *Schoch* (Fn. 5), Rn. 121.

46 *Kugelmann* (Fn. 9), 6. Kapitel Rn. 5; *Papier*, DVBl. 1996, S. 125 (127); *Pieroth/Schlink/Kniesel* (Fn. 9), § 9 Rn. 4; *Selmer*, in: Hendler/Ibler/Soria, FS Götz, 2005, S. 391 (402).

47 *Denninger* (Fn. 42), E Rn. 70; *Kugelmann* (Fn. 9), 6. Kapitel Rn. 4; *Schoch* (Fn. 5), Rn. 118.

48 § 23a Abs. 1 S. 1 Nr. 1 bwPolG; Art. 34a Abs. 1 S. 1 Nr. 1, Abs. 3 bayPAG; § 33b Abs. 2 S. 1 bbgPolG; § 10a Abs. 1 S. 1 hambGDatPol; § 15a i. V. m. § 6 und 7 hessSOG; § 34a Abs. 1 S. 1 Nr. 1 mvSOG; § 33a Abs. 1 Nr. 1 ndsSOG; § 31 Abs. 1 rpPOG; § 28b Abs. 1 S. 1 saarlPolG; § 185a Abs. 1 S. 2 i. V. m. § 185 Abs. 2 S. 2 shLVwG; § 34a Abs. 3 S. 1 Nr. 1 thürPAG.

zeilichen E-Mail-Überwachung darstellt. Die Durchführung der präventivpolizeilichen E-Mail-Überwachung im Bereich klassischer Gefahrenabwehr geht davon aus, dass die Zielperson die polizeilichen Schutzgüter stört. Aufgrund ihrer genannten polizeirechtlichen Rechtsstellung (Störerqualität) befinden sich die Zielpersonen in einem asymmetrischen informationellen Rechtsverhältnis zur überwachenden Polizeibehörde, in dem die Polizei ohne den Willen der betroffenen Telekommunikationsteilnehmer die E-Mail-Kommunikation des Bürgers beobachtet[49].

Einige polizei- und ordnungsgesetzliche Ermächtigungsvorschriften zur Telekommunikationsüberwachung lassen auch ausdrücklich zu, dass eine präventiv-polizeiliche E-Mail-Überwachung im Bereich klassischer Gefahrenabwehr ausnahmsweise an den Nichtstörer adressiert ist[50]. Wie oben dargelegt wurde, gilt dies nur für den Fall des polizeirechtlichen Notstands. In den Bundesländern, deren polizei- und ordnungsgesetzliche Ermächtigungsvorschriften zur Telekommunikationsüberwachung nicht ausdrücklich die Heranziehung des Nichtverantwortlichen regeln, kann auch ein Nichtstörer nach den allgemeinen Regelungen der Verantwortlichkeit den Adressaten der präventiv-polizeilichen E-Mail-Überwachung darstellen, soweit die Voraussetzungen des polizeilichen Notstands[51] erfüllt sind.

Nach Art. 34a Abs. 3 Satz 1 Nr. 1 bayPAG und § 34a Abs. 1 Satz 1 Nr. 2 mvSOG kann sich die präventiv-polizeiliche E-Mail-Überwachung gegen die Personen, deren Leben oder Gesundheit gefährdet ist, richten. Ein möglicher Anwendungsfall dieser beiden polizei- und ordnungsgesetzlichen Vorschriften im Bereich der E-Mail-Überwachung dürfte die Überwachung der E-Mail-Kommunikation eines (vermissten) Suizidwilligen zur Verhinderung eines Selbstmordes sein[52]. Hier stellt sich die Frage: Entspricht die eine Selbsttötung versuchende Zielperson, deren E-Mail-Verkehr gemäß Art. 34a Abs. 3 Satz 1 Nr. 1 bayPAG oder § 34a Abs. 1 Satz 1 Nr. 2 mvSOG von der Polizei überwacht wird, dem Begriff des Störers oder des Nichtstörers? Die Antwort hängt nicht davon ab, ob das Recht auf Selbsttötung ange-

49 Neben der heimlichen Informationserhebung kann eine asymmetrische Informationsbeziehung zwischen Staat und Bürger zwangsweise auch durch gesetzliche Sanktionen für die Nichterfüllung bestimmter Auskunftspflichten begründet werden (*Gusy* (Fn. 38), Rn. 75).

50 § 23a Abs. 1 S. 1 Nr. 1 bwPolG; § 33b Abs. 2 S. 1 bbgPolG; § 10a Abs. 1 S. 1 hambGDatPol i. V. m. § 10 hambSOG; § 33a Abs. 1 Nr. 2 ndsSOG; § 31 Abs. 1 rpPOG; § 28b Abs. 1 S. 1 saarlPolG.

51 Dazu oben Fn. 41.

52 Bay. LT-Drs. 15/2096, S. 23; MV-LT-Drs. 4/2116, S. 27. Zwar fehlt es in anderen Bundesländern, in denen die präventiv-polizeiliche E-Mail-Überwachung zulässig ist, an einer solchen Regelung, jedoch ist es möglich, dass die Polizei gemäß dem Wortlaut „zur Abwehr einer Gefahr für das Leben einer Person" der gesetzlichen Ermächtigungsvorschriften zum präventiv-polizeilichen Zugriff auf die Telekommunikation eine Maßnahme der E-Mail-Überwachung gegen einen potenziellen Selbstmörder durchführt (vgl. BW-LT-Drs. 14/3156, S. 59).

nommen wird[53]. Maßgebend ist vielmehr, ob sich der Suizidwillige, der die Zielperson präventiv-polizeilicher E-Mail-Überwachung darstellt, in einem die freie Willensbestimmung ausschließenden psychischen Ausnahmezustand befindet. Zur öffentlichen Sicherheit, die ein polizeiliches Schutzgut darstellt, gehört die Unverletzlichkeit individueller Rechte und Rechtsgüter[54]. Zwar ist der Selbsttötungsversuch nach dem StGB nicht strafbar[55], jedoch bedroht er ein hochwertiges individuelles Rechtsgut (Leben). Dies hat zur Folge, dass im Fall des Selbstmordversuchs die sachliche polizeiliche Eingriffsschwelle bereits erreicht wird, weil ein polizeiliches Schutzgut (d. h. öffentliche Sicherheit) in dieser Situation gefährdet ist[56]. Die Entstehung der Gefahr für die öffentliche Sicherheit kann nur verneint werden, wenn man die Selbsttötung als einen zulässigen Verzicht auf das Recht auf Leben (Art. 2 Abs. 2 Satz 1 GG)[57] oder als eine Ausübung des durch Art. 2 Abs. 2 Satz 1 GG geschützten negativen Rechts auf Leben[58] betrachtet. Denn es gibt in dieser Situation kein gefährdetes Recht auf Leben[59]. Von der Auf-

53 Für das verfassungsrechtlich geschützte Recht auf Selbsttötung *Dreier*, in: Dreier, GG, Bd. 1, Art. 1 I, Rn. 157; *Epping*, Grundrechte, Rn. 101; *Fink*, Selbstbestimmung und Selbsttötung, S. 110; *Jarass*, in: Jarass/Pieroth, GG, Art. 2 Rn. 8; *Manssen*, Grundrechte, Rn. 265; *Michael/Morlok*, Grundrechte, Rn. 46, 160; *Murswiek*, in: Sachs, GG, Art. 2 Rn. 211; *Pieroth/Schlink*, Grundrechte, Rn. 419; *Sachs*, in: Stern, Staatsrecht, Bd. IV/1, S. 148 f.; *Schulze-Fielitz*, in: Dreier, GG, Bd. 1, Art. 2 II, Rn. 32; *Sodan*, in: Sodan, GG, Art. 2 Rn. 21; *Zippelius/Würtenberger*, Staatsrecht, § 24 Rn. 2; dagegen VG Karlsruhe, NJW 1988, S. 1536 (1537); *Czinczoll*, Solidaritätspflichten, S. 127 f.; *Leisner*, in: Leisner/Görlich, Recht auf Leben, S. 38; *von Münch*, in: Stödter, FS Ipsen, S. 113 (127); *Starck*, in: von Mangoldt/Klein/Starck, GG, Bd. 1, Art. 2 Rn. 192; *Sturm*, in: Leibholz/Faller/Mikat/Reis, FS Geiger, S. 173 (188); *Wilms/Jäger*, ZRP 1988, S. 41 (42).

54 *Götz* (Fn. 9), § 4 Rn. 3; *Gusy* (Fn. 9), Rn. 79; *Kugelmann* (Fn. 9), 4. Kapitel Rn. 48; *Pieroth/Schlink/Kniesel* (Fn. 9), § 8 Rn. 3; *Schenke* (Fn. 5), Rn. 53; *Schoch* (Fn. 5), Rn. 66; *Würtenberger/Heckmann* (Fn. 9), Rn. 399.

55 Die strafrechtliche Sanktion des § 323c StGB richtet sich nicht gegen den Selbstmord, sondern gegen die unterlassene Hilfeleistung.

56 VG Karlsruhe, NJW 1988, S. 1536 (1537); *Knemeyer*, VVDStRL 35 (1977), S. 221 (253 f.). Nach *U. Di Fabio* stellt die Selbsttötung auch eine Gefahr für die öffentliche Ordnung dar (*Di Fabio*, in: Maunz/Dürig, GG, Art. 2 Abs. 2 Rn. 48).

57 Dazu *Fink* (Fn. 53), S. 126 ff.

58 *Fink* (Fn. 53), S. 110; *Michael/Morlok* (Fn. 53), Rn. 46, 160; *Pieroth/Schlink* (Fn. 53), Rn. 419; a. A. *Di Fabio* (Fn. 56), Art. 2 Abs. 2 Rn. 47; *Epping* (Fn. 53), Rn. 101; *Hellermann*, Negative Seite der Freiheitsrechte, S. 136 f.; *Jarass* (Fn. 53), Art. 2 Rn. 81; *Kunig*, in: von Münch/Kunig, GG, Bd. 1, Art. 2 Rn. 50; *Lorenz*, in: Isensee/Kirchhof, HStR, Bd. 6, 2. Aufl., § 128, Rn. 62; *Müller-Terpitz*, in: Isensee/Kirchhof, HStR, Bd. 7, § 147 Rn. 38; *Sachs* (Fn. 53), S. 148; *Schulze-Fielitz* (Fn. 53), Art. 2 II Rn. 32; *Sodan* (Fn. 53), Art. 2 Rn. 21; *Starck* (Fn. 58), Art. 2 Rn. 192; *Zippelius/Würtenberger* (Fn. 58), § 24 Rn. 2.

59 Diese beiden Auffassungen (Verzicht auf das Recht auf Leben oder Ausübung des negativen Rechts auf Leben) führen jedoch zu Schwierigkeiten bei der Rechtfertigung der polizeilichen Maßnahmen zur Unterbindung eines Suizides. Folgt man diesen beiden Meinungen, gefährdet ein Suizidversuch das durch Art. 2 Abs. 2 S. 1 GG geschützte Rechtsgut überhaupt nicht.

fassung, dass der Selbstmord einen zulässigen Verzicht auf das Recht auf Leben oder die Ausübung des negativen Rechts auf Leben darstellt, abgesehen, ist der Suizidwillige für die Gefahr des Lebens verantwortlich, weil diese Gefahr unmittelbar durch seinen Selbsttötungsversuch verursacht wird. Die Antwort auf die Frage, ob sich die Selbsttötung als eine Ausübung des Grundrechts (Art. 2 Abs. 1 GG) ansehen lässt[60], spielt keine Rolle für die Verantwortlichkeit des Suizidwilligen. Dieser Faktor (d. h. Recht auf Selbsttötung aus Art. 2 Abs. 1 GG) betrifft nach der Theorie der unmittelbaren Verursachung, die sich als das Zurechnungsprinzip des Polizeirechts ansehen lässt[61], nicht den Kausalzusammenhang zwischen der Entstehung der Gefahr und dem Verhalten des Suizidwilligen. Deswegen ist der Suizidwillige, dessen E-Mail-Verkehr gemäß Art. 34a Abs. 3 Satz 1 Nr. 1 bayPAG oder § 34a Abs. 1 Satz 1 Nr. 2 mvSOG überwacht wird, als Störer einzustufen. Nicht zu übersehen ist allerdings, dass sich die meisten Selbstmörder in einer die freie Willensentschließung ausschließenden psychischen Ausnahmesituation befinden[62]. Dieser psychische Ausnahmezustand ist mit der Naturgewalt, die das individuelle Rechtsgut bedroht, gleichzustellen[63]. Insoweit ist der Suizidwillige, der sich in einer psychischen Ausnahmesituation befindet, nicht für die Gefahr, die durch seinen Selbstmordversuch verursacht wird, verantwortlich[64]. Er ist in dieser Konstellation kein

Falls keine Gefahr im Sinne des Polizeirechts vorliegt, ist es schwer einzusehen, wieso die polizeilichen Maßnahmen zur Unterbindung einer Selbsttötung durchgeführt werden dürfen, ohne dass die Eingriffsschwelle erreicht wird. Wenn man im Vergleich dazu die Ansicht, dass das Recht auf Selbsttötung aus Art. 2 Abs. 1 GG hergeleitet werden könne (*Murswiek* (Fn. 58), Art. 2 Rn. 211; *Jarass* (Fn. 53), Art. 2 Rn. 8; *Sachs* (Fn. 53), S. 148 f.; *Schulze-Fielitz* (Fn. 53), Art. 2 II Rn. 32; *Sodan* (Fn. 53), Art. 2 Rn. 21; *Zippelius/Würtenberger* (Fn. 58), § 24 Rn. 2), vertritt, lässt sich die Gefahr für das Recht auf Leben, die durch eine Ausübung des Grundrechts des Art. 2 Abs. 1 GG verursacht wird, bejahen. Aufgrund der aus Art. 2 Abs. 2 S. 1 GG hergeleiteten staatlichen Schutz*pflicht*, nach der der Schutz des Suizidwilligen vor sich selbst verfassungsrechtlich geboten ist (*Knemeyer* (Fn. 56), S. 221 (253 f.)), *muss* die Polizei beim Fall des Selbsttötungsversuchs einschlägige Maßnahmen ergreifen. Auch wenn eine solche staatliche Schutzpflicht nicht anerkannt wird, *darf* die Polizei aufgrund staatlicher Schutz*befugnis*, die sich aus Art. 2 Abs. 2 S. 1 GG ergibt (*Jarass* (Fn. 53), Art. 2 Rn. 100), eine Maßnahme zur Unterbrechung der Selbsttötung durchführen.

60 Dafür *Manssen* (Fn. 53), Rn. 265; *Murswiek* (Fn. 58), Art. 2 Rn. 211; *Jarass* (Fn. 53), Art. 2 Rn. 8; *Sachs* (Fn. 53), S. 148 f.; *Schulze-Fielitz* (Fn. 53), Art. 2 II Rn. 32; *Sodan* (Fn. 53), Art. 2 Rn. 21; *Zippelius/Würtenberger* (Fn. 58), § 24 Rn. 2.

61 Vgl. OVG Hamburg, NJW 2000, S. 2600 (2601); VGH Kassel, NJW 1999, S. 3650 (3652); *Götz* (Fn. 9), § 9 Rn. 10 ff.; *Gusy* (Fn. 9), Rn. 335 ff.; *Kugelmann* (Fn. 9), 6. Kapitel Rn. 27 ff.; *Pieroth/Schlink/Kniesel* (Fn. 9), § 9 Rn. 42 ff.; *Schenke* (Fn. 5), Rn. 242; *Schoch* (Fn. 5), Rn. 128 f.; *Würtenberger/Heckmann* (Fn. 9), Rn. 441 ff.; kritisch *Denninger* (Fn. 42), E Rn. 77 ff.

62 Vgl. *Knemeyer* (Fn. 56), S. 221 (254 f.) mit Fn. 111.

63 *Waechter*, NVwZ 1997, S. 729 (736).

64 In der Literatur wird überwiegend vertreten, dass die Frage, ob sich der potenzielle Selbstmörder in einem psychischen Ausnahmezustand befindet, auf der Ebene der Feststellung einer Gefahr zu behandeln sei (*Denninger* (Fn. 42), E Rn. 32; *Götz* (Fn. 9), § 4 Rn. 32; *Gusy*

Störer, sondern Nichtstörer[65]. Die nach Art. 34a Abs. 3 Satz 1 Nr. 1 bayPAG oder § 34a Abs. 1 Satz 1 Nr. 2 mvSOG durchgeführte E-Mail-Überwachung, die sich gegen einen Suizidwilligen richtet, ist als eine polizeiliche Maßnahme, die im polizeilichen Notstand ergriffen wird, zu bewerten, soweit sich der Suizidwillige in einem psychischen Ausnahmelage befindet[66].

Im Bereich der klassischen Gefahrenabwehr kann sich die präventiv-polizeiliche E-Mail-Überwachung gemäß Art. 34a Abs. 1 Satz 1 Nr. 3 bayPAG und § 34a Abs. 3 Satz 1 Nr. 3 thürPAG gegen „Kontakt- und Begleitpersonen" richten, soweit Tatsachen die Annahme rechtfertigen, dass sie für die in Art. 34a Abs. 1 Satz 1 Nr. 1 bayPAG und § 34a Abs. 3 Satz 1 Nr. 1 thürPAG genannten Personen bestimmte oder von diesen herrührende Mitteilungen entgegennehmen oder weitergeben sowie die in Art. 34a Abs. 1 Satz 1 Nr. 1 bayPAG und § 34a Abs. 3 Satz 1 Nr. 1 thürPAG genannten Per-

(Fn. 9), Rn. 86; *Knemeyer* (Fn. 56), S. 221 (254f.); *Kugelmann* (Fn. 9), 4. Kapitel Rn. 55; *Pieroth/Schlink/Kniesel* (Fn. 9), § 8 Rn. 31; *Schenke* (Fn. 5), Rn. 57; *Schoch* (Fn. 5), Rn. 74; *Würtenberger/Heckmann* (Fn. 9), Rn. 402). Diese (herrschende) Auffassung, die sich auf den Zusammenhang zwischen der Entstehung einer Gefahr und dem Defizit freier Willensbestimmung konzentriert, erscheint auf den ersten Blick plausibel. Bei näherem Hinsehen verliert sie jedoch ihre Überzeugungskraft. Denn die Frage, ob eine Gefahr für die öffentliche Sicherheit vorliegt, hängt nicht davon ab, ob der Selbsttötungsversuch auf einer freien Willensbestimmung basiert. Auch in der Konstellation, dass der Suizidwillige ein Recht auf Selbsttötung aus Art. 2 Abs. 1 GG hat und er sich nicht in einem psychischen Ausnahmezustand befindet, ist die Entstehung einer Gefahr, die durch seinen Selbstmordversuch verursacht wird, dogmatisch nicht zu verneinen, weil das Leben des Suizidwilligen, dessen Unverletzlichkeit dem Begriff der öffentlichen Sicherheit entspricht, in dieser Situation bereits gefährdet ist. Für das Bestehen einer Gefahr ist die psychische Lage des Suizidwilligen also nicht entscheidend. Vielmehr stellt die psychische Situation des Suizidwilligen einen maßgeblichen Faktor für die Bestimmung der Verantwortlichkeit des Suizidwilligen dar. D. h., die psychische Situation des Suizidwilligen ist nicht auf der Ebene der Gefahr, sondern auf der Ebene der Verantwortlichkeit zu diskutieren.

65 A. A. *Götz* (Fn. 9), § 14 Rn. 35.

66 Wird die psychische Ausnahmesituation des Suizidwilligen festgestellt, liegt eine Ermessensreduzierung auf Null für die Polizei vor. Denn in dieser Situation *muss* (nicht nur *kann*) die Polizei wegen der aus Art. 2 Abs. 2 S. 1 GG hergeleiteten Schutz*pflicht* (nicht nur Schutz*befugnis*) eine solche Selbsttötung, die von der psychischen Ausnahmesituation des Suizidwilligen ausgeht, unterbrechen (*Di Fabio* (Fn. 56), Art. 2 Abs. 2 Rn. 48; *Murswiek* (Fn. 58), Art. 2 Rn. 210; *Sachs* (Fn. 53), S. 149; *Schulze-Fielitz* (Fn. 53), Art. 2 II Rn. 85; *Zippelius/Würtenberger* (Fn. 58), § 24 Rn. 3). Zu beachten ist, dass die Ermessensreduzierung auf Null, deren Grundlage die staatliche Schutzpflicht aus Art. 2 Abs. 2 S. 1 GG ist, nur für das Entschließungsermessen gilt. Zur Rettung einer Person, die aufgrund psychischer Ausnahmesituation die Selbsttötung versucht, kann die Polizei auch andere rechtmäßige Maßnahmen wählen (Auswahlermessen). Allerdings wird das polizeiliche Auswahlermessen begrenzt, wenn die polizei- und ordnungsgesetzlichen Ermächtigungsvorschriften die Subsidiarität der Telekommunikationsüberwachung gegenüber anderen polizeilichen Standardmaßnahmen regeln (vgl. Art. 34a Abs. 1 S. 2 bayPAG; § 34a Abs. 1 S. 2 mvSOG; § 28b Abs. 1 saarlPolG; § 34a Abs. 3 S. 1 thürPAG).

sonen ihre Kommunikationseinrichtungen benutzen werden[67]. Die Einordnung der hier genannten Kontakt- und Begleitpersonen, die sich nicht im Vorfeld der Gefahr, sondern im Bereich klassischer Gefahrenabwehr befinden, ist aus der Sicht polizeirechtlicher Gefahrenzurechnung zu klären. Unter dem Aspekt der unmittelbaren Verursachung sind die Kontakt- und Begleitpersonen nicht für die Gefahr, die die Polizei durch eine präventive E-Mail-Überwachung abwehrt, verantwortlich, weil diese abzuwehrende Gefahr bereits unmittelbar von den in Art. 34a Abs. 1 Satz 1 Nr. 1 bayPAG und § 34a Abs. 3 Satz 1 Nr. 1 thürPAG genannten Personen verursacht wird. Es gibt keine Kausalbeziehung zwischen der Gefahrentstehung und der Kontakttätigkeit. Infolgedessen stellen die in Art. 34a Abs. 1 Satz 1 Nr. 3 bayPAG und § 34a Abs. 3 Satz 1 Nr. 3 thürPAG genannten Kontakt- und Begleitpersonen keinen Störer, sondern Nichtstörer dar. Art. 34a Abs. 1 Satz 1 Nr. 3 bayPAG und § 34a Abs. 3 Satz 1 Nr. 3 thürPAG können (im Bereich klassischer Gefahrenabwehr) nur angewendet werden, wenn die Voraussetzungen des polizeilichen Notstands (Art. 10 Abs. 1 und 2 bayPAG und § 10 Abs. 1 und 2 thürPAG) erfüllt sind. Die in Art. 34a Abs. 1 Satz 1 Nr. 3 bayPAG und § 34a Abs. 3 Satz 1 Nr. 3 thürPAG genannten Kontakt- und Begleitpersonen (im Bereich klassischer Gefahrenabwehr) können nur im Fall des polizeilichen Notstands ausnahmsweise die Adressaten der Maßnahme zur präventiven E-Mail-Überwachung sein. Aufgrund der Nachrangigkeit des polizeilichen Notstands[68] ist vor allem zu beachten, dass ein präventiv-polizeilicher Zugriff auf die E-Mail-Kommunikation der in Art. 34a Abs. 1 Satz 1 Nr. 3 bayPAG und § 34a Abs. 3 Satz 1 Nr. 3 thürPAG genannten Kontakt- und Begleitpersonen (im Bereich der klassischen Gefahrenabwehr) nur zulässig ist, wenn die Gefahr durch die Heranziehung des Verantwortlichen nicht erfolgreich abgewehrt werden kann.

b) Zielpersonen im Vorfeld der Gefahr als Nichtstörer

Das durch die als Realakt zu qualifizierende Maßnahme präventiv-polizeilicher E-Mail-Überwachung begründete Verwaltungsrechtsverhältnis zwischen der überwachenden Polizeibehörde und den Zielpersonen kann auch im Vorfeld der Gefahr entstehen, wenn die polizei- und ordnungsgesetzlichen Vorschriften die präventive Telekommunikationsüberwachung im Gefahrenvorfeld zulassen[69]. Sowohl die „potenziellen Straf-

67 Obwohl in Baden-Württemberg und Brandenburg die Kontakt- und Begleitpersonen die Adressaten der präventiv-polizeilichen E-Mail-Überwachung darstellen können, kann diese polizeiliche Überwachungsmaßnahme gegen Kontakt- und Begleitpersonen nur im Vorfeld der Gefahr durchgeführt werden (vgl. § 23a Abs. 1 S. 1 Nr. 2 Buchstabe b und c bwPolG; § 33b Abs. 2 S. 2 bbgPolG).

68 *Götz* (Fn. 9), § 10 Rn. 6.

69 Vgl. § 23a Abs. 1 S. 1 Nr. 2 bwPolG; Art. 34a Abs. 1 S. 1 Nr. 2 und 3 bayPAG; § 33b Abs. 1 und Abs. 2 S. 2 in Verbindung mit § 33a Abs. 1 Nr. 2 bbgPolG; § 28b Abs. 1 S. 1 Nr. 2 saarlPolG; § 34a Abs. 3 S. 1 Nr. 2 und 3 thürPAG.

täter“ als auch die „Kontakt- und Begleitpersonen“ können die Zielpersonen der präventiv-polizeilichen E-Mail-Überwachung zur Verhütung künftiger Straftaten sein[70]. Hier wird die Frage aufgeworfen, ob die Zielpersonen der präventiv-polizeilichen E-Mail-Überwachung, die im Vorfeld der Gefahr durchgeführt wird, dem Begriff des Störers entsprechen.

Dabei ist davon auszugehen, dass im Vorfeld der Gefahr (noch) keine konkrete Gefahr besteht[71]. Deswegen betrifft die polizeiliche Maßnahme, die im Vorfeld der Gefahr durchgeführt wird, wie im 3. Kapitel bereits ausgeführt wurde, nur eine geringere hinreichende Wahrscheinlichkeit des Schadenseintritts[72]. Die polizeiliche Maßnahme im Vorfeld der Gefahr bezieht sich nur auf die Vorsorge für eine künftige Gefahr[73]. Die polizeiliche Vorfeldbefugnis besagt keine Erosion der Gefahrenschwelle[74], sondern die Absenkung der polizeilichen Eingriffsschwelle: Die Polizei kann durch die Ausübung ihrer Vorfeldbefugnis in Grundrechte eingreifen, ohne dass eine Gefahr besteht. Da im Vorfeld der Gefahr noch keine Gefahr besteht, fehlt im Vorfeld der Gefahr ein Verursacher der Gefahr[75]. In diesem Zusammenhang ist festzuhalten, dass sich der Adressat der polizeilichen Vorfeldmaßnahme nicht als Störer ansehen lässt[76]. Die Zielpersonen der präventiv-polizeilichen E-Mail-Überwachung, die im Vorfeld der Gefahr durchgeführt wird, sind Nichtstörer. Diese Konsequenz gilt sowohl für die potenziellen Straftäter als auch für die Kontakt- und Begleitpersonen[77]. Die polizei- und ordnungsgesetzlichen Ermächtigungsvorschriften zur Telekommunikationsüberwachung im Vorfeld der Gefahr stellen spezielle Voraussetzungen eines qualifizierten polizeilichen Notstands dar.

---

70 Im Saarland kann sich die präventiv-polizeiliche E-Mail-Überwachung im Vorfeld der Gefahr gemäß § 28b Abs. 1 S. 1 Nr. 2 saarlPolG nur gegen potenzielle Straftäter richten. Kontakt- und Begleitpersonen sind keine Adressaten der präventiv-polizeilichen E-Mail-Überwachung im Vorfeld der Gefahr.

71 *Möstl*, DVBl. 2007, S. 581 (586).

72 Siehe 3. Kapitel Fn. 61.

73 *Kugelmann*, DÖV 2003, S. 781 (789). Insoweit kann die polizeiliche Maßnahme im Vorfeld der Gefahr als Risikobekämpfung betrachtet werden (*Schulze-Fielitz*, in: Horn, FS Schmitt Glaeser, S. 407 (411)). Zu beachten ist, dass eine solche Risikobekämpfung auf die vorsorgende Vermeidung zukünftiger Gefahren abzielt. Demzufolge betrifft die polizeiliche Vorfeldmaßnahme keine neuartige Risikoverwaltung, sondern die Gefahrenabwehrverwaltung (*Möstl* (Fn. 71), S. 581 (585), a. A. *Schulze-Fielitz*, in: Hoffmann-Riem/Schmidt-Aßmann/Voßkuhle, GVwR, Bd. 1, § 12, Rn. 28 f.).

74 A. A. *Trute*, in: Erbguth/Müller/Neumann, GS Jeand'Heur, S. 403 (406 ff.).

75 *Möstl* (Fn. 71), S. 581 (586).

76 Vgl. *Horn*, DÖV 2003, S. 746 (749); *Möstl* (Fn. 71), S. 581 (586); *Würtenberger/Heckmann* (Fn. 9), Rn. 183.

77 Es wird im Schrifttum vertreten, dass die Kontakt- und Begleitpersonen weder Störer noch Nichtstörer seien (*Pieroth/Schlink/Kniesel* (Fn. 9), § 14 Rn. 135). Folgt man dieser Auffassung, ist die Einordnung der Kontakt- und Begleitpersonen aus Sicht polizeirechtlicher Zurechnung unklar.

II. Rechtsverhältnis zwischen dem Rechtsträger der überwachenden Polizeibehörde und den betroffenen Nichtzielpersonen

1. Weiter Kreis der betroffenen Nichtzielpersonen

a) Kreis der potenziell betroffenen Nichtzielpersonen

Bei der Durchführung einer präventiv-polizeilichen Telekommunikationsüberwachung können Nichtzielpersonen aufgrund technischer Gründe betroffen sein. Dies wird auch vom Gesetzgeber durch die „Unvermeidbarkeitsklausel", die sich in polizei- und ordnungsgesetzlichen Ermächtigungsvorschriften zur Telekommunikationsüberwachung findet[78], anerkannt. Zu betonen ist, dass der Eingriff in das Fernmeldegeheimnis mitbetroffener Dritter, zu dem die präventiv-polizeiliche Telekommunikationsüberwachung führt, nicht durch die „Unvermeidbarkeitsklausel" in Polizei- und Ordnungsgesetzen entfällt. Die „Unvermeidbarkeitsklausel" bezieht sich auch nicht auf die Frage nach der Verfassungsmäßigkeit des Zugriffs auf die Telekommunikation der betroffenen Nichtzielpersonen. Vielmehr besagt die „Unvermeidbarkeitsklausel" nur, dass die Möglichkeit des Eingriffs in Grundrechte mitbetroffener Dritter, der sich aus technischem Grund ergibt, keine negative Voraussetzung der Durchführung einer präventiv-polizeilichen Telekommunikationsüberwachung darstellt.

Die Zahl der betroffenen Nichtzielpersonen (Streubreite) ist im Fall der präventiv-polizeilichen E-Mail-Überwachung besonders groß. Da sich die E-Mail-Kommunikation auf den Informationsaustausch zwischen dem Absender und dem Empfänger per E-Mail erstreckt, ist ein E-Mail-Verkehr ohne Kommunikationspartner unmöglich. Dies hat zur Folge, dass der Zugriff auf die E-Mail-Kommunikation der Zielperson zugleich in das Fernmeldegeheimnis ihres Kommunikationspartners eingreift, obwohl er nicht Adressat der Überwachungsmaßnahme ist. Im Vergleich zur Telefon-Kommunikation, die sich in der Regel auf ein Gespräch zwischen zwei Personen bezieht, können mehr Kommunikationspartner bei einem E-Mail-Verkehr vorliegen, weil eine E-Mail gleichzeitig an mehrere Empfänger abgeschickt werden kann. Je mehr Empfänger die überwachte E-Mail der Zielperson erhalten, umso größer ist der Kreis der betroffenen Nichtzielpersonen, deren Fernmeldegeheimnis (Art. 10 Abs. 1 GG) durch die E-Mail-Überwachung beeinträchtigt wird.

Die Streubreite bei der präventiv-polizeilichen E-Mail-Überwachung erschöpft sich nicht in den Kommunikationspartnern der Zielperson. Setzt die Polizei im E-Mail-Knoten, über den die E-Mails der Zielperson übertra-

78 Vgl. § 23a Abs. 1 S. 4 bwPolG; Art. 34a Abs. 2 S. 2 bayPAG; § 33b Abs. 4 S. 1 bbgPolG; § 10a Abs. 1 S. 2 hambGDatPol; § 34a Abs. 1 S. 3 mvSOG; § 33a Abs. 2 S. 3 ndsSOG; § 31 Abs. 2 S. 1 rpPOG; § 28b Abs. 1 S. 4 saarlPolG; § 185a Abs. 3 S. 4 i. V. m. § 185 Abs. 4 shLVwG; § 34a Abs. 3 S. 3 thürPAG.

gen werden, ein Überwachungsprogramm (E-Mail-Filter) zur Ermittlung der „gefährlichen E-Mail" ein, können alle E-Mail-Datenpakete, die über den kontrollierten E-Mail-Knoten übermittelt werden, dadurch von der Polizei abgefangen und analysiert werden. Dies ist technisch unvermeidbar. Denn um nach dem einschlägigen Stichwort, das z. B. eine bestimmte E-Mail-Adresse betrifft, die „gefährliche E-Mail" aufzuklären, muss der E-Mail-Filter alle über den kontrollierten E-Mail-Knoten übertragenen E-Mails „öffnen" und ihre Inhalte „lesen"[79]. Diese technische Unvermeidbarkeit führt zu dem Risiko, dass die E-Mails unbeteiligter Dritter bei der Durchführung einer präventiv-polizeilichen E-Mail-Überwachung von der Polizei mitgelesen werden können. Dies ist der Fall, wenn die E-Mails unbeteiligter Dritter wegen eines technischen Fehlers des im kontrollierten E-Mail-Knoten eingesetzten Überwachungsprogramms die automatische Prüfung nicht bestehen und damit an den Rechner der überwachenden Polizeibehörde weitergeleitet werden. Berücksichtigt man, dass unzählige E-Mail-Datenpakete über den kontrollierten E-Mail-Knoten übertragen werden können, lässt sich nicht leugnen, dass die Zahl potenziell betroffener unbeteiligter Dritter bei der Durchführung einer präventiv-polizeilichen E-Mail-Überwachung besonders hoch ist.

b) Grundrechtseingriff und seine Rechtfertigung

Wenn die E-Mails der Nichtzielpersonen, die die Kommunikationspartner der Zielpersonen sind, aufgrund technischer Gründe unvermeidbar durch eine präventiv-polizeiliche E-Mail-Überwachung von der Polizei mitgelesen werden, schädigt diese polizeiliche Überwachungsmaßnahme, die sich gegen die in den Polizei- und Ordnungsgesetzen vorgeschriebenen Zielpersonen richtet, auch die Vertraulichkeit der E-Mail-Kommunikation Dritter. Darüber hinaus werden die personenbezogenen Daten unbeteiligter Dritter betroffen. Denn die E-Mail-Adressen (und ggf. die IP-Adressen) unbeteiligter Dritter, die dem Begriff der personenbezogenen Daten entsprechen[80], werden aufgrund des Zugriffs auf den Telekommunikationsvorgang auch von der Polizei erhoben. Da das Fernmeldegeheimnis eine spezielle Garantie gegenüber dem Recht auf informationelle Selbstbestimmung (Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 GG) darstellt, führt die Erhebung der personenbezogenen Daten Dritter im laufenden Vorgang einer E-Mail-Kommunikation auch zum Eingriff in den Schutzbereich des Art. 10 Abs. 1 GG[81].

79 Vgl. *Schmidt*, CR 2003, S. 839; *Spindler/Ernst*, CR 2004, S. 437 (438); *Willer/Hoppen*, CR 2007, S. 610 (615).

80 OLG Bamberg, MMR 2006, S. 481 (482 f.); LG Berlin, MMR 2007, S. 799; AG Wuppertal, MMR 2008, S. 632; *Czychowski/Nordemann*, NJW 2008, S. 3095 (3096); *Dammann*, in: Simitis, BDSG, § 3 Rn. 10; *Jandt*, MMR 2006, S. 652 (654); *Roßnagel*, NZV 2006, S. 281 (282); *Warg*, MMR 2006, S. 77 (80 f.).

81 BVerfGE 100, 313 (358); 107, 299 (312); 110, 33 (53); 113, 348 (364); BVerfGE 100, 313 (359); BVerfG, NJW 2007, S. 351 (354 f.); *Gusy* in: von Mangoldt/Klein/Starck, GG, Bd. 1, Art. 10

Obwohl die E-Mails der Nichtzielpersonen, die nicht die Kommunikationspartner der Zielpersonen sind, in den meisten Fällen die virtuelle Prüfung bestehen können und damit nicht an den Rechner der Polizeibehörde weitergeleitet werden, kann man nicht leugnen, dass die im kontrollierten E-Mail-Knoten durchgeführte automatische Prüfung einen Zugriff auf den Telekommunikationsvorgang unbeteiligter Dritter darstellt. Deswegen führt eine solche automatische Prüfung zum Eingriff in das Fernmeldegeheimnis unbeteiligter Dritter, deren E-Mails über den kontrollierten E-Mail-Knoten übertragen werden. Zwar greift die elektronische Datenerfassung nach dem Urteil des Bundesverfassungsgerichts vom 11. 3. 2008 nicht in den Schutzbereich des Rechts auf informationelle Selbstbestimmung ein, wenn das automatische Filtern von Daten unverzüglich vorgenommen wird und negativ ausfällt sowie zusätzlich rechtlich und technisch gesichert ist, dass die Daten anonym bleiben und sofort spurenlos und ohne die Möglichkeit, einen Personenbezug herzustellen, gelöscht werden[82], jedoch kann diese Ablehnung des Grundrechtseingriffs nicht in gleicher Weise für den Fall der virtuellen Prüfung der über den kontrollierten E-Mail-Knoten übermittelten E-Mails, die von unbeteiligten Dritten abgeschickt werden, gelten. Denn ob die im kontrollierten E-Mail-Knoten automatisch geprüften E-Mails anonym bleiben, spielt keine Rolle für die Frage, ob in das Fernmeldegeheimnis, das den Vorgang der E-Mail-Kommunikation schützt, eingegriffen wird. Sofern die Übertragung der E-Mails unbeteiligter Dritter durch den von der überwachenden Polizeibehörde eingesetzten E-Mail-Filter elektronisch kontrolliert wird, liegt ein Eingriff in das Fernmeldegeheimnis unbeteiligter Dritter vor.

Damit stellt sich die Frage, ob die bei der Durchführung einer präventivpolizeilichen E-Mail-Überwachung aus technischen Gründen verursachte Erhebung der Daten unbeteiligter Dritter, die in das Fernmeldegeheimnis unbeteiligter Dritter eingreift, verfassungsrechtlich zulässig ist. Durch den Beschluss der 1. Kammer des Zweiten Senats erklärte das Bundesverfassungsgericht, dass das Recht unbeteiligter Dritter auf informationelle Selbstbestimmung aus Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 GG durch die Erhebung und die kurzzeitige Speicherung der IMSI- und IMEI-Kennung ihrer Mobiltelefone bei Einsatz eines „IMSI-Catchers“ gemäß § 100i StPO nicht verletzt werde[83]. In Bezug auf die Rechtfertigung habe die staatliche Informationserhebung durch den Einsatz eines „IMSI-Catchers“ zur wirksamen Strafverfolgung einerseits formelle Verfassungsmäßigkeit, weil sie in § 100i StPO ihre gesetzliche Grundlage finden könne[84]. Andererseits ent-

Rn. 103; *Hermes*, in: Dreier, GG, Bd. 1, Art. 10 Rn. 94; *Jarass* (Fn. 53), Art. 10 Rn. 2; *Löwer*, in: von Münch/Kunig, GG, Bd. 1, Art. 10 Rn. 55; *Pagenkopf*, in: Sachs, GG, Art. 10 Rn. 52.

82 BVerfGE 120, 378 (399).

83 BVerfG, NJW 2007, S. 351.

84 BVerfG, NJW 2007, S. 351 (355).

spreche sie materiell dem Grundsatz der Verhältnismäßigkeit[85]. In diesem Punkt führe die Durchführung der Maßnahme nach § 100i StPO nur zu einem geringen Eingriff in die Grundrechte Dritter. Denn die erhobenen technischen Kommunikationsdaten würden automatisch und anonym abgeglichen und unverzüglich gelöscht[86]. Dadurch seien unbeteiligte Dritte nicht identifizierbar[87]. Da die Eingriffsintensität winzig sei, sei der Verzicht auf die Benachrichtigung mitbetroffener Dritter verhältnismäßig[88]. Der Verzicht auf die Benachrichtigung könne die Vertiefung des Grundrechtseingriffs vermeiden, weil für die Benachrichtigung eine Ermittlung des Personenbezugs erforderlich sei. Die Ermittlung des Personenbezugs führe jedoch zur Identität des mitbetroffenen Dritten, die den Eingriff in das Grundrecht mitbetroffener Dritter intensiviere[89]. Obwohl dieser Beschluss des Bundesverfassungsgerichts die Verfassungsmäßigkeit des § 100i StPO betrifft, kann sein Fazit – teilweise – auch für die präventiv-polizeiliche E-Mail-Überwachung gelten. Der im kontrollierten E-Mail-Knoten eingesetzte E-Mail-Filter, der nach einem einschlägigen Stichwort die „gefährliche E-Mail" ermitteln kann, muss zwar alle über den kontrollierten E-Mail-Knoten übermittelte E-Mails „öffnen" und ihre Inhalte „lesen", allerdings geht es dabei nur um eine virtuelle Überprüfung[90]. Für die überwachende Polizeibehörde sind diese vom E-Mail-Filter (virtuell) geöffneten und überprüften E-Mails unbeteiligter Dritter nicht lesbar[91]. Bei der virtuel-

85 BVerfG, NJW 2007, S. 351 (355 f.).

86 BVerfG, NJW 2007, S. 351 (356). Aus diesem Grund sieht das Bundesverfassungsgericht die Erhebung der Kommunikationsdaten durch den Einsatz eines „IMSI-Catchers" als einen geringen und rechtfertigbaren Eingriff in das Recht unbeteiligter Dritter auf informationelle Selbstbestimmung an, wenn die erhobenen Daten unbeteiligter Dritter automatisch und anonym abgeglichen und unverzüglich gelöscht werden. Im Gegensatz dazu führt die automatische Erfassung des Kraftfahrzeugkennzeichens nach dem Urteil des Bundesverfassungsgerichts vom 11. 3. 2008 allerdings nicht zum Eingriff in das Recht auf informationelle Selbstbestimmung, wenn die Daten nach der Erfassung anonym bleiben und sofort spurenlos gelöscht werden (BVerfGE 120, 378 (399)). Die Beurteilung der Frage, ob ein automatischer und anonymer Datenabgleich zu einem Eingriff in das Recht auf informationelle Selbstbestimmung unbeteiligter Dritter führt, erfolgt damnach nicht einheitlich.

87 BVerfG, NJW 2007, S. 351 (356).

88 BVerfG, NJW 2007, S. 351 (356).

89 BVerfG, NJW 2007, S. 351 (356).

90 *Spindler/Ernst* (Fn. 79), S. 437 (438).

91 Trotz der physischen Unlesbarkeit ist der Eingriff in das Fernmeldegeheimnis eines unbeteiligten Dritten durch virtuelle Überprüfung seiner E-Mail nicht abzuleugnen. Art. 10 Abs. 1 GG schützt sowohl die Vertraulichkeit des Kommunikationsinhalts als auch die Vertraulichkeit des Kommunikationsvorgangs (BVerfGE 67, 157 (172); 85, 386 (396); *Gusy* (Fn. 81), Art. 10 Rn. 45; *Hermes* (Fn. 81), Art. 10 Rn. 41; *Hufen*, Grundrechte, § 17 Rn. 7; *Löwer* (Fn. 81), Art. 10 Rn. 22; *Manssen*, Grundrechte, Rn. 529; *Stern*, in: Stern, Staatsrecht, Bd. IV/1, S. 226 f.). Durch die virtuelle Öffnung und Überprüfung der E-Mails liegt ein Zugriff auf den Telekommunikationsvorgang bereits vor. Ob die betroffenen Inhalte der Telekommunikation

len Überprüfung durch einen E-Mail-Filter, die in das Fernmeldegeheimnis unbeteiligter Dritter eingreift, sind die mitbetroffenen Dritten nicht identifizierbar. Da die Inhalte der E-Mails unbeteiligter Dritter in der Regel keine E-Mail-Adresse der Zielperson enthalten, können die E-Mails unbeteiligter Dritter in den meisten Fällen die virtuelle Überprüfung überstehen, ohne dass eine Kopie der (virtuell) überprüften E-Mail auf den Server der überwachenden Polizeibehörde übertragen wird. Deswegen liegt ein Zugriff auf die E-Mail-Kommunikation unbeteiligter Dritter zwar vor, jedoch werden im Normalfall die Daten unbeteiligter Dritter nicht von der Polizei erhoben. Eine Kopie der virtuell überprüften E-Mail unbeteiligter Dritter wird nur ausnahmsweise auf den Server der überwachenden Polizeibehörde übertragen, wenn ein technischer Fehler bei der virtuellen Überprüfung aufgetreten ist oder die unbeteiligten Dritten die Kommunikationspartner der Zielperson sind oder die Inhalte der E-Mails unbeteiligter Dritter aus anderen Gründen die E-Mail-Adresse der Zielperson enthalten. Folglich führt die virtuelle Überprüfung durch den Einsatz eines E-Mail-Filters, die einen Zugriff auf die E-Mail-Kommunikation unbeteiligter Dritter darstellt, zu einem geringen Eingriff in das durch Art. 10 Abs. 1 GG geschützte Grundrecht unbeteiligter Dritter. Unter dem Aspekt des Verhältnismäßigkeitsgrundsatzes kann der Eingriff in das Grundrecht unbeteiligter Dritter nach der Abwägung zwischen dem großen Gewicht der durch die präventiv-polizeiliche Telekommunikationsüberwachung geschützten Rechtsgüter und dem niedrigen Eingriffsgrad für unbeteiligte Dritte verfassungsrechtlich gerechtfertigt werden.

2. Realakt als Entstehungsgrund des Rechtsverhältnisses

Wenn die E-Mails der Nichtzielpersonen über den kontrollierten E-Mail-Knoten übertragen und durch den von der Polizeibehörde (mit Hilfe des Diensteanbieters) eingesetzten E-Mail-Filter virtuell überprüft werden, liegt ein Rechtsverhältnis zwischen diesen Nichtzielpersonen und der überwachenden Polizeibehörde vor. Dieses Rechtsverhältnis wird durch die Maßnahme der präventiv-polizeilichen E-Mail-Überwachung begründet. Wie oben bereits dargelegt wurde, ist die Maßnahme der präventiv-polizeilichen E-Mail-Überwachung mangels Regelungscharakters als Realakt zu qualifizieren[92]. Mithin ist die Entstehung des Rechtsverhältnisses zwischen

anonym sind, ist für die Entstehung eines Eingriffs in das Fernmeldegeheimnis nicht relevant. Denn wie oben bereits dargelegt wurde, besteht ein Eingriff in das Fernmeldegeheimnis unbeteiligter Dritter, sofern die Übertragung der E-Mails unbeteiligter Dritter durch den von der überwachenden Polizeibehörde eingesetzten E-Mail-Filter elektronisch kontrolliert wird. Verfassungsrechtlich spielt die Anonymität der betroffenen Telekommunikationsinhalte insoweit nur eine Rolle für die Reduzierung des Eingriffsgewichts (vgl. BVerfGE 100, 313 (376); 107, 299 (320)).

92 Siehe oben A I 1.

betroffenen Nichtzielpersonen und der überwachenden Polizeibehörde eine Folge des Grundrechtseingriffs, der durch einen Realakt erfolgt.

3. Rechtsposition der betroffenen Nichtzielpersonen gegenüber der überwachenden Polizeibehörde

Da unbeteiligte Dritte keine Gefahr verursachen, werden sie von der überwachenden Polizeibehörde nicht als Zielpersonen der Überwachungsmaßnahme angesehen. Insoweit ist es unumstritten, dass die unbeteiligten mitbetroffenen Dritten Nichtstörer sind.

Zwar sind unbeteiligte Dritte als Nichtstörer zu betrachten, jedoch ist der Fall, dass die E-Mails unbeteiligter Dritter durch den im kontrollierten E-Mail-Knoten eingesetzten E-Mail-Filter virtuell geöffnet und überprüft werden, keine Inanspruchnahme nichtverantwortlicher Dritter. Denn sie (unbeteiligte Dritte) sind keine rechtlichen Adressaten der polizeilichen Überwachungsmaßnahme. Vielmehr sind sie nur tatsächlich mitbetroffen. Der Grund dafür, dass das durch Art. 10 Abs. 1 GG geschützte Fernmeldegeheimnis mitbetroffener unbeteiligter Dritter durch die präventiv-polizeiliche E-Mail-Überwachung beeinträchtigt wird, besteht nicht darin, dass sie bei der Durchführung einer präventiv-polizeilichen E-Mail-Überwachung als Verantwortliche in Anspruch genommen werden, sondern darin, dass ein solcher Zugriff auf ihre E-Mail-Kommunikation aus technischen Gründen unvermeidbar ist.

III. Asymmetrie des Rechtsverhältnisses zwischen der überwachenden Polizeibehörde und den betroffenen Nutzern der E-Mail-Dienste

1. Übermächtige Informationsbefugnis der Polizei und Schwierigkeit des Rechtsschutzes im laufenden Überwachungsverhältnis

Das Rechtsverhältnis zwischen der überwachenden Polizeibehörde und den betroffenen Nutzern der E-Mail-Dienste ist asymmetrisch. Bei der Durchführung einer präventiv-polizeilichen E-Mail-Überwachung hat die überwachende Polizeibehörde eine übermächtige Informationsbefugnis. Aufgrund der gesetzlichen Ermächtigung kann die Polizeibehörde gegen oder ohne den Willen der Zielpersonen die E-Mail-Kommunikation überwachen. Ferner können auch die unbeteiligten Dritten, deren E-Mails über den kontrollierten E-Mail-Knoten übertragen werden, wegen der technischen Unvermeidbarkeit durch die präventiv-polizeiliche E-Mail-Überwachung betroffen sein. Angesichts der polizeilichen Informationserhebung durch eine E-Mail-Überwachung, die in das durch Art. 10 Abs. 1 GG geschützte Grundrecht eingreift, müssen die betroffenen Nutzer der

E-Mail-Dienste die übermächtige Informationsbefugnis der Polizei dulden[93].

Die Asymmetrie des Rechtsverhältnisses zwischen der überwachenden Polizeibehörde und den betroffenen Nutzern der E-Mail-Dienste verschärft sich dadurch, dass der Rechtsschutz der betroffenen Nutzer der E-Mail-Dienste im laufenden Überwachungsverhältnis schwierig ist. Wie bereits ausgeführt wurde, ist die Maßnahme der E-Mail-Überwachung, die den Entstehungsgrund des Rechtsverhältnisses zwischen der überwachenden Polizeibehörde und den betroffenen Nutzern der E-Mail-Dienste darstellt, als Realakt zu qualifizieren. Dies erschwert die Möglichkeit, dass der Grad des Grundrechtseingriffs durch eine Verfahrensbeteiligung reduziert werden kann. Unter dem Begriff des Verwaltungsverfahrens versteht man die Tätigkeit der Behörde im Zusammenhang mit dem Erlass eines Verwaltungsakts oder dem Abschluss eines öffentlich-rechtlichen Vertrags[94]. Die Durchführung eines Realakts entspricht nicht dem Verwaltungsverfahren im Sinne des § 9 VwVfG, obwohl er Außenwirkung hat[95]. Da die betroffenen Nutzer der E-Mail-Dienste keine Beteiligten am Verwaltungsverfahren im Sinne des § 9 VwVfG sind, haben sie keine Verfahrensrechte nach dem VwVfG wie etwa das Recht auf Anhörung, das Recht auf Akteneinsicht usw. Unter Berücksichtigung der europäischen Rechtsentwicklung wird im Schrifttum vertreten, dass die §§ 9 ff. VwVfG zumindest analog anzuwenden seien, wenn die Verwaltung zielgerichtete belastende Realakte vornehme[96]. Dieser Vorschlag für die Ausweitung des Anwendungsbereichs der Verfahrensrechte ist unter dem Aspekt der „Grundrechtsverwirklichung durch Verfahren“[97] bedeutsam. Da es in den Polizei- und Ordnungsgesetzen kaum Regelungen für das Verfahrensrecht der betroffenen Nutzer der E-Mail-Dienste gibt, lassen sich die Landesverwaltungsverfahrensgesetze oder §§ 9 ff. VwVfG analog anwenden. In der Sache ist eine solche analoge Anwendung der verwaltungsverfahrensgesetzlichen Vorschriften bei der Durchführung der präventiv-polizeilichen E-Mail-Überwachung jedoch unmöglich. Der Grund dafür, dass sich die Telekommunikationsüber-

93 Vgl. *Gusy* (Fn. 38), Rn. 75.

94 Vgl. Legaldefinition des § 9 VwVfG. Die Landesverwaltungsverfahrensgesetze entsprechen § 9 VwVfG.

95 Vgl. *Clausen*, in: Knack/Henneke, VwVfG, § 9 Rn. 2; *Kopp/Ramsauer* (Fn. 11), § 9 Rn. 4; *Maurer* (Fn. 8), § 19 Rn. 2; *Schmitz*, in: Stelkens/Bonk/Sachs, VwVfG, § 9 Rn. 86; *Ziekow* (Fn. 12), § 9 Rn. 8.

96 *Kopp/Ramsauer* (Fn. 11), § 9 Rn. 5; *Stelkens* (Fn. 11), § 35 Rn. 44.

97 Dazu BVerfGE 69, 315 (355); *Bethge*, NJW 1982, S. 1 ff.; *Dreier* (Fn. 53), Vorb. Rn. 105 f.; *Jarass* (Fn. 53), Vorb. vor Art. 1 Rn. 11 ff.; *Maurer* (Fn. 8), § 19 Rn. 9; *Ossenbühl*, in: Müller/Rhinow/Schmid/Wildhaber, FS Eichenberger, S. 183 ff.; *Sachs*, in: Sachs, GG, vor Art. 1 Rn. 34; *Schmidt-Aßmann*, in: Merten/Papier, HGR, Bd. 2, 2006, § 45, Rn. 4 ff.; *Schoch*, Die Verwaltung 25 (1992), S. 21 (26); *Steiner*, NZS 2002, S. 113 ff.; *Zippelius/Würtenberger* (Fn. 58), § 17 Rn. 42 ff.

wachung als eine effektive Maßnahme zur Gefahrenabwehr ansehen lässt, besteht darin, dass diese polizeiliche Maßnahme verdeckt ist[98]. Zur Erhaltung der Heimlichkeit der E-Mail-Überwachung wird auf die Benachrichtigung der Zielpersonen im Laufe der Durchführung der Überwachungsmaßnahme verzichtet. Wie oben dargelegt wurde, gilt der Verzicht auf die Benachrichtigung von Betroffenen auch für die unbeteiligten mitbetroffenen Dritten, andernfalls verstärkt die für die Benachrichtigung notwendige Identifizierung von unbeteiligten mitbetroffenen Dritten die Intensität des Eingriffs. In einem laufenden Überwachungsverhältnis sind die betroffenen Nutzer der E-Mail-Dienste völlig ahnungslos. Die Heimlichkeit der Überwachung sperrt die Möglichkeit der Verfahrensbeteiligung. Bemerkenswert ist, dass sich die Nachteile, die die Heimlichkeit der Überwachung den betroffenen Nutzern der E-Mail-Dienste bringt, nicht im Defizit am Rechtsschutz, der durch die (analoge) Ausübung der im VwVfG oder in den Landesverwaltungsverfahrensgesetzen vorgeschriebenen Verfahrensrechte gewährleistet wird, erschöpfen. Vielmehr zeigt sich die Asymmetrie des Rechtsverhältnisses zwischen der überwachenden Polizeibehörde und den betroffenen Nutzern der E-Mail-Dienste auch im Bereich des durch das Gerichtsverfahren sichergestellten Rechtsschutzes. Mangels der Benachrichtigung der Zielpersonen im Laufe der Durchführung einer Überwachungsmaßnahme kann der gerichtliche Rechtsschutz gegen den polizeilichen Zugriff auf die E-Mail-Kommunikation der Zielpersonen erst dann verwirklicht werden, wenn die Überwachungsmaßnahme endet. Anders ausgedrückt: Die Möglichkeit der Anrufung des Verwaltungsgerichts liegt tatsächlich erst dann vor, nachdem das durch Art. 10 Abs. 1 GG geschützte Grundrecht der Zielpersonen beeinträchtigt worden ist. Aus der Sicht des effektiven Rechtsschutzes, den Art. 19 Abs. 4 GG erfordert[99], wäre die Eröffnung des Verwaltungsrechtswegs nach der Beendigung der Überwachungsmaßnahme zu spät[100].

2. Richtervorbehalt als effektive Verfahrenssicherung?

Wegen dieser Schwierigkeiten des Rechtsschutzes im Rechtsverhältnis zwischen der überwachenden Polizeibehörde und den betroffenen Nutzern der E-Mail-Dienste ist nach Verfahrenssicherungen zu suchen. Denn der „Grundrechtsschutz durch Verfahren", der zu den objektiven Grundrechts-

98 *Schäfer* (Fn. 5), S. 166.

99 Dazu BVerfGE 94, 166 (194); 107, 395 (405); 117,71 (122); *Degenhart*, in: Isensee/Kirchhof, HStR, Bd. 5, 3. Aufl., § 115, Rn. 6, 17, 29; *Hofmann*, in: Schmidt-Bleibtreu/Hofmann/Hopfauf, GG, Art. 19 Rn. 29; *Huber*, in: von Mangoldt/Klein/Starck, GG, Bd. 1, Art. 19 Rn. 453 ff.; *Jarass* (Fn. 53), Art. 19 Rn. 50; *Krebs*, in: von Münch/Kunig, GG, Bd. 1, Art. 19 Rn. 62; *Sachs* (Fn. 97), Art. 19 Rn. 143 ff.; *Schulze-Fielitz* (Fn. 53), Art. 19 IV Rn. 80 f., 106 ff.; *Sodan* (Fn. 53), Art. 19 Rn. 31.

100 Vgl. *Gusy*, ZRP 2003, S. 275.

gehalten gehört[101], darf nicht hinter die Heimlichkeit der Überwachungsmaßnahme zurücktreten. Jedenfalls ist die Entscheidung über die Durchführung einer präventiv-polizeilichen E-Mail-Überwachung nicht ohne begleitende Kontrolle zu treffen. Dabei kann die Anordnung der Überwachung unter Richtervorbehalt, die in polizei- und ordnungsgesetzlichen Ermächtigungsvorschriften zur Telekommunikationsüberwachung vorgeschrieben wird[102], die Rechtswidrigkeit der Entscheidung über den Zugriff auf die E-Mail-Kommunikation verhindern[103]. Zu betonen ist, dass die richterliche Anordnung keine Maßnahme, die auf unmittelbare Rechtswirkung nach außen gerichtet ist, darstellt. Der „Adressat" der richterlichen Anordnung ist nicht die Zielperson, sondern die überwachende Polizeibehörde.

Der Grund, dass der Richtervorbehalt als eine wirksame verfahrensrechtliche Vorkehrung betrachtet werden kann[104], besteht in der persönlichen und sachlichen Unabhängigkeit der Richter[105]. Da Art. 10 GG die Frage, welches Organ über den Eingriff in das Fernmeldegeheimnis entscheiden kann, nicht regelt, hat der Gesetzgeber dahingehend einen Ermessensspielraum[106]. Allerdings ist der Spielraum des Gesetzgebers nicht grenzenlos. Aufgrund der Heimlichkeit der Eingriffe in das Fernmeldegeheimnis erklärte das Bundesverfassungsgericht, dass Art. 10 GG eine Kontrolle durch unabhängige und an keine Weisung gebundene staatliche Organe

101 *Zippelius/Würtenberger* (Fn. 58), § 17 Rn. 42.

102 § 23a Abs. 3 S. 1 bwPolG; Art. 34c Abs. 1 i. V. m. Art. 34 Abs. 4 S. 1 bayPAG; § 33b Abs. 5 S. 1 bbgPolG; § 10c Abs. 1 S. 1 hambGDatPol; § 15a Abs. 4 S. 1 hessSOG; § 34a Abs. 4 S. 1 i. V. m. § 34 Abs. 3 S. 1 mvSOG; § 33a Abs. 4 S. 1 ndsSOG; § 31 Abs. 5 S. 1 rpPOG; § 28b Abs. 5 S. 1 saarlPolG; § 186 Abs. 1 S. 1 shLVwG; § 34a Abs. 5 S. 1 thürPAG.

103 Obwohl die Anordnung der Überwachung unter Richtervorbehalt nicht von Art. 10 GG geboten wird, ist diese verfahrensrechtliche Vorkehrung nach *C. Gusy* und *G. Hermes* bei der Telekommunikationsüberwachung erforderlich, wenn es keine vergleichbare Maßnahme zur Verfahrenssicherung gibt (*Gusy* (Fn. 81), Art. 10 Rn. 74; *Hermes* (Fn. 81), Art. 10 Rn. 89). *H. Schulze-Fielitz* sieht den Richtervorbehalt als eine gesetzlich vorzusehende Vorkehrung für die heimlichen Grundrechtseingriffe an (*Schulze-Fielitz* (Fn. 53), Art. 19 IV Rn. 144). Diesen Auffassungen wird vom Bundesverfassungsgericht gefolgt. Durch sein Urteil über die „Online-Durchsuchung" zeigte das Bundesverfassungsgericht, dass eine vorbeugende Kontrolle durch eine unabhängige Instanz verfassungsrechtlich geboten sei, wenn eine heimliche Ermittlungsmaßnahme einen schwerwiegenden Grundrechtseingriff bewirke. Neben dem Richtervorbehalt dürfe der Gesetzgeber eine andere Stelle nur dann mit der Kontrolle betrauen, wenn diese gleiche Gewähr für ihre Unabhängigkeit und Neutralität wie ein Richter biete (BVerfGE 120, 274 (332)).

104 Ausgehend von seiner präventiven Funktion kann der Richtervorbehalt einerseits eine mögliche Willkür der Polizeibehörde verhindern und damit die Grundrechte gewährleisten.

105 BVerfGE 103, 142 (151); 109, 279 (357); *Koch*, Datenerhebung, S. 210; *Kutscha*, NVwZ 2003, 1296 (1299); *Michael/Morlok* (Fn. 53), Rn. 592. Zur persönlichen und sachlichen Unabhängigkeit der Richter *Detterbeck*, in: Sachs, GG, Art. 97 Rn. 11 ff.; *Sodan*, in: Isensee/Kirchhof, HStR, Bd. 5, 3. Aufl., § 113 Rn. 22 ff., 70 ff.; *Papier*, NJW 2001, S. 1089 ff.

106 BVerfGE 100, 313 (361).

und Hilfsorgane gebiete[107]. Jedenfalls kann der Behördenleitervorbehalt diese Voraussetzungen nicht erfüllen[108], weil es dem Behördenleiter an der Unabhängigkeit fehlt[109].

Die Wirksamkeit des Richtervorbehalts ist jedoch nicht zu überschätzen. Unter dem Gesichtspunkt des Gewaltenteilungsgrundsatzes ist der Richtervorbehalt, nach dem das Gericht eine vorbeugende Kontrolle durchführen kann, nicht frei von Zweifeln. Die Einführung des Richtervorbehalts hat zur Folge, dass der Richter wegen seiner Überprüfungsbefugnis vorbeugend über den Zugriff auf den E-Mail-Verkehr entscheiden kann. Falls sich die gerichtliche vorbeugende Kontrolle am Maßstab einer umfassenden Kontrolldichte orientiert, dürfte die Gefahrenprognose, die zu den typischen polizeilichen Instrumenten gezählt wird[110], durch die verwaltungsbegleitende Gerichtskontrolle[111] ersetzt werden[112]. Um einen solchen Ersatz der polizeilichen Gefahrenprognose zu vermeiden, könnte der Richter die Dichte der (vorbeugenden) Kontrolle reduzieren, wobei es nicht um den Verzicht auf die richterliche Überprüfungsbefugnis, der nach Art. 19 Abs. 4 GG unzulässig ist, geht. Dies führt jedoch wohl dazu, dass eine einseitige polizeiliche Entscheidung über die Durchführung einer Überwachungsmaßnahme faktisch durch die Reduzierung der Kontrolldichte zugelassen wird. Zudem kann das rechtliche Gehör der Zielpersonen bei der vorbeugenden Gerichtskontrolle nicht gewährt werden, weil ansonsten die Heimlichkeit der polizeilichen Überwachungsmaßnahme verloren geht[113]. Dies hat zur Folge, dass die richterliche Entscheidung über die Durchführung einer präventiv-polizeilichen E-Mail-Überwachung nur auf den Informationen, die die Polizei vorlegt, basieren kann[114]. Da es in den polizei- und ordnungsrechtlichen Ermächtigungsvorschriften zur Telekommunikationsüberwachung an Regelungen über die richterliche Sachaufklärung fehlt, ist eine Prüfung, die über die Schlüssigkeitsprüfung exekutiver Sachverhalts-

107 BVerfGE 100, 313 (361).

108 *Kutscha* (Fn. 105), 1296 (1299); a. A. *Götz* (Fn. 9), § 17 Rn. 51; *Koch* (Fn. 105), S. 210; *Würtenberger/Heckmann* (Fn. 9), Rn. 577.

109 *Kutscha* (Fn. 105), 1296 (1299).

110 *Götz* (Fn. 9), § 6 Rn. 9; *Schenke* (Fn. 5), Rn. 77; *Würtenberger/Heckmann* (Fn. 9), Rn. 416 f.

111 Kritisch dazu *Schmidt-Aßmann*, in: Maunz/Dürig, GG, Art. 19 Abs. 4 Rn. 176.

112 Die polizeiliche Gefahrenprognose kann vom Gericht (nachträglich) überprüft werden (*Schenke* (Fn. 5), Rn. 51, 77). Sie kann aber nicht durch die vorbeugende Gerichtskontrolle ersetzt werden. Zur Grenze der verwaltungsbegleitenden Gerichtskontrolle *Lingemann*, Gefahrenprognose, 1985, S. 48 ff., *Schäfer* (Fn. 5), S. 168; *Schmidt-Aßmann*, in: Schoch/Schmidt-Aßmann/Pietzner, VwGO, Einleitung Rn. 170; *Würtenberger/Heckmann* (Fn. 9), Rn. 578.

113 *Koch* (Fn. 105), S. 210; *Kutscha* (Fn. 105), 1296 (1298); *Würtenberger/Heckmann* (Fn. 9), Rn. 578.

114 Vgl. *Gusy*, JZ 1998, S. 167 (169); *Schäfer* (Fn. 5), S. 168; *Kutscha* (Fn. 105), 1296 (1298); *Würtenberger/Heckmann* (Fn. 9), Rn. 578.

darstellung hinausgeht[115], im Verfahren der vorbeugenden Gerichtskontrolle sehr schwierig[116]. Mangels anderer Erkenntnisquellen[117] kann der Richter im Rahmen der vorbeugenden Gerichtskontrolle in der Regel bloß die Begründung der Polizei auf ihre Plausibilität überprüfen[118]. Nach empirischen Untersuchungen wird denn auch der Antrag eines Zugriffs auf die Telekommunikation selten vom Richter abgelehnt[119]. In diesem Zusammenhang ist eine wirksame Repräsentation der Belange der Zielpersonen im Verfahren der vorbeugenden Gerichtskontrolle kaum möglich. Aus diesem Grund ist sehr fraglich, ob der Richtervorbehalt ein „Allheilmittel" zum präventiven Rechtsschutz ist[120]. Die Effizienz des Richtervorbehalts zur Verbesserung der Asymmetrie des Rechtsverhältnisses zwischen der überwachenden Polizeibehörde und betroffenen Nutzern der E-Mail-Dienste lässt sich nicht abschließend bewerten. Dementsprechend geht es beim Richtervorbehalt (nur) um eine Mindestsicherung im Verfahren.

Nach den polizei- und ordnungsgesetzlichen Ermächtigungsvorschriften zur Telekommunikationsüberwachung kann der Richtervorbehalt ausnahmsweise durchbrochen werden: Bei Gefahr im Verzug darf eine präventiv-polizeiliche Telekommunikationsüberwachung durch den Behördenleiter angeordnet werden[121]. Ob die Situation der „Gefahr im Verzug" vorliegt, ist eng auszulegen[122]. Zwar soll die Auslegung des Begriffs der „Gefahr im Verzug" nach dem Urteil des Bundesverfassungsgerichts einer unbeschränkten gerichtlichen Kontrolle unterliegen[123], jedoch dürfte eine volle

115 Nach dem Urteil des Bundesverfassungsgerichts muss der Richter bei einer präventiven Kontrolle selbst die Tatsachen feststellen (BVerfGE 83, 24 (33); vgl. auch *Maurer*, Staatsrecht, § 19 Rn. 14). Faktisch werden die richterliche Sachprüfung mangels der Anhörung der Zielpersonen jedoch zur Plausibilitäts- bzw. Schlüssigkeitsprüfung exekutiver Sachverhaltsdarstellung (*Gusy* (Fn. 114), S. 167 (171)).

116 Vgl. dazu *Gusy* (Fn. 114), S. 167 (171).

117 Der von der Polizei vorgelegte Antrag stellt in der Tat die einzige informationelle Grundlage der richterlichen Entscheidung dar (*Gusy* (Fn. 81), Art. 10 Rn. 85).

118 *Gusy* (Fn. 100), S. 275; *Koch* (Fn. 105), S. 211 mit Fn. 882.

119 *Albrecht/Dorsch/Krüpe*, Rechtswirklichkeit und Effizienz, S. 23; *Backes/Gusy*, Telefonüberwachung, S. 44.

120 *Kutscha* (Fn. 105), 1296 (1298); *Trute* (Fn. 74), S. 403 (421).

121 § 23a Abs. 3 S. 7 i. V. m. § 23 Abs. 3 S. 8 bwPolG; Art. 34c Abs. 1 i. V. m. Art. 34 Abs. 4 S. 1 und 2 bayPAG; § 33b Abs. 5 S. 1 bbgPolG; § 10c Abs. 1 S. 2 hambGDatPol; § 15a Abs. 4 S. 1 hessSOG; § 34a Abs. 4 S. 1 i. V. m. § 34 Abs. 3 S. 2 mvSOG; § 33a Abs. 5 S. 1 und 3 ndsSOG; § 31 Abs. 5 S. 6 rpPOG; § 28b Abs. 5 S. 4 saarlPolG; § 186 Abs. 1 S. 2 und 3 shLVwG; § 34a Abs. 5 S. 2 thürPAG.

122 BVerfGE 103, 142 (153); *Epping* (Fn. 53), Rn. 672; *Hermes* (Fn. 81), Art. 13 Rn. 31; *Jarass* (Fn. 53), Art. 13 Rn. 19; *Stern* (Fn. 91), S. 276; *Zippelius/Würtenberger* (Fn. 58), § 28 Rn. 29.

123 BVerfGE 103, 142 (158 ff.); vgl. auch *Epping* (Fn. 53), Rn. 672; *Gornig*, in: von Mangoldt/Klein/Starck, GG, Bd. 1, Art. 13 Rn. 71; *Hermes* (Fn. 81), Art. 13 Rn. 31; *Jarass* (Fn. 53), Art. 13 Rn. 19; *Kunig* (Fn. 58), Art. 13 Rn. 32; *Stern* (Fn. 91), S. 276; *Zippelius/Würtenberger* (Fn. 58), § 28 Rn. 29.

Gerichtskontrolle, wie oben ausgeführt wurde, wegen der einseitigen Informationsbasis faktisch nicht immer effektiv sein.

IV. Beendigung des Rechtsverhältnisses zwischen der überwachenden Polizeibehörde und den betroffenen Nutzern der E-Mail-Dienste

Da das Rechtsverhältnis zwischen der überwachenden Polizeibehörde und den betroffenen Nutzern der E-Mail-Dienste, das durch die als Realakt zu qualifizierende Maßnahme der präventiv-polizeilichen Mail-Überwachung begründet wird, aus einem konkreten und einmaligen Anlass besteht, ist es kein Dauer-Verwaltungsrechtsverhältnis. Dieses Rechtsverhältnis wird beendet, wenn die Maßnahme der präventiv-polizeilichen E-Mail-Überwachung wegen des Ablaufs der durch die Anordnung festgelegten Frist endet[124] oder aufgrund des Eingriffs in den Kernbereich privater Lebensgestaltung unterbrochen wird[125] oder mangels der richterlichen Bestätigung oder des Fortbestehens der in Ermächtigungsvorschriften bezeichneten Voraussetzung beendigt wird[126].

Folge der Beendigung des Rechtsverhältnisses zwischen der überwachenden Polizeibehörde und den betroffenen Nutzern der E-Mail-Dienste ist die Unterrichtungspflicht der Polizei. Nach dem Abschluss der Maßnahme der präventiv-polizeilichen E-Mail-Überwachung ist derjenige, gegen den sich die Überwachungsmaßnahme gerichtet hat und dessen personenbezogene Daten durch die Überwachungsmaßnahme erhoben wurden, vom polizeilichen Zugriff auf seine E-Mail-Kommunikation zu benachrichtigen[127], es sei denn, dass die nachträgliche Unterrichtung des betroffenen Nutzers der E-Mail-Dienste den Zweck der Überwachungsmaßnahme gefährden würde[128]. Da auch die dem Begriff der personenbezoge-

124 Zur Anordnungsdauer § 23a Abs. 3 S. 7 i. V. m. § 23 Abs. 3 S. 4 bwPolG; Art. 34c Abs. 3 S. 4 und 5 bayPAG; § 33b Abs. 5 S. 5 und 6 bbgPolG; § 10c Abs. 2 S. 3 und 4 hambGDatPol; § 15a Abs. 4 S. 4 i. V. m. § 15 Abs. 5 S. 6 und 7 hessSOG; § 34a Abs. 4 S. 2 und 3 mvSOG; § 33a Abs. 4 S. 2 und 3 ndsSOG; § 31 Abs. 5 S. 2 und 3 rpPOG; § 28b Abs. 5 S. 2 und 3 saarlPolG; § 186a Abs. 5 S. 3 und 4 shLVwG; § 34a Abs. 6 S. 3 und 4 thürPAG.

125 Dazu Art. 34a Abs. 1 S. 4 bayPAG; § 33b Abs. 2 S. 3 bbgPolG; § 33a Abs. 3 S. 1 und 2 ndsSOG; § 28b Abs. 1 S. 6 i.V.m § 28a Abs. 2 S. 2 saarlPolG; § 186a Abs. 2 S. 1 und 4 shLVwG; § 34b Abs. 1 S. 1 thürPAG.

126 Dazu § 23a Abs. 4 bwPolG; Art. 34c Abs. 3 S. 6 bayPAG; § 33b Abs. 5 S. 7 bbgPolG; § 10c Abs. 4 S. 1 hambGDatPol; § 15a Abs. 4 S. 4 i. V. m. § 15 Abs. 5 S. 9 hessSOG; § 33a Abs. 5 S. 6 ndsSOG; § 186a Abs. 6 S. 2 shLVwG; § 34a Abs. 5 S. 3 thürPAG.

127 § 23a Abs. 8 S. 1 i. V. m. § 23 Abs. 6 S. 1 bwPolG; Art. 34c Abs. 5 S. 1 bayPAG; § 33b Abs. 7 i. V. m. § 29 Abs. 7 S. 1 bbgPolG; § 10c Abs. 2 S. 3 und 4 hambGDatPol; § 29 Abs. 6 S. 1 hessSOG; § 34a Abs. 7 S. 1 mvSOG; § 30 Abs. 4 S. 1 ndsSOG; § 40 Abs. 5 S. 1 und 2 rpPOG; § 28 Abs. 5 S. 1 saarlPolG; § 186 Abs. 4 S. 1 shLVwG; § 34 Abs. 9 S. 2 Nr. 2 thürPAG.

128 § 23a Abs. 8 S. 1 i. V. m. § 23 Abs. 6 S. 1 bwPolG; Art. 34c Abs. 5 S. 2 bayPAG; § 33b Abs. 7 i. V. m. § 29 Abs. 7 S. 1 und Abs. 8 S. 1 bbgPolG; § 10c Abs. 4 S. 1 hambGDatPol; § 29 Abs. 6

nen Daten entsprechende E-Mail-Adresse der Kommunikationspartner der Zielpersonen durch eine präventiv-polizeiliche E-Mail-Überwachung von der Polizei erhoben wird, sind sie (Kommunikationspartner der Zielpersonen) nach dem Abschluss der Überwachungsmaßnahme darüber zu unterrichten[129], auch wenn die Benachrichtigung nach gesetzlichen Vorschriften nur für die Zielpersonen, gegen die sich die Maßnahme der präventiv-polizeilichen E-Mail-Überwachung gerichtet hat, gilt[130]. Diese Konsequenz gilt auch für unbeteiligte Dritte, deren E-Mails über den kontrollierten E-Mail-Knoten übermittelt und von der Polizei wegen eines technischen Fehlers des Überwachungsprogramms mitgelesen wurden. Im Gegensatz dazu kann die Polizei auf die nachträgliche Benachrichtigung sonstiger unbeteiligter Dritter, deren E-Mails nur von dem im kontrollierten E-Mail-Knoten eingesetzten E-Mail-Filter virtuell überprüft und nicht auf den Server der überwachenden Polizeibehörde übertragen wurden, verzichten, weil, wie bereits dargelegt wurde, die für die Benachrichtigung notwendige Identifizierung eines unbeteiligten mitbetroffenen Dritten zu einer weiteren Datenerhebung führt[131] und damit den Grundrechtseingriff intensiviert[132].

Nach § 23a Abs. 8 Satz 1 in Verbindung mit § 23 Abs. 6 Satz 5 Nr. 2 bwPolG und § 29 Abs. 6 Satz 3 hessSOG unterbleibt die Unterrichtung, wenn die Ermittlung der betroffenen Person oder deren Anschrift einen unverhältnismäßigen Verwaltungsaufwand erfordern würde. Zudem ist die Benachrichtigung gemäß § 34 Abs. 10 Satz 1 Nr. 2 thürPAG nicht geboten, sobald sie bedeutende Vermögenswerte gefährdet. Der nachträgliche gerichtliche Rechtsschutz gegen die präventiv-polizeiliche Überwachungsmaßnahme ist faktisch dann möglich, wenn die betroffenen Personen über die Maßnahme verdeckter Informationserhebung, die bereits abgeschlossen ist, unterrichtet werden. Jedoch wird die Möglichkeit des gerichtlichen Rechtsschutzes, der sich gegen einen schweren Eingriff in das Fernmeldegeheimnis richtet, gemäß den genannten polizei- und ordnungsgesetzlichen Vorschriften ausgeschlossen. Hier bedarf es einer Verhältnismäßigkeitsprüfung. Das Gewicht des Verwaltungsaufwands oder der Vermögenswerte ist in Relation zu der Tiefe des Eingriffs in das Fernmeldgeheimnis zu setzen.

S. 4 hessSOG; § 34a Abs. 7 S. 1 mvSOG; § 30 Abs. 4 S. 3 ndsSOG; § 40 Abs. 5 S. 4 rpPOG; § 28 Abs. 5 S. 1 saarlPolG; § 186 Abs. 4 S. 4 shLVwG; § 34 Abs. 10 S. 1 Nr. 1 thürPAG.

129 So ausdrücklich § 34 Abs. 10 S. 1 Nr. 2 Buchstabe d thürPAG.

130 Gemäß § 29 Abs. 6 S. 1 und 2 hessSOG ist nur die Person, gegen die sich die Maßnahme gerichtet hat, zu unterrichten. Es fehlt an Regelungen über die Unterrichtung der Kommunikationspartner der Zielpersonen. Methodisch ist diese Lücke des Gesetzes durch Analogie zu füllen.

131 So ausdrücklich § 29 Abs. 7 S. 2 bbgPolG; § 30 Abs. 4 S. 4 ndsSOG; § 40 Abs. 6 Nr. 2 rpPOG; § 28 Abs. 5 S. 2 saarlPolG; § 186 Abs. 4 S. 2 shLVwG.

132 BVerfG, NJW 2007, S. 351 (356).

Unter dem Gesichtspunkt der Rechtsgüterabwägung gibt es bei dem Konflikt zwischen dem Aufwand zur Erfüllung der Benachrichtigungspflicht und der Ermöglichung effektiven Rechtsschutzes gegen erhebliche Grundrechtseingriffe keinen „unverhältnismäßigen" Verwaltungsaufwand und keine „bedeutenden" Vermögenswerte. Ob eine solche Einschränkung der polizeilichen Unterrichtungspflicht angemessen ist, ist zu bezweifeln.

B. Rechtsverhältnis zwischen der überwachenden Polizeibehörde und den Anbietern der E-Mail-Dienste

Ohne technische Hilfe der E-Mail-Provider würde eine präventiv-polizeiliche E-Mail-Überwachung erschwert werden. Alle polizei- und ordnungsgesetzlichen Ermächtigungsvorschriften zur Telekommunikationsüberwachung schreiben die Mitwirkungspflicht der Diensteanbieter vor[133]. Die „Mitwirkungspflicht" bezeichnet das im Folgenden zu erörternde Rechtsverhältnis zwischen der überwachenden Polizeibehörde und den Anbietern der E-Mail-Dienste bei der Durchführung einer präventiv-polizeilichen E-Mail-Überwachung.

I. Verwaltungsakt als Entstehungsgrund des Rechtsverhältnisses

1. Verwaltungsaktscharakter der polizeilichen Anordnung

Wie bereits im 1. Kapitel dargelegt wurde, eröffnet § 110 TKG die rechtliche Möglichkeit der technischen Vorkehrung für die Umsetzung der E-Mail-Überwachung[134]. Nach § 110 Abs. 1 Satz 1 TKG sind die Anbieter der E-Mail-Dienste verpflichtet, auf eigene Kosten technische Einrichtungen zur Umsetzung einer E-Mail-Überwachung vorzuhalten. Trotz dieser im TKG vorgeschriebenen Pflicht der E-Mail-Provider wird das bei der Durchführung einer präventiv-polizeilichen E-Mail-Überwachung entstehende Rechtsverhältnis zwischen der überwachenden Polizeibehörde und den Anbietern der E-Mail-Dienste nicht durch telekommunikationsgesetzliche Vorschriften begründet. Denn § 110 Abs. 1 Satz 1 TKG stellt keine Rechtsgrundlage der präventiv-polizeilichen Telekommunikationsüberwachung dar[135]. Zudem bezieht sich § 110 Abs. 1 Satz 1 TKG nicht auf die Tätigkeit

133 § 23a Abs. 5 bwPolG; Art. 34b bayPAG; § 33b Abs. 6 bbgPolG; § 10a Abs. 3 hambGDatPol; § 15a Abs. 1 und 2 hessSOG; § 34a Abs. 6 mvSOG; § 33a Abs. 7 ndsSOG; § 31 Abs. 6 rpPOG; § 28b Abs. 2 saarlPolG; § 185a Abs. 4 shLVwG; § 34a Abs. 1 thürPAG.

134 Siehe 1. Kapitel A II.

135 *Bock*, in: Geppert/Piepenbrock/Schütz/Schuster, TKG, § 110 Rn. 1; *Eckhardt*, in: Heun, Handbuch Telekommunikationsrecht, B Rn. 100; *Graulich*, in: Arndt/Fetzer/Scherer, TKG, § 110 Rn. 31; *Klesczewski*, in: Säcker, TKG, § 110 Rn. 4; *Löwnau*, in: Scheurle/Mayen, TKG, § 110 Rn. 1.

der Mithilfe, sondern auf den Vorhalt technischer Einrichtungen. Ob die Durchführung einer präventiv-polizeilichen E-Mail-Überwachung zulässig ist, hängt davon ab, ob der Landesgesetzgeber durch Polizei- und Ordnungsgesetze die Polizei ermächtigt, eine Telekommunikation zu überwachen. Es ist nur möglich, dass die E-Mail-Provider eine Mitwirkungspflicht für den präventiv-polizeilichen Zugriff auf die E-Mail-Kommunikation übernehmen, wenn die E-Mail-Überwachung in den Polizei- und Ordnungsgesetzen ihre Rechtsgrundlage findet.

Auch die polizei- und ordnungsgesetzlichen Vorschriften, die die Mitwirkungspflicht der Diensteanbieter regeln, lassen sich nicht als Entstehungsgrund des Rechtsverhältnisses zwischen der überwachenden Polizeibehörde und den Anbieter der E-Mail-Dienste auffassen. Zwar sind die E-Mail-Provider nach diesen Vorschriften verpflichtet, der Polizei die Überwachung eines E-Mail-Verkehrs zu ermöglichen, jedoch ist eine solche Mitwirkungspflicht nicht hinreichend konkret. Die Frage, ab wann und wie die Anbieter der E-Mail-Dienste den präventiv-polizeilichen Zugriff auf die E-Mail-Kommunikation ermöglichen müssen, regeln die gesetzlichen Vorschriften nicht. Die konkreten Inhalte der Mitwirkungspflicht werden nur bestimmt, wenn die Polizei von den E-Mail-Providern die technische Hilfe im Einzelfall verlangt.

Da sich die konkreten Inhalte der Mitwirkungspflicht der E-Mail-Provider unmittelbar aus der von der überwachenden Polizeibehörde getroffenen Anordnung technischer Hilfe ergeben, wird das Rechtsverhältnis zwischen der überwachenden Polizeibehörde und den Anbietern der E-Mail-Dienste, das sich auf die Mitwirkungspflicht der E-Mail-Provider bezieht, durch die polizeiliche Anordnung technischer Hilfe begründet. In Bezug auf die Rechtnatur ist diese Anordnung, durch die die überwachende Polizeibehörde im Einzelfall die konkreten Inhalte der Mitwirkungspflicht der E-Mail-Provider bestimmt, als Verwaltungsakt zu qualifizieren[136]. Die Begriffsmerkmale des Verwaltungsakts sind erfüllt: Durch diese Anordnung erlegt die Polizeibehörde einem bestimmten Anbieter der E-Mail-Dienste im Einzelfall eine konkrete Verhaltenspflicht auf. Diese polizeiliche Willenserklärung, die die Verhaltenspflicht eines bestimmten E-Mail-Providers begründet, ist nicht privatrechtlich, weil sie der Konkretisierung der in den polizei- und ordnungsgesetzlichen Ermächtigungsvorschriften vorgeschriebenen (allgemeinen) Mitwirkungspflicht des Diensteanbieters dient.

136 *Schäfer* (Fn. 5), S. 84. Im Ergebnis wohl auch *Berner/Köhler* (Fn. 6), Art. 34b Rn. 4.

2. Begründung des Rechtsverhältnisses zwischen der überwachenden Polizeibehörde und den Anbietern der E-Mail-Dienste durch Abschluss eines Verwaltungsvertrags?

Abzulehnen ist die Möglichkeit, dass die überwachende Polizeibehörde durch Abschluss eines Verwaltungsvertrags mit einem Anbieter der E-Mail-Dienste den Anspruch auf die technische Hilfe durchsetzt und damit ein Rechtsverhältnis zu diesem E-Mail-Provider begründet[137]. Denn die (allgemeine) Mitwirkungsverpflichtung, nach der die Anbieter der E-Mail-Dienste durch technische Hilfe eine präventiv-polizeiliche E-Mail-Überwachung ermöglichen müssen, wird bereits vom Gesetzgeber durch die polizei- und ordnungsgesetzlichen Bestimmungen zwangsweise auferlegt. Es steht den E-Mail-Providern nicht frei, ob sie die Mitwirkungspflicht übernehmen. Da die Anbieter der E-Mail-Dienste der überwachenden Polizeibehörde den Anspruch auf technische Hilfe nicht verweigern können, liegt eine freie Willenserklärung (d. h. freie Annahme der E-Mail-Provider), die ein Element eines Vertrags darstellt, nicht vor[138]. Aufgrund der erzwungenen Leistung technischer Hilfe stellt das Rechtsverhältnis zwischen der überwachenden Polizeibehörde und den Anbietern der E-Mail-Dienste keinen Verwaltungsvertrag, sondern einen Verwaltungsakt dar.

Zudem kann die Konsequenz, dass das Rechtsverhältnis zwischen der überwachenden Polizeibehörde und den Anbietern der E-Mail-Dienste nicht durch einen Verwaltungsvertrag begründet wird, auch aus § 58 Abs. 1 VwVfG[139] hergeleitet werden. Gemäß § 58 Abs. 1 VwVfG wird ein in Rechte Dritter eingreifender Verwaltungsvertrag erst wirksam, wenn der Dritte schriftlich zustimmt. Das Ziel dieser Vorschrift ist der Rechtsschutz Dritter durch Verfahren[140], weil die betroffenen Dritten einen in ihre Rechte eingreifenden Verwaltungsvertrag nicht anfechten können[141]. Falls die überwachende Polizeibehörde mit einem E-Mail-Provider einen Verwaltungsvertrag, nach dem der E-Mail-Provider eine für die Durchführung präventiv-polizeilicher E-Mail-Überwachung notwendige technische Hilfe leisten muss, abschließt, ist dieser Verwaltungsvertrag ein drittbelastender Vertrag, der in den Anwendungsbereich des § 58 Abs. 1 VwVfG fällt. Denn

137 Nach § 54 S. 1 VwVfG kann ein Rechtsverhältnis auf dem Gebiet des öffentlichen Rechts durch Vertrag begründet werden.

138 Eine freie Willensübereinstimmung (d. h. eine Einigung zwischen zwei oder mehreren Rechtssubjekten) ist erforderlich für die Entstehung eines Verwaltungsvertrags (*Detterbeck* (Fn. 8), Rn. 784; *Maurer* (Fn. 8), § 14 Rn. 6; *Peine* (Fn. 8), Rn. 772).

139 Es gibt keine abweichenden Vorschriften in den Landesverwaltungsverfahrensgesetzen.

140 Vgl. *Bonk*, in: Stelkens/Bonk/Sachs, VwVfG, § 58 Rn. 1; *Henneke* (Fn. 12), § 58 Rn. 2; *Kopp/Ramsauer* (Fn. 11), § 58 Rn. 4; *Peine* (Fn. 8), Rn. 811; *Schlette*, Verwaltung als Vertragspartner, S. 432; *Staudenmayer*, Verwaltungsvertrag, S. 4; *Tiedemann*, in: Obermayer, VwVfG, § 58 Rn. 1; *Ziekow* (Fn. 12), § 58 Rn. 4.

141 *Kopp/Ramsauer* (Fn. 11), § 58 Rn. 1.

der Inhalt dieses Verwaltungsvertrags bezieht sich auf die Ermöglichung eines präventiv-polizeilichen Zugriffs auf die E-Mail-Kommunikation, der in das Grundrecht Dritter (d. h. in das Fernmeldegeheimnis betroffener Nutzer der E-Mail-Dienste) eingreift. Die Wirksamkeit eines solchen Verwaltungsvertrags hängt von der Zustimmung der betroffenen Dritten ab. Die betroffenen Dritten können ihre Zustimmung dann geben oder verweigern, wenn sie benachrichtigt wurden. Allerdings betrifft der Inhalt des Verwaltungsvertrags, den die überwachende Polizeibehörde mit dem E-Mail-Provider abschließt, eine technische Mithilfe bei der verdeckten Informationserhebung. Insoweit ist die Zustimmung Dritter, die nach § 58 Abs. 1 VwVfG eine Wirksamkeitsvoraussetzung für einen drittbelastenden Verwaltungsvertrag darstellt, vor dem Abschluss der präventiv-polizeilichen E-Mail-Überwachung faktisch überhaupt nicht möglich. Auch wenn man die Auffassung, dass § 58 Abs. 1 VwVfG den Abschluss eines drittbelastenden Vertrags, dem die betroffenen Dritten (noch) nicht zustimmen, nicht verbiete[142], vertritt, ist die Erfüllung eines solchen Verwaltungsvertrags problematisch. Ein in Rechte Dritter eingreifender Verwaltungsvertrag, der die Voraussetzungen der Vertragsnichtigkeit (§ 59 VwVfG) nicht erfüllt, ist bis zur Erteilung der Zustimmung Dritter schwebend unwirksam[143]. Zwar sind die Vertragsparteien bis zur Entscheidung Dritter (vorläufig) an ihre Vertragserklärungen gebunden[144], dies bedeutet allerdings nicht, dass die Vertragsparteien aufgrund der Bindung an Vertragserklärungen in Rechte Dritter eingreifen dürfen. Vor allem ist es wegen der schwebenden Unwirksamkeit des Vertrags schwer einzusehen, warum die Vertragsparteien (d. h. die überwachende Polizeibehörde und der E-Mail-Provider) zur Erfüllung des noch nicht wirksamen Verwaltungsvertrags in das Grundrecht betroffener Dritter, gegenüber denen der abgeschlossene Verwaltungsvertrag schwebend unwirksam ist[145], eingreifen können. Durch die Erfüllung eines solchen Verwaltungsvertrags wird der Rechtsschutz betroffener Dritter durch Verfahren, der das Ziel des § 58 Abs. 1 VwVfG darstellt, verletzt. Die Unzulässigkeit der Erfüllung eines drittbelastenden Verwaltungsvertrags, dem betroffene Dritte nicht zustimmen, führt dazu, dass der Abschluss eines Verwaltungsvertrags mit E-Mail-Providern sein verfolgtes Ziel, also eine wirkungsvolle präventiv-polizeiliche E-Mail-Überwachung, nicht erreichen kann. Unter dem Gesichtspunkt der Geeignetheit kann die überwachende Polizeibehörde insoweit nicht durch Abschluss eines Ver-

142 *Bonk* (Fn. 140), § 58 Rn. 4; *Staudenmayer* (Fn. 140), S. 4.

143 *Bonk* (Fn. 140), § 58 Rn. 4; *Bull/Mehde* (Fn. 8), Rn. 858; *Henneke* (Fn. 12), § 58 Rn. 13; *Kopp/Ramsauer* (Fn. 11), § 58 Rn. 2, 12, 19; *Peine* (Fn. 8), Rn. 816; *Schlette* (Fn. 140), S. 433; *Staudenmayer* (Fn. 140), S. 6; *Tiedemann* (Fn. 140), § 58 Rn. 16; *Ziekow* (Fn. 12), § 58 Rn. 11.

144 *Bonk* (Fn. 140), § 58 Rn. 5; *Kopp/Ramsauer* (Fn. 11), § 58 Rn. 19; *Schlette* (Fn. 140), S. 433; *Staudenmayer* (Fn. 140), S. 6; *Tiedemann* (Fn. 140), § 58 Rn. 16.

145 *Bonk* (Fn. 140), § 58 Rn. 4.

waltungsvertrags den in die Berufsfreiheit eingreifenden Anspruch auf die technische Hilfe eines E-Mail-Providers durchsetzen.

II. Polizeilicher grenzüberschreitender Anspruch auf die technische Hilfe der E-Mail-Provider

Da die E-Mail-Kommunikation in der virtuellen Welt erfolgt, kann ein E-Mail-Provider bundesweit oder weltweit E-Mail-Dienste anbieten. Beispielsweise kann ein baden-württembergischer Kunde durch eine Anmeldung über Internet E-Mail-Dienste, deren Anbieter keinen Firmensitz in Baden-Württemberg hat, nutzen. Ein deutscher Kunde kann auch durch die E-Mail-Dienste eines ausländischen Providers, dessen Firmensitz sich nicht in Deutschland befindet, seine E-Mails übermitteln. Hier wird die Frage aufgeworfen: Kann die Polizeibehörde, die eine präventive E-Mail-Überwachung durchführt, den E-Mail-Providern, die im Gebiet der örtlichen Zuständigkeit der überwachenden Polizeibehörde keinen Sitz haben, durch einen Verwaltungsakt eine konkrete Mitwirkungspflicht auferlegen?

1. Nationaler grenzüberschreitender Anspruch auf die technische Hilfe der E-Mail-Provider

a) Zulässigkeit der nationalen grenzüberschreitenden Tätigkeit der Polizei

Gemäß dem Wortlaut der polizei- und ordnungsgesetzlichen Ermächtigungsvorschriften zur präventiven Telekommunikationsüberwachung erstreckt sich die Mitwirkungspflicht der Diensteanbieter auf jeden E-Mail-Provider, der den Zielpersonen E-Mail-Dienste anbietet. Danach ist deutlich, dass die E-Mail-Provider, die nur in einem anderen Bundesland Sitze haben, nicht ausscheiden[146]. Insoweit ist die Antwort auf die Frage, ob die E-Mail-Provider im Landesgebiet, innerhalb dessen die überwachende Polizeibehörde die Gefahrenabwehraufgabe wahrnehmen muss, einen Firmensitz haben müssen, klar. Entscheidend ist nur, ob die E-Mail-Provider den Zielpersonen, die im Bezirk der überwachenden Polizeibehörde eine Gefahr verursachen, E-Mail-Dienste anbieten[147]. Diese Konsequenz entspricht dem oben bereits dargelegten Kriterium für die Bestimmung der örtlichen Zuständigkeit: Die Polizei kann eine Maßnahme zur Gefahrenabwehr ergreifen, wenn die abzuwehrende Gefahr in ihrem Bezirk auftritt[148]. Maßgeblich für die örtliche Zuständigkeit für die Durchführung einer präventiv-polizeilichen E-Mail-Überwachung ist nicht der Sitz der Zielpersonen oder der E-Mail-Provider, sondern die Antwort auf die Frage, wo die abzuwehrende Gefahr auftritt. Ausgehend davon kann

146 *Berner/Köhler* (Fn. 6), Art. 34b Rn. 2.
147 *Berner/Köhler* (Fn. 6), Art. 34b Rn. 2.
148 Dazu siehe oben A I 2.

die den E-Mail-Verkehr der Zielpersonen überwachende Polizeibehörde einem E-Mail-Provider, dessen Firmensitz nicht im Gebiet ihrer örtlichen Zuständigkeit liegt, durch einen Verwaltungsakt eine konkrete Mitwirkungspflicht auferlegen, wenn er den Zielpersonen, die im Bezirk der überwachenden Polizeibehörde eine Gefahr verursachen, die E-Mail-Dienste anbietet. Bei einem solchen nationalen grenzüberschreitenden Anspruch auf die technische Hilfe der E-Mail-Provider geht es nicht um die kompetenzwidrige Geltung eines Landesgesetzes in einem anderen Bundesland, sondern um eine notwendige Maßnahme zur Abwehr der Gefahren, die im Gebiet der örtlichen Zuständigkeit der überwachenden Polizeibehörde auftreten. Da der nationale grenzüberschreitende Anspruch der Polizei auf die technische Hilfe der landesfremden E-Mail-Provider eine polizeiliche Tätigkeit zum wirksamen Vollzug des auf den Landesbereich beschränkten Gesetzes darstellt, ist er nicht unzulässig[149].

b) Zustimmung des betroffenen Nachbarbundeslandes und der Grundsatz der Bundestreue

Zwar besteht der nationale grenzüberschreitende Anspruch der Polizei auf die Mitwirkung der landesfremden E-Mail-Provider aus der Sicht der örtlichen Zuständigkeit zweifelsfrei, jedoch sind die polizei- und ordnungsgesetzlichen spezifischen Regelungen über die in einem anderen Bundesland vorgenommenen Amtshandlungen der Landespolizeibeamten nicht zu übersehen. Nach den einschlägigen Vorschriften ist die Voraussetzung für die nationale grenzüberschreitende Tätigkeit der Landespolizeibeamten entweder die Anforderung oder die Zustimmung einer zuständigen Stelle[150]. Deswegen kann die überwachende Polizeibehörde einem landes-

149 Vgl. BVerwGE 79, 339 (342); im Ergebnis auch *Schäfer* (Fn. 5), S. 229.

150 § 79 Abs. 1 S. 1 i. V. m. § 78 Abs. 1 S. 1 Nr. 1 bwPolG; Art. 10 Abs. 2 i. V. m. Art. 11 Abs. 3 S. 1 Nr. 1 bayPOG; § 7 Abs. 1 i. V. m. § 8 Abs. 1 S. 1 Nr. 1 berlASOG; § 76 Abs. 1 S. 1 i. V. m. § 77 Abs. 1 S. 1 Nr. 1 bbgPolG; § 82 Abs. 1 i. V. m. § 81 Abs. 1 S. 1 Nr. 1 bremPolG; § 30b Abs. 1 i. V. m. § 30a Abs. 1 S. 1 Nr. 1 hambSOG; § 103 Abs. 1 S. 1 i. V. m. § 102 Abs. 1 S. 1 Nr. 1 hessSOG; § 10 Abs. 1 S. 1 i. V. m. § 9 Abs. 1 S. 1 Nr. 1 mvSOG; § 104 Abs. 1 S. 1 i. V. m. § 103 Abs. 1 S. 1 Nr. 1 ndsSOG; § 8 Abs. 1 i. V. m. § 9 Abs. 1 S. 1 Nr. 1 nwPOG; § 87 Abs. 1 S. 1 i. V. m. § 86 Abs. 1 S. 1 Nr. 1 rpPOG; § 89 Abs. 1 S. 1 i. V. m. § 88 Abs. 1 S. 1 Nr. 1 saarlPolG; § 78 Abs. 1 S. 1 sächsPolG; § 92 Abs. 1 S. 1 i. V. m. § 91 Abs. 1 S. 1 Nr. 1 saSOG; § 171 Abs. 1 i. V. m. § 170 Abs. 1 S. 1 Nr. 1 shLVwG; § 10 Nr. 1 thürPOG. Die Anwendung von § 79 Abs. 1 S. 1 i. V. m. § 78 Abs. 1 S. 1 Nr. 1 bwPolG und § 89 Abs. 1 S. 1 i. V. m. § 88 Abs. 1 S. 1 Nr. 1 saarlPolG ist nicht zu verneinen. Die genannten polizeigesetzlichen Vorschriften regeln die Voraussetzungen für die nationalen grenzüberschreitenden Tätigkeiten des Polizeivollzugsdienstes bzw. der Vollzugpolizei. Da gemäß § 23a bwPolG und § 28b saarPolG nicht die Polizei(verwaltungs)behörde, sondern der Polizeivollzugsdienst bzw. die Vollzugspolizei für die präventiv-polizeiliche Telekommunikationsüberwachung zuständig ist, sind § 79 Abs. 1 S. 1 i. V. m. § 78 Abs. 1 S. 1 Nr. 1 bwPolG und § 89 Abs. 1 S. 1 i. V. m. § 88 Abs. 1 S. 1 Nr. 1 saarlPolG anzuwenden, wenn der E-Mail-Provider nur in einem anderen Bundesland seinen Firmensitz hat.

fremden E-Mail-Provider, dessen Sitz sich im Gebiet eines anderen Bundeslandes befindet, durch einen Verwaltungsakt eine konkrete Mitwirkungspflicht nur auferlegen, wenn sie dieses Nachbarbundesland über die nationale grenzüberschreitende Tätigkeit benachrichtigt und seine Zustimmung eingeholt hat. Hier stellt sich die Frage: Kann ein betroffenes Nachbarbundesland, vor allem ein betroffenes Nachbarbundesland, in dem eine Ermächtigungsvorschrift zur präventiv-polizeilichen Telekommunikationsüberwachung fehlt, die nationale grenzüberschreitende Tätigkeit der überwachenden Polizeibehörde ablehnen? Dazu wird in der Literatur vertreten, dass die Hoheitsgewalt des betroffenen Nachbarbundeslandes durch die nationale grenzüberschreitende Telekommunikationsüberwachung des „Anordnungsbundeslandes" nicht beeinträchtigt werde[151]. Das betroffene Nachbarbundesland müsse die nationale grenzüberschreitende Gefahrenabwehrmaßnahme der Telekommunikationsüberwachung dulden[152]. Diese Duldungspflicht des Nachbarbundeslandes ergebe sich aus dem Grundsatz der Bundestreue[153]. Ein Bundesland könne nicht ablehnen, dass Maßnahmen gegenüber einem Störer, der im Gebiet eines anderen Bundeslandes eine Gefahr verursache, ergriffen werden können[154]. Falls das betroffene Nachbarbundesland die nationale grenzüberschreitende präventiv-polizeiliche Telekommunikationsüberwachung, die in seinem Gebiet durchgeführt werde, versage, werde die der Erfüllung der staatlichen Schutzpflicht dienende effektive Gefahrenabwehr des „Anordnungsbundeslandes" verhindert[155]. Dies führe zugleich zu einer empfindlichen Störung der bundesstaatlichen Ordnung[156].

Ob die oben genannte Auffassung, die auf dem Grundsatz der Bundestreue basiert, überzeugend ist, ist zweifelhaft. Nach dem Grundsatz der Bundestreue, der als ein Satz des ungeschriebenen Verfassungsrechts angesehen wird[157], sind sowohl der Bund als auch die Bundesländer verpflichtet, bei der Wahrnehmung der Kompetenz die Interessen anderer Mitglieder des Bundesstaats nicht zu missachten[158]. Dies gilt auch für das Verhältnis

151 *Schäfer* (Fn. 5), S. 98, 230.

152 *Schäfer* (Fn. 5), S. 98, 230.

153 *Schäfer* (Fn. 5), S. 91 ff.; zum Grundsatz der Bundestreue *Bauer*, Bundestreue, 1992; *Gröpl*, Staatsrecht, Rn. 658 ff.; *Isensee*, in: Isensee/Kirchhof, HStR, Bd. 6, 3. Aufl., § 126 Rn. 160 ff.; *Sachs* (Fn. 97), Art. 20 Rn. 68 ff.; *Zippelius/Würtenberger* (Fn. 58), § 14 Rn. 40 ff.

154 *Schäfer* (Fn. 5), S. 98.

155 *Schäfer* (Fn. 5), S. 98, 230.

156 *Schäfer* (Fn. 5), S. 98, 230.

157 *Degenhart*, Staatsorganisationsrecht, Rn. 482; *Gröpl* (Fn. 153), Rn. 660; *Hofmann* (Fn. 99), Art. 20 Rn. 13; *Maurer* (Fn. 115), § 10 Rn. 50; *Schnapp*, in: von Münch/Kunig, GG, Bd. 2, Art. 20 Rn. 11; *Zippelius/Würtenberger* (Fn. 58), § 14 Rn. 40.

158 Vgl. *Gröpl* (Fn. 153), Rn. 661; *Isensee* (Fn. 153), Rn. 162; *Leisner*, in: Sodan, GG, Art. 20 Rn. 19; *Maurer* (Fn. 115), § 10 Rn. 52; *Pieroth*, in: Jarass/Pieroth, GG, Art. 20 Rn. 22 f.; *Sachs*

zwischen einem Bundesland und seinem Nachbarbundesland[159]. Zu beachten ist, dass der Grundsatz der Bundestreue subsidiär zur Füllung von Regelungslücken dient[160]. Da die Polizei- und Ordnungsgesetze ausdrücklich regeln, dass die Zustimmung des betroffenen Nachbarbundeslandes eine Voraussetzung der nationalen grenzüberschreitenden polizeilichen Tätigkeit eines Bundeslandes darstellt, gibt es keine Regelungslücke. Methodisch ist insoweit schwer einzusehen, wieso sich eine Zustimmungs*pflicht* des betroffenen Bundeslandes, das nach den positiv-rechtlichen Vorschriften ausdrücklich eine Zustimmungs*befugnis* hat, aus dem Grundsatz der Bundestreue ergeben kann.

Da das betroffene Nachbarbundesland keine (generelle) Zustimmungspflicht hat, kann es seine Zustimmung geben oder verweigern. Dabei geht es um das behördliche Ermessen des betroffenen Nachbarbundeslandes. Das betroffene Nachbarbundesland muss seine Zustimmung nur geben, wenn eine „Ermessensreduzierung auf Null" vorliegt. Berücksichtigt man, dass die Durchführung der präventiv-polizeilichen Telekommunikationsüberwachung (durch die technische Mitwirkung der Provider) der Abwehr der gegenwärtigen Gefahr und dem Schutz besonders hochrangiger Rechtsgüter dient, dürfte sich eine „Ermessensreduzierung auf Null", die im Einzelfall der Grund für die Bestimmungspflicht des betroffenen Nachbarbundeslandes ist, leicht ergeben.

Wenn das betroffene Nachbarbundesland die nationale grenzüberschreitende Tätigkeit der überwachenden Polizeibehörde ablehnt, liegt eine öffentlich-rechtliche Streitigkeit vor. Diese ist nicht verfassungsrechtlicher, sondern verwaltungsrechtlicher Natur. Da es für das betroffene Nachbarbundesland keine ausdrücklichen Regelungen über die Ausübung seiner Zustimmungskompetenz gibt, kann der Grundsatz der Bundestreue, der zur Füllung der Regelungslücke dient, als eine Ausübungsschranke der Zustimmungskompetenz des betroffenen Nachbarbundeslandes angesehen werden. Obwohl die Bundestreue ein ungeschriebener Verfassungsgrundsatz ist, bedeutet dies nicht, dass die öffentlich-rechtliche Streitigkeit, die sich auf die Ablehnung der nationalen grenzüberschreitenden polizeilichen Tätigkeit und die Verletzung des Grundsatzes der Bundestreue bezieht, verfassungsrechtlicher Natur ist. Nach der ständigen Rechtspre-

(Fn. 97), Art. 20 Rn. 70; *Schnapp* (Fn. 157), Art. 20 Rn. 11; *Sommermann*, in: von Mangoldt/Klein/Starck, GG, Bd. 2, Art. 20 Rn. 38.

159 *Bauer*, in: Dreier, GG, Bd. 2, Art. 20 (Bundesstaat) Rn. 40; *Gröpl* (Fn. 153), Rn. 659; *Hofmann* (Fn. 99), Art. 20 Rn. 15; *Isensee* (Fn. 153), Rn. 163; *Leisner* (Fn. 158), Art. 20 Rn. 17; *Maurer* (Fn. 115), § 10 Rn. 52; *Pieroth* (Fn. 158), Art. 20 Rn. 21; *Sommermann* (Fn. 158), Art. 20 Rn. 37.

160 Vgl. *Bauer* (Fn. 153), S. 371 ff.; *Bauer* (Fn. 159), Art. 20 (Bundesstaat) Rn. 39; *Gröpl* (Fn. 153), Rn. 658; *Isensee* (Fn. 153), Rn. 166; *Maurer* (Fn. 115), § 10 Rn. 50, 53; *Sachs* (Fn. 97), Art. 20 Rn. 68.

chung des Bundesverfassungsgerichts ist die Pflicht zu bundesfreundlichem Verhalten akzessorischer Natur[161]. Mit anderen Worten: Der Grundsatz der Bundestreue begründet nicht selbstständig eine Pflicht des Bundes oder eines Bundeslandes[162]. Er kann nur innerhalb eines anderweitig begründeten Rechtsverhältnisses oder einer anderweitig begründeten Rechtspflicht moderieren, variieren oder ergänzen[163]. Zwar stellt die Bundestreue einen ungeschriebenen Verfassungsgrundsatz dar, jedoch beschränkt sich ihr Anwendungsbereich nicht auf das verfassungsrechtliche Verhältnis zwischen Mitgliedern des Bundesstaats[164]. Vielmehr ist dieser ungeschriebene Verfassungsgrundsatz auch anwendbar für verwaltungsrechtliche Rechte und Pflichten im Verhältnis zwischen Mitgliedern des Bundesstaats[165]. Berücksichtigt man, dass die Zustimmungskompetenz des betroffenen Nachbarbundeslandes nicht im Grundgesetz oder in Landesverfassungen, sondern in Polizei- und Ordnungsgesetzen vorgeschrieben ist, betrifft die Frage, ob das betroffene Nachbarbundesland der in seinem Gebiet durchgeführten nationalen grenzüberschreitenden präventiv-polizeilichen E-Mail-Überwachung zustimmt, das verwaltungsrechtliche Verhältnis zwischen dem „Anordnungsbundesland" und dem betroffenen Nachbarbundesland. Unstreitig ist, dass sich der Grundsatz der Bundestreue in diesem verwaltungsrechtlichen Rechtsverhältnis zwischen Bundesländern auswirkt. Jedoch formt der Grundsatz der Bundestreue nicht automatisch ein verwaltungsrechtliches Rechtsverhältnis in ein verfassungsrechtliches um[166]. Aufgrund seiner verwaltungsrechtlichen Natur ist dieses Rechtsverhältnis zwischen Bundesländern kein Streitgegenstand des für verwaltungsrechtliche Streitigkeiten nicht anwendbaren Art. 93 Abs. 1 Nr. 4 Var. 2 GG (in Verbindung mit § 13 Nr. 8 BVerfGG)[167]. Für eine

161 BVerfGE 42, 103 (177); 95, 250 (266); 103, 81 (88); 104, 238 (247); 110, 33 (52); vgl. auch *Degenhart* (Fn. 157), Rn. 488; *Hofmann* (Fn. 99), Art. 20 Rn. 14; *Isensee* (Fn. 153), Rn. 166; *Leisner* (Fn. 158), Art. 20 Rn. 18; *Maurer* (Fn. 115), § 10 Rn. 53; *Pieroth* (Fn. 158), Art. 20 Rn. 21; *Sachs* (Fn. 97), Art. 20 Rn. 69; *Sommermann* (Fn. 158), Art. 20 Rn. 37; *Zippelius/Würtenberger* (Fn. 58), § 14 Rn. 40.

162 BVerfGE 42, 103 (117); 95, 250 (266); 103, 81 (88); 104, 238 (247); *Degenhart* (Fn. 157), Rn. 488; *Hofmann* (Fn. 99), Art. 20 Rn. 14; *Isensee* (Fn. 153), Rn. 166; *Leisner* (Fn. 158), Art. 20 Rn. 18; *Maurer* (Fn. 115), § 10 Rn. 53; *Zippelius/Würtenberger* (Fn. 58), § 14 Rn. 40.

163 BVerfGE 104, 238 (247 f.); *Hofmann* (Fn. 99), Art. 20 Rn. 14; *Isensee* (Fn. 153), Rn. 166; *Maurer* (Fn. 115), § 10 Rn. 53; *Zippelius/Würtenberger* (Fn. 58), § 14 Rn. 40.

164 BVerfGE 103, 81 (88); *Maurer* (Fn. 115), § 10 Rn. 53.

165 BVerfGE 103, 81 (88); *Maurer* (Fn. 115), § 10 Rn. 53.

166 BVerfGE 103, 81 (88).

167 *Fleury*, Verfassungsprozessrecht, Rn. 444; *Hillgruber/Goos*, Verfassungsprozessrecht, Rn. 65; *Hopfauf*, in: Schmidt-Bleibtreu/Hofmann/Hopfauf, GG, Art. 93 Rn. 143; *Löwer*, in: Isensee/Kirchhof, HStR, Bd. 3, § 70 Rn. 50; *Meyer*, in: von Münch/Kunig, GG, Bd. 3, Art. 93 Rn. 51; *Pestalozza*, Verfassungsprozessrecht, § 10 Rn. 2; *Pieroth* (Fn. 158), Art. 93 Rn. 38; *Sachs*, Verfassungsprozessrecht, Rn. 322, 333; *Schlaich/Korioth*, Bundesverfassungsgericht, Rn. 107; *Sturm*, in: Sachs, GG, Art. 93 Rn. 72; *Wieland*, in: Dreier, GG, Bd. 3, Art. 93 Rn. 72.

verwaltungsrechtliche Streitigkeit zwischen Bundesländern ist der Rechtsweg zum Bundesverwaltungsgericht vorrangig (§§ 40 Abs. 1, 50 Abs. 1 Nr. 1 VwGO)[168]. Allerdings ist in der Praxis fraglich, ob eine solche Verwaltungsklage tatsächlich erhoben wird. Denn der Rechtsweg zum Bundesverwaltungsgericht kann zur Bekanntmachung der Durchführung einer präventiv-polizeilichen E-Mail-Überwachung führen. Dies widerspricht der Heimlichkeit der polizeilichen Überwachungsmaßnahme. Insoweit dürfte eine solche Verwaltungsklage nur erhoben werden, wenn die Überwachungsmaßnahme erledigt ist.

2. Internationaler grenzüberschreitender Anspruch auf die technische Hilfe der E-Mail-Provider

Sieht man die Mitwirkung der E-Mail-Provider als einen notwendigen Teil einer effektiven präventiv-polizeilichen E-Mail-Überwachung an, kann die überwachende Polizeibehörde einem ausländischen E-Mail-Provider, der in Deutschland keinen Sitz hat, zur Abwehr der in ihrem Bezirk auftretenden Gefahr unter dem Gesichtspunkt der örtlichen Zuständigkeit theoretisch durch einen Verwaltungsakt eine konkrete Mitwirkungspflicht auferlegen und damit mit diesem ausländischen E-Mail-Provider ein Rechtsverhältnis begründen. Dies ist nur dann möglich, wenn der polizeiliche Vollzug des Landesgesetzes im Ausland durch völkerrechtliche Vereinbarungen geregelt ist[169].

Auch im Rahmen der EU nach dem Vertrag von Lissabon ist eine polizeiliche Zusammenarbeit der Mitgliedstaaten nicht im alleinigen Rekurs auf die Bestimmungen der Art. 67, 87 f. AEUV zulässig. Vielmehr bedürfte es hier konkretisierender sekundärrechtlicher Bestimmungen.

Auch wenn eine völkerrechtliche Vereinbarung die internationale grenzüberschreitende Tätigkeit der deutschen Polizeibehörde zulässt, kann ein Anspruch auf die technische Hilfe eines ausländischen E-Mail-Providers schwierig sein. Denn eine Mitwirkung eines E-Mail-Providers setzt voraus, dass er die technische Einrichtung zur Umsetzung einer E-Mail-Überwachung vorhält. Für einen ausländischen E-Mail-Provider, dessen Sitz sich nicht in Deutschland befindet, ist das TKG allerdings unanwendbar[170]. Dementsprechend besteht die Pflicht aus § 110 Abs. 1 Satz 1 TKG dort

168 *Fleury* (Fn. 167), Rn. 444; *Hillgruber/Goos* (Fn. 167), Rn. 65; *Hopfauf* (Fn. 167), Art. 93 Rn. 143; *Löwer* (Fn. 167), Rn. 50; *Meyer* (Fn. 167), Art. 93 Rn. 51; *Pestalozza* (Fn. 167), § 10 Rn. 2; *Pieroth* (Fn. 158), Art. 93 Rn. 38; *Sachs* (Fn. 167), Rn. 322, 333; *Schlaich/Korioth* (Fn. 167), Rn. 107; *Sturm* (Fn. 167), Art. 93 Rn. 72; *Wieland* (Fn. 167), Art. 93 Rn. 72.

169 § 79 Abs. 1 S. 2 bwPolG; § 76 Abs. 1 S. 2 bbgPolG; § 103 Abs. 1 S. 2 hessSOG; § 10 Abs. 1 S. 2 mvSOG; § 104 Abs. 1 S. 3 ndsSOG; § 8 Abs. 3 nwPOG; § 87 Abs. 1 S. 2 rpPOG; § 89 Abs. 2 saarlPolG; § 78 Abs. 1 S. 2 sächsPolG; § 92 Abs. 1 S. 2 saSOG; § 10 Nr. 2 thürPOG.

170 *Bock* (Fn. 135), § 110 Rn. 96.

nicht[171]. So wird ein ausländischer E-Mail-Provider an einer präventiv-polizeilichen E-Mail-Überwachung kaum mitwirken können, weil er mangels dahingehender telekommunikationsrechtlicher Pflicht keine Überwachungseinrichtung vorhalten wird[172].

III. Rechtsposition der Anbieter der E-Mail-Dienste gegenüber der überwachenden Polizeibehörde

Nach der Darstellung des Entstehungsgrunds des Rechtsverhältnisses ist die Rechtsposition der E-Mail-Provider, die bei der Durchführung einer präventiv-polizeilichen E-Mail-Überwachung aufgrund der als Verwaltungsakt zu qualifizierenden polizeilichen Anordnung mitwirken, zu behandeln. Da sich die Anbieter der E-Mail-Dienste durch ihre technische Hilfe an der Erfüllung einer polizeilichen Verwaltungsaufgabe (Gefahrenabwehr) beteiligen, lässt sich die Frage nach der Rechtsposition der E-Mail-Provider gegenüber der überwachenden Polizeibehörde einerseits aus der Sicht des Verwaltungsorganisationsrechts erörtern. Berücksichtigt man, dass sich ein polizeilicher Verwaltungsakt gegen die Anbieter der E-Mail-Dienste richtet, geht es andererseits um deren polizeirechtliche Verantwortlichkeit.

1. Verwaltungsorganisationsrechtliche Rechtsposition der E-Mail-Provider

Die technische Mitwirkung eines E-Mail-Providers, die dem präventiv-polizeilichen Zugriff auf die E-Mail-Kommunikation der Zielpersonen dient, betrifft die verwaltungsorganisationsrechtliche Problematik der Beteiligung Privater an Verwaltungsaufgaben. Insoweit kann die Rechtsposition der E-Mail-Provider gegenüber der überwachenden Polizeibehörde zunächst aus Sicht des Verwaltungsorganisationsrechts erörtert werden. Hier ist zu fragen, wie die Mithilfe eines E-Mail-Providers bei der Durchführung einer präventiv-polizeilichen E-Mail-Überwachung organisationsrechtlich zu qualifizieren ist.

a) Formen der Beteiligung Privater an Verwaltungsaufgaben

Es gibt unterschiedliche Formen der Beteiligung Privater an Verwaltungsaufgaben. Ihre begriffliche Abgrenzung voneinander ist zu erläutern; andernfalls ist eine richtige verwaltungsorganisationsrechtliche Einordnung des E-Mail-Providers, der bei der Durchführung einer präventiv-polizeilichen E-Mail-Überwachung aufgrund der Anordnung der Polizeibehörde mitwirkt, unmöglich.

171 *Bock* (Fn. 135), § 110 Rn. 96.

172 Im Gegensatz dazu ist ein polizeilicher Anspruch auf technische Hilfe eines deutschen E-Mail-Providers, der die Telekommunikationsanlagen im Ausland betreibt oder diese von einem ausländischen Dritten betreiben lässt, problemlos. Denn er fällt in den Anwendungsbereich des § 110 Abs. 1 S. 1 TKG (*Bock* (Fn. 135), § 110 Rn. 97; *Schäfer* (Fn. 5), S. 74).

aa) Beliehene

Der Begriff des Beliehenen, bei dem es sowohl um die Organisationsprivatisierung (formelle Privatisierung)[173] als auch um die funktionelle Privatisierung gehen kann, meint Privatpersonen, denen von einem Hoheitsträger spezielle hoheitliche Befugnisse zur selbstständigen Erfüllung bestimmter Verwaltungsaufgaben übertragen werden[174]. Da Beliehene aufgrund einer Übertragung der Kompetenz im eigenen Namen hoheitlich handeln können[175], entsprechen sie dem Begriff der Behörde im Sinne des § 1 Abs. 4 VwVfG[176]. Im Umfang der übertragenen Befugnisse gehört die Tätigkeit des Beliehenen zur mittelbaren Staatsverwaltung[177]. Berücksichtigt man, dass es bei der Beleihung um eine Übertragung hoheitlicher Befugnisse des Staats geht, bedarf diese Form der Beteiligung Privater an Verwaltungsaufgaben einer gesetzlichen Grundlage[178]. Davon ausgehend lässt sich das Rechtsverhältnis zwischen dem beleihenden Verwaltungsträger und dem Beliehenen durch Gesetz oder durch Rechtsverordnung, Verwaltungsakt oder Verwaltungsvertrag[179] aufgrund einer gesetzlichen Ermächtigung begründen[180].

---

173 *Burgi*, in: Erichsen/Ehlers, AllgVerwR, § 9 Rn. 25; *Peine*, DÖV 1997, S. 353 (360 f.).

174 *Burgi* (Fn. 173), § 9 Rn. 24; *Detterbeck* (Fn. 8), Rn. 192; *von Heimburg*, Verwaltungsaufgaben, S. 36; *Heintzen*, VVDStRL 62 (2003), S. 220 (240 f.); *Maurer* (Fn. 8), § 23 Rn. 56; *Peine* (Fn. 8), Rn. 108; *Schmitz* (Fn. 95), § 1 Rn. 256; *Schulze-Fielitz* (Fn. 73), § 12, Rn. 106; *Stober*, in: Wolff/Bachof/Stober/Kluth/Müller, VerwR, Bd. 3, § 90 Rn. 4; *Voßkuhle*, VVDStRL 62 (2003), S. 266 (299) mit Fn. 137; *Ziekow* (Fn. 12), § 1 Rn. 34.

175 *Remmert*, Private Dienstleistungen, S. 258.

176 *Burgi* (Fn. 173), § 9 Rn. 24, 30; *Detterbeck* (Fn. 8), Rn. 193; *Kopp/Ramsauer* (Fn. 11), § 1 Rn. 58; *Maurer* (Fn. 8), § 23 Rn. 56, 58; *Peine* (Fn. 8), Rn. 110; *Schmitz* (Fn. 95), § 1 Rn. 256; *Stober* (Fn. 174), § 90 Rn. 54; *Ziekow* (Fn. 12), § 1 Rn. 34.

177 *Burgi* (Fn. 173), § 9 Rn. 24; *Detterbeck* (Fn. 8), Rn. 193; *Maurer* (Fn. 8), § 23 Rn. 56; *Peine* (Fn. 8), Rn. 80; *Stuible-Treder*, Die Beliehene, S. 84.

178 *Burgi* (Fn. 173), § 9 Rn. 27; *Detterbeck* (Fn. 8), Rn. 192; *Heintzen* (Fn. 174), S. 220 (240); *Kopp/Ramsauer* (Fn. 11), § 1 Rn. 58; *Maurer* (Fn. 8), § 23 Rn. 57; *Schmitz* (Fn. 95), § 1 Rn. 257; *Schulze-Fielitz* (Fn. 73), Rn. 106; *Stuible-Treder* (Fn. 177), S. 84. Dies bedeutet, dass die Beleihung unter institutionellem Gesetzesvorbehalt steht (*Burgi* (Fn. 173), § 9 Rn. 27; *Kopp/Ramsauer* (Fn. 11), § 1 Rn. 58; *Ossenbühl*, VVDStRL 29 (1971), S. 137 (173 f.); *Stober* (Fn. 174), § 90 Rn. 44; *Stuible-Treder* (Fn. 177), S. 84; *Trute*, in: Hoffmann-Riem/Schmidt-Aßmann/Voßkuhle, GVwR, Bd. 1, § 6 Rn. 92).

179 Nach *R. Michaelis* kann nur der einseitige staatliche Hoheitsakt in Form eines Gesetzes oder eines Verwaltungsakts den Beleihungsakt darstellen (*Michaelis*, Der Beliehene, S. 138 ff.). Dieser Ansicht ist nicht zu folgen. Wenn man akzeptiert, dass das Rechtsverhältnis zwischen dem beleihenden Verwaltungsträger und dem Beliehenen durch Verwaltungsakt begründet werden kann, erscheint es auch möglich, dass eine Beleihung durch Verwaltungsvertrag, der einen Verwaltungsakt ersetzt (§ 54 S. 2 VwVfG), möglich ist (vgl. auch *von Heimburg* (Fn. 174), S. 37; *Stuible-Treder* (Fn. 177), S. 89).

180 *Burgi* (Fn. 173), § 9 Rn. 27; *von Heimburg* (Fn. 174), S. 36 f.; *Kopp/Ramsauer* (Fn. 11), § 1 Rn. 58; *Maurer* (Fn. 8), § 23 Rn. 57; *Peine* (Fn. 8), Rn. 110; *Stober* (Fn. 174), § 90 Rn. 44; *Stuible-Treder* (Fn. 177), S. 85 ff. Die Möglichkeit der Beleihung durch privatrechtlichen Ver-

bb) Verwaltungshelfer

Der Begriff des Verwaltungshelfers, der der funktionalen Privatisierung entspricht[181], erstreckt sich auf Privatpersonen, die sich an der Wahrnehmung der Verwaltungsaufgaben beteiligen. Im Gegensatz zu Beliehenen handeln Verwaltungshelfer allerdings im Auftrag und nach Weisung der Behörde[182]. Bei der Verwaltungshilfe geht es nicht um die Übertragung der hoheitlichen Kompetenz, sondern um die Ausübung der die Behörde unterstützenden Tätigkeiten[183]. Ein Verwaltungshelfer ist kein Verwaltungsträger[184]. Vielmehr stellt er nur ein Werkzeug bzw. einen verlängerten Arm der Behörde dar[185]. Mangels Selbstständigkeit wird das Handeln des Verwaltungshelfers dem beauftragenden Verwaltungsträger zugerechnet[186]. Das Rechtsverhältnis zwischen der Behörde und dem Verwaltungshelfer wird entweder durch einen privatrechtlichen Vertrag oder durch einen Verwaltungsvertrag begründet[187]. Eine gesetzliche Ermächtigung ist hier nicht erforderlich[188].

cc) Erfüllungsgehilfe der Behörde

Vom Verwaltungshelfer zu unterscheiden ist der Erfüllungsgehilfe der Behörde[189]. Diese Form der Beteiligung Privater an Verwaltungsaufgaben betrifft – wie Verwaltungshelfer – keine Übertragung hoheitlicher Befugnis. Vielmehr bezieht sich die Erfüllungshilfe der Behörde auf „Private, mit denen der Staat privatrechtliche Verträge abschließt und die dann in Erfüllung ihrer vertraglichen Pflicht für den Staat tätig werden“[190]. Im Gegensatz zum Verwaltungshelfer besitzt der Erfüllungsgehilfe der Behörde jedoch Selbstständigkeit[191]. Ein Beispiel dafür ist der private Abschleppunterneh-

---

trag ist abzulehnen. Denn die Übertragung hoheitlicher Befugnis ist ausdrücklich öffentlichrechtlich. Sie ist kein Gegenstand privatrechtlichen Vertrags (vgl. auch *Stuible-Treder* (Fn. 177), S. 90).

181 *Burgi* (Fn. 173), § 9 Rn. 32; *Schmitz* (Fn. 95), § 1 Rn. 134; *Stober* (Fn. 174), § 90a Rn. 1.

182 *Detterbeck* (Fn. 8), Rn. 194; *Stober* (Fn. 174), § 90a Rn. 1; *Ziekow* (Fn. 12), § 1 Rn. 35.

183 *Detterbeck* (Fn. 8), Rn. 194; *Maurer* (Fn. 8), § 23 Rn. 59.

184 *Detterbeck* (Fn. 8), Rn. 194.

185 *Kopp/Ramsauer* (Fn. 11), § 1 Rn. 58; *Peine* (Fn. 8), Rn. 109; Nach *H. Maurer* ist die Konstellation, dass der Verwaltungshelfer der verlängerte Arm der Behörde ist, heute aber „nicht zwingend, nicht einmal typisch“ (*Maurer* (Fn. 8), § 23 Rn. 59).

186 *Detterbeck* (Fn. 8), Rn. 194; *Heintzen* (Fn. 174), S. 220 (254); *Ziekow* (Fn. 12), § 1 Rn. 35.

187 *Burgi* (Fn. 173), § 9 Rn. 33; *Maurer* (Fn. 8), § 23 Rn. 59.

188 *Burgi*, Funktionale Privatisierung, S. 153; *Kopp/Ramsauer* (Fn. 11), § 1 Rn. 58; *Maurer* (Fn. 8), § 23 Rn. 59; *Schulze-Fielitz* (Fn. 73), Rn. 105. In der Literatur wird jedoch vertreten, dass ein dauerhafter Einsatz eines Verwaltungshelfers unter den Gesetzesvorbehalt falle (vgl. *Remmert* (Fn. 175), S. 263 f.).

189 *Ehlers*, Verwaltung in Privatrechtsform, S. 504 ff.; *Ziekow*, Öffentliches Wirtschaftsrecht, § 4 Rn. 35.

190 *Detterbeck* (Fn. 8), Rn. 195.

191 BGHZ 121, 161 (164 f.); *Ziekow* (Fn. 12), § 1 Rn. 36. Obwohl der Erfüllungsgehilfe der Behörde selbstständig handeln kann, bedeutet dies nicht, dass der Staat nicht für seinen

mer, der damit betraut wird, ein verbotswidrig parkendes Fahrzeug zu beseitigen[192]. Allerdings wird in der neueren Literatur vertreten, dass sich die als ein klassisches Begriffsmerkmal des Verwaltungshelfers angesehene Unselbstständigkeit nicht durchhalten lasse[193]. Folgt man dieser Auffassung, kann der Erfüllungsgehilfe der Behörde als ein „selbstständiger Verwaltungshelfer" betrachtet werden[194].

dd) Indienstnahme Privater

Auch die Indienstnahme Privater, die als das Ergebnis einer funktionalen Privatisierung angesehen wird[195], stellt eine Form der Beteiligung Privater an Verwaltungsaufgaben dar[196]. Dabei geht es um die Auferlegung der (berufsbezogenen bzw. unternehmensbezogenen) Pflichten zur Gewährleistung der ordnungsgemäßen Erfüllung der Verwaltungsaufgaben[197]. Die Indienstnahme Privater unterscheidet sich von der Beleihung dadurch, dass die Indienstnahme keine Übertragung staatlicher Kompetenz (Hoheitsbefugnis) betrifft[198]. Daraus ergeben sich zwei Konsequenzen: Da sich die Indienstnahme Privater nicht auf die Einräumung hoheitlicher Kompetenz, sondern auf die der Wahrnehmung der Verwaltungsaufgaben dienende Nutzung der vorhandenen Sach- und Personalkapazitäten Privater erstreckt[199], ist der Gegenstand der Indienstnahme eine Tätigkeit, die nicht nur der Staat, sondern auch der Private ausüben kann[200]. Zudem begründet die Indienstnahme mangels der Übertragung hoheitlicher Befugnis keine öffentlich-rechtliche Berechtigung, sondern eine öffentlich-rechtliche Verpflichtung[201].

Die Indienstnahme ist auch vom Verwaltungshelfer abzugrenzen. Der Unterschied zwischen diesen beiden Rechtsinstituten besteht darin, dass

---

Erfüllungsgehilfen haftet. Im Bereich der Eingriffsverwaltung ist der Erfüllungsgehilfe der Behörde, der nach der (problematischen) Werkzeugtheorie wegen seiner Selbstständigkeit nicht als Werkzeug des Staats erscheint, auch als Beamter im haftungsrechtlichen Sinne anzusehen (BGHZ 121, 161 (165 f.); *Ossenbühl*, Staatshaftungsrecht, S. 21 f.).

192 BGHZ 121, 161 (166); *Detterbeck* (Fn. 8), Rn. 195; *Ossenbühl* (Fn. 191), S. 20; *Ziekow* (Fn. 189), § 4 Rn. 35.

193 Vgl. *Maurer* (Fn. 8), § 23 Rn. 59; *Stober* (Fn. 174), § 90a Rn. 13 f.

194 Vgl. OLG Hamm, NJW 2001, S. 375 (376); *Di Fabio*, VVDStRL 56 (1997), S. 235 (273); *Stober* (Fn. 174), § 90a Rn. 14.

195 *Heintzen* (Fn. 174), S. 220 (255).

196 Gegen den Begriff der Indienstnahme Privater *Manssen*, in: von Mangoldt/Klein/Starck, GG, Bd. 1, Art. 12 Rn. 200.

197 *Dreier*, Hierarchische Verwaltung, S. 248; *Stober* (Fn. 174), § 90a Rn. 61.

198 *Dreier* (Fn. 197), S. 248; *Friedrich*, Die Verpflichtung privater Telekommunikationsunternehmen, S. 89; *von Heimburg* (Fn. 174), S. 38; *Stober* (Fn. 174), § 90a Rn. 62; *Tettinger/Wank*, GewO, § 69 Rn. 47.

199 *Stober* (Fn. 174), § 90a Rn. 62.

200 *Michaelis* (Fn. 179), S. 82.

201 *Michaelis* (Fn. 179), S. 83.

die indienstgenommenen Privaten selbstständig die Verwaltungsaufgaben wahrnehmen[202]. Zwar besitzen die indienstgenommenen Privaten Selbstständigkeit, jedoch kann man die Indienstnahme Privater nicht mit dem Erfüllungsgehilfen der Behörde gleichsetzen. Da das Begriffsmerkmal der Indienstnahme Privater die Überbürdung der (berufsbezogenen bzw. unternehmensbezogenen) Pflicht ist, stellt diese Form der Beteiligung Privater an Verwaltungsaufgaben im Gegensatz zur durch einen Vertrag begründeten Erfüllungshilfe der Behörde eine Wahrnehmung der Verwaltungsaufgaben gegen den Willen der indienstgenommenen Privaten dar[203]. Folglich kommt eine vertragliche Indienstnahme nicht in Betracht[204]. Im Schrifttum wird vertreten, dass die Indienstnahme unmittelbar durch das Gesetz begründet werde[205]. Die im Gesetz vorgeschriebene (berufsbezogene bzw. unternehmensbezogene) Pflicht zur Wahrnehmung der Verwaltungsaufgaben bedürfe keiner Konkretisierung durch Verwaltungsakt[206]. Die Pflicht, die durch Verwaltungsakt konkretisiert werde, gehöre nicht zur (gesetzlichen) Indienstnahme Privater[207]. Die Ablehnung der durch Verwaltungsakt konkretisierten und begründeten Indienstnahme hat allerdings keine Argumentationsbasis[208]. Jedenfalls ist der Unterschied zwischen Indienstnahme durch Gesetz und Verwaltungsakt unbedeutend, weil die Interessenlage in beiden Fällen gleich ist[209].

b) E-Mail-Provider als indienstgenommene Private

Nach der Erörterung der begrifflichen Abgrenzung zwischen den unterschiedlichen Formen der Beteiligung Privater an Verwaltungsaufgaben ist festzuhalten, dass die E-Mail-Provider, die bei der Durchführung einer präventiv-polizeilichen E-Mail-Überwachung mitwirken müssen, indienstgenommene Private sind[210]. Bei der technischen Mitwirkung der E-Mail-Provider handelt es sich nicht um eine Übertragung der polizeilichen Befugnis, sondern um eine Vollzugsunterstützung polizeilichen Zugriffs auf die E-Mail-Kommunikation der Zielpersonen. Die E-Mail-Provider haben keine hoheitliche Kompetenz, über die Überwachung eines E-Mail-

202 *Friedrich* (Fn. 198), S. 89; *Stuible-Treder* (Fn. 177), S. 62. Ausgehend davon sieht *J. Stuible-Treder* die Indienstnahme Privater jedoch als eine Beleihung an (*Stuible-Treder* (Fn. 177), S. 62).

203 *Schulze-Fielitz* (Fn. 73), Rn. 107; *Voßkuhle*, in: Hoffmann-Riem/Schmidt-Aßmann/Voßkuhle, GVwR, Bd. 1, § 1 Rn. 60; *Voßkuhle* (Fn. 174), S. 266 (299 f.) mit Fn. 139.

204 A. A. *Heintzen* (Fn. 174), S. 220 (255); *Stober* (Fn. 174), § 90a Rn. 62.

205 *H. P. Ipsen*, in: FS Kaufmann, S. 141 (144 f.).

206 *Ipsen* (Fn. 205), S. 141 (144 f.).

207 *Ipsen* (Fn. 205), S. 141 (143 ff.).

208 *Michaelis* (Fn. 179), S. 79.

209 *Michaelis* (Fn. 179), S. 79; *Vogel*, Öffentliche Wirtschaftseinheiten, S. 31.

210 *Friedrich* (Fn. 198), S. 92; *R. P. Schenke*, AöR 125 (2000), S. 1 (37); *Waechter*, VerwArch. 87 (1996), S. 68 (70).

Verkehrs zu entscheiden. Aus diesem Grund sind sie keine Beliehene. Berücksichtigt man, dass die Mithilfe der E-Mail-Provider eine fachmännische technische Unterstützung polizeilicher Überwachungsmaßnahmen darstellt, erstreckt sich die Erfüllung der Mitwirkungspflicht der E-Mail-Provider nicht auf eine untergeordnete Tätigkeit nach fachlicher Weisung der Polizeibehörde. Da die E-Mail-Provider bei der Beteiligung an Verwaltungsaufgaben der Gefahrenabwehr selbstständig handeln, sind sie keine Verwaltungshelfer. Die E-Mail-Provider, die bei der präventiv-polizeilichen E-Mail-Überwachung mithelfen, sind auch keine Erfüllungsgehilfen der Polizeibehörde, weil die technische Mitwirkung eine Wahrnehmung der Verwaltungsaufgaben gegen den Willen der E-Mail-Provider darstellt. Wie bereits dargelegt wurde, wird das Rechtsverhältnis zwischen der überwachenden Polizeibehörde und den E-Mail-Providern, die eine präventiv-polizeiliche E-Mail-Überwachung ermöglichen müssen, nicht durch einen Vertrag, sondern durch einen Verwaltungsakt, der die in den Polizei- und Ordnungsgesetzen vorgeschriebene allgemeine Mitwirkungspflicht der Anbieter konkretisiert, begründet. Insoweit geht es bei der Beteiligung der E-Mail-Provider an der Durchführung der präventiv-polizeilichen E-Mail-Überwachung um die Erfüllung der von der überwachenden Polizeibehörde durch Verwaltungsakt auferlegten Pflicht. Die technische Mithilfe der E-Mail-Provider entspricht der Indienstnahme Privater.

2. Polizeirechtliche Rechtsposition der E-Mail-Provider

Da das Rechtsverhältnis zwischen der überwachenden Polizeibehörde und den E-Mail-Providern durch polizeilichen Verwaltungsakt begründet wird, stellen die E-Mail-Provider, denen die Polizeibehörde bei der Durchführung einer präventiven E-Mail-Überwachung eine Mitwirkungspflicht auferlegt, nicht nur indienstgenommene Private, sondern auch Adressaten der polizeilichen Maßnahme dar. In diesem Zusammenhang ist die polizeirechtliche Rechtsposition der E-Mail-Provider zu untersuchen. Dabei handelt es sich um die Verantwortlichkeit der E-Mail-Provider.

Es wird vertreten, dass ein privater Betrieb verantwortlich für den vorsätzlichen Missbrauch seiner Anlagen sei[211]. Diese Verantwortlichkeit ergebe sich aus der Standespflicht der Unternehmer[212]. Nach seiner Standespflicht sei ein privater Betrieb verpflichtet, einen Missbrauch seiner Anlagen zu verhindern[213]. Folgt man dieser Auffassung, sind die E-Mail-Provider verantwortlich für die Gefahr eines Missbrauchs des E-Mail-Kommunikationswegs. Allerdings ist dieser Auffassung nicht zuzustimmen. Die Standespflicht, dass ein privater Betrieb den Missbrauch seiner Anlagen abwehren muss, findet keine positiv-rechtliche Grundlage. Insoweit exis-

211 *Waechter* (Fn. 210), S. 68 (89).
212 *Waechter* (Fn. 210), S. 68 (89 f.).
213 *Waechter* (Fn. 210), S. 68 (90).

tiert eine solche „Pflicht" nicht rechtlich, sondern moralisch. Ob eine sittliche „Pflicht" eine rechtliche Verantwortlichkeit begründen kann, ist sehr fragwürdig. Da die Pflicht der Missbrauchsabwehr nicht im Gesetz vorgeschrieben ist, handelt es sich bei der Verletzung dieser „Pflicht" nicht um eine Beeinträchtigung der öffentlichen Sicherheit. Ferner ist auch zweifelhaft, ob man diese moralische „Pflicht" mit den „Regeln der Sitte", die sich auf die öffentliche Ordnung beziehen, gleichsetzen kann. Folglich verursacht die Bereitstellung der Telekommunikationsanlage, die eine durch Grundrechte geschützte Tätigkeit darstellt, keine Gefahr im Sinne des Polizeirechts. Nach der Theorie der unmittelbaren Verursachung sind die E-Mail-Provider auch nicht mitverantwortlich für die durch eine präventivpolizeiliche E-Mail-Überwachung abzuwehrende Gefahr, weil diese Gefahr nicht von E-Mail-Providern, sondern unmittelbar von den im polizei- und ordnungsgesetzlichen Ermächtigungsvorschriften zur Telekommunikationsüberwachung genannten Zielpersonen verursacht wird[214]. Demzufolge sind E-Mail-Provider als Nichtstörer anzusehen[215]. Die polizei- und ordnungsgesetzlichen Regelungen über die Mitwirkung der Diensteanbieter beschreiben eine Inanspruchnahme nichtverantwortlicher Dritter.

IV. Entschädigungsanspruch der E-Mail-Provider gegenüber der Polizeibehörde

Unter dem Aspekt der Kostenlast betrifft die technische Mithilfe der E-Mail-Provider sowohl die Kosten für die Überwachungsausstattung als auch die Kosten für den konkret-individuellen Zugriff auf eine E-Mail-Kommunikation[216]. Gemäß § 110 Abs. 1 Satz 1 TKG muss der E-Mail-Provider die Kosten für die Überwachungseinrichtungen tragen. In Baden-Württemberg[217], Bayern[218], Brandenburg[219], Mecklenburg-Vorpommern[220], Niedersachsen[221], Saarland[222], Schleswig-Holstein[223] und Thüringen[224] haben die E-Mail-Provider, die sich an einer Durchführung präventiv-polizeilicher E-Mail-Überwachung beteiligen, gegenüber der Polizeibehörde einen Entschädigungsanspruch bezüglich der Kosten für die konkrete Überwachung eines E-Mail-Verkehrs. Die Frage, ob die Polizeibehörde in Ham-

214 *Schenke* (Fn. 210), S. 1 (39).
215 *Schenke* (Fn. 210), S. 1 (40).
216 *Schenke* (Fn. 210), S. 1 (38).
217 § 23a Abs. 5 S. 4 bwPolG.
218 Art. 34b Abs. 4 bayPAG.
219 § 33b Abs. 6 S. 3 bbgPolG.
220 § 34a Abs. 6 S. 2 mvSOG.
221 § 33a Abs. 7 S. 2 ndsSOG.
222 § 28b Abs. 3 saarlPolG.
223 § 185a Abs. 4 S. 2 shLVwG.
224 § 34a Abs. 7 thürPAG.

burg, Hessen und Rheinland-Pfalz die bei der Durchführung einer präventiven E-Mail-Überwachung mithelfenden E-Mail-Provider entschädigen muss, wird nicht ausdrücklich geregelt. Zwar gibt es keine ausdrücklichen Regelungen über die Verteilung der Kostenbelastung in diesen drei Bundesländern, jedoch ist der Entschädigungsanspruch der E-Mail-Provider gegenüber der Polizeibehörde nicht abzulehnen. In der Literatur wird vertreten, dass eine Indienstnahme Privater ohne Entschädigung angenommen werden könne, wenn eine Sachnähe, die aus der Sachverantwortung der indienstgenommenen Privaten hergeleitet werde, vorliege[225]. Dies gilt allerdings nicht für die E-Mail-Provider, die bei der Durchführung einer präventiv-polizeilichen E-Mail-Überwachung mithelfen[226]. Da die Gefahrenabwehr, an der sich die E-Mail-Provider beteiligen, die originäre Aufgabe der Polizei darstellt[227], gibt es keine „Sachnähe" der Mitwirkungspflicht der E-Mail-Provider zum von der Polizeibehörde verfolgten Zweck (Gefahrenabwehr)[228]. Ferner sind die E-Mail-Provider, wie bereits dargelegt wurde, nicht verantwortlich für die Gefahr, die die in den polizei- und ordnungsgesetzlichen Ermächtigungsvorschriften zur Telekommunikationsüberwachung vorgeschriebenen Zielpersonen verursachen. Berücksichtigt man, dass sich die E-Mail-Provider als Nichtstörer im Sinne des Polizeirechts betrachten lassen, ist ihr Entschädigungsanspruch jedenfalls wegen der Entschädigung des Nichtstörers im Falle polizeilichen Notstands zu bejahen[229].

C. Rechtsverhältnis zwischen den Anbietern der E-Mail-Dienste und den betroffenen Nutzern der E-Mail-Dienste

I. Privatrechtliche Natur des Rechtsverhältnisses

Das Rechtsverhältnis zwischen den E-Mail-Providern und ihren Kunden, die die E-Mail-Dienste nutzen, wird durch privatrechtliche Verträge begründet. Die privatrechtliche Natur des Rechtsverhältnisses wird nicht durch die Beteiligung der E-Mail-Provider an der Durchführung einer präventiv-polizeilichen E-Mail-Überwachung verändert. Da die Polizeibehörde

225 *Waechter* (Fn. 210), S. 68 (96). Eine solche Meinung findet ihre Grundlage in den vom Bundesverfassungsgericht entwickelten Kriterien für die Zulässigkeit der Sonderabgabe (vgl. dazu BVerfGE 55, 274 (305 ff.)).

226 Vgl. *von Hammerstein*, MMR 2004, S. 222 (226); *Schenke* (Fn. 210), S. 1 (39).

227 Wie bereits im 2. Kapitel ausgeführt wurde, geht es bei der Gefahrenabwehr um die Erfüllung einer staatlichen Schutzpflicht.

228 Vgl. *von Hammerstein* (Fn. 226), S. 222 (226); *Schenke* (Fn. 210), S. 1 (39); *Scholz*, ArchPT 1995, S. 169 (170 f.).

229 *Schenke* (Fn. 210), S. 1 (40).

den E-Mail-Providern die Befugnis zur Telekommunikationsüberwachung nicht überträgt, werden die Tätigkeiten, die die E-Mail-Provider im Rahmen ihrer Mitwirkungspflicht ausüben, der überwachenden Polizeibehörde zugerechnet. Zwischen den E-Mail-Providern und den betroffenen Nutzern der E-Mail-Dienste besteht insoweit kein öffentlich-rechtliches Rechtsverhältnis, das aufgrund einer präventiv-polizeilichen Überwachung des E-Mail-Verkehrs begründet wird.

II. E-Mail-Provider als Vertreter des Fernmeldegeheimnisses der betroffenen Nutzer der E-Mail-Dienste?

Da die E-Mail-Provider ihren Kunden durch privatrechtliche Verträge E-Mail-Dienste anbieten, stellt sich die Frage: Können die E-Mail-Provider für ihre Kunden das Fernmeldegeheimnis des Art. 10 Abs. 1 GG geltend machen und damit die technische Mitwirkung ablehnen? Dies ist zu verneinen. Denn die privaten Unternehmen, die die Telekommunikationsdienstleistungen erbringen, zählen nicht zu den Teilnehmern der Telekommunikation[230]. Sie sind nicht Träger des Grundrechts des Art. 10 Abs. 1 GG[231]. Deswegen lassen sich die E-Mail-Provider nicht als Grundrechtsvertreter der betroffenen Nutzer der E-Mail-Dienste betrachten. Zwar können die E-Mail-Provider den Verwaltungsakt, durch den die überwachende Polizeibehörde eine konkrete Mitwirkungspflicht auferlegt, vor Gericht angehen. Dabei müssten sie sich jedoch nicht auf das Fernmeldegeheimnis ihrer Kunden, sondern auf Art. 12 Abs. 1 GG beziehen.

D. Zusammenfassung des 6. Kapitels

Das Rechtsverhältnis zwischen der überwachenden Polizeibehörde und den betroffenen Nutzern der E-Mail-Dienste wird durch die Maßnahme der präventiv-polizeilichen E-Mail-Überwachung, die als Realakt einzustufen ist, begründet. Die Frage nach dem Wohnsitz oder Aufenthaltsort der Zielpersonen spielt keine Rolle für die örtliche Zuständigkeit der überwachenden Polizeibehörde. Die Zielperson ist in der Regel als Störer im Sinne des Polizeirechts zu qualifizieren. Die Adressaten der Maßnahme präventiv-polizeilicher E-Mail-Überwachung im Vorfeld der Gefahr (potenzielle Straftäter und Kontakt- und Begleitpersonen) sind als Nichtstörer anzusehen, weil im Vorfeld der Gefahr noch keine konkrete Gefahr besteht. Ferner sind mitbetroffene unbeteiligte Dritte, deren E-Mails durch den kontrollierten E-Mail-Knoten übertragen werden, Nichtstörer. Die Konstellation, dass E-Mails unbeteiligter Dritter aus einem technischen Grund vom Überwachungsprogramm virtuell überprüft oder von der Polizei mitgelesen

230 *Gusy* (Fn. 81), Art. 10 Rn. 49; *Hermes* (Fn. 81), Art. 10 Rn. 28.
231 *Gusy* (Fn. 81), Art. 10 Rn. 49; *Hermes* (Fn. 81), Art. 10 Rn. 28.

werden, entspricht dem polizeilichen Notstand jedoch nicht. Das Rechtsverhältnis zwischen der überwachenden Polizeibehörde und den betroffenen Nutzern der E-Mail-Dienste ist asymmetrisch. Dabei geht es um die polizeiliche Informationserhebung ohne die Kenntnis der Betroffenen. Mangels einer Verfahrensbeteiligung des Betroffenen kann der Richtervorbehalt vorbeugend rechtswidrige Überwachungsmaßnahmen verhindern. Allerdings ist die vorbeugende Gerichtskontrolle aufgrund der einseitigen Informationsbasis des Richters nicht immer hinreichend effektiv. Dieses asymmetrische Rechtsverhältnis wird beendet, wenn die Maßnahme der E-Mail-Überwachung abgeschlossen ist. Nach Abschluss der Überwachungsmaßnahme ist die Polizei verpflichtet, die Betroffenen über die verdeckte Informationserhebung zu unterrichten.

Das Rechtsverhältnis zwischen der überwachenden Polizeibehörde und den E-Mail-Providern, die die präventiv-polizeiliche E-Mail-Überwachung ermöglichen müssen, wird durch einen Verwaltungsakt begründet. Wenn sich die E-Mail-Provider, die den Zielpersonen E-Mail-Dienste anbieten, nicht im Gebiet des Bundeslandes der überwachenden Polizeibehörde befinden, geht es um einen polizeilichen grenzüberschreitenden Anspruch auf die technische Hilfe der E-Mail-Provider. Der Anspruch auf die technische Hilfe der E-Mail-Provider, deren Sitz sich im Gebiet eines anderen Bundeslandes befindet, bedarf der Zustimmung des betroffenen Nachbarbundeslandes. Im Vergleich dazu ist ein internationaler grenzüberschreitender Anspruch auf die technische Hilfe eines ausländischen E-Mail-Providers bereits aus praktischen Gründen schwieriger. Denn die in § 110 Abs. 1 Satz 1 TKG geregelte Vorhaltungspflicht der Diensteanbieter gilt nicht für den ausländischen E-Mail-Provider.

Wenn sich die E-Mail-Provider aufgrund der polizeilichen Anordnung an der Durchführung einer präventiv-polizeilichen E-Mail-Überwachung beteiligen, stellen sie einerseits indienstgenommene Private dar. Andererseits lassen sie sich jedoch nicht als Störer ansehen. Insoweit ist ein Entschädigungsanspruch gegenüber der Polizeibehörde, die die präventive E-Mail-Überwachung durchführt, zu bejahen.

Das Rechtsverhältnis zwischen den E-Mail-Providern und den betroffenen Nutzern der E-Mail-Dienste ist privatrechtlich. E-Mail-Provider sind nicht Vertreter ihrer Kunden in Hinblick auf deren Fernmeldegeheimnis.

7. Kapitel: Gerichtlicher Rechtsschutz gegen die Maßnahme der präventiv-polizeilichen E-Mail-Überwachung und die polizeiliche Anordnung der Mitwirkung

In diesem Kapitel wird der gerichtliche Rechtsschutz gegen die Maßnahme präventiv-polizeilicher E-Mail-Überwachung und gegen die polizeiliche Anordnung, nach der sich die E-Mail-Provider an dem präventiv-polizeilichen Zugriff auf die E-Mail-Kommunikation beteiligen müssen, diskutiert. Die statthafte Klageart hängt von der Rechtsnatur der polizeilichen Maßnahmen ab. Wie im 6. Kapitel dargelegt wurde, ist die Maßnahme der präventiv-polizeilichen E-Mail-Überwachung als Realakt einzustufen. Zudem wird das Rechtsverhältnis zwischen der überwachenden Polizeibehörde und den E-Mail-Providern, die bei der Durchführung einer präventiv-polizeilichen E-Mail-Überwachung mitwirken müssen, durch die als Verwaltungsakt zu qualifizierende polizeiliche Anordnung begründet. Ausgehend von der Rechtsnatur dieser polizeilichen Maßnahmen kommen die allgemeine Leistungsklage (gegen die noch laufende oder zukünftige polizeiliche Überwachungsmaßnahme), die Feststellungsklage (gegen die erledigte polizeiliche Überwachungsmaßnahme) und die Anfechtungsklage (gegen die polizeiliche Anordnung der Mitwirkung) in Betracht.

A. Eröffnung des Verwaltungsrechtswegs

Nach der Generalklausel des § 40 Abs. 1 VwGO ist der Verwaltungsrechtsweg in allen öffentlich-rechtlichen Streitigkeiten nichtverfassungsrechtlicher Art gegeben, soweit es keine gesetzliche Sonderzuweisung gibt. Wie im 6. Kapitel bereits dargelegt wurde, sind Verhältnisse, die zwischen der überwachenden Polizeibehörde, den betroffenen Nutzern der E-Mail-Dienste und den E-Mail-Providern entstehen, nicht verfassungsrechtlicher, sondern verwaltungsrechtlicher Art. Hinsichtlich des Rechtsschutzes gegen die Maßnahme der E-Mail-Überwachung, die ihre Rechtsgrundlage in den Polizei- und Ordnungsgesetzen findet, besteht keine gesetzliche Sonderzuweisung, weil diese polizeiliche Maßnahme, wie im 3. Kapitel ausgeführt wurde, in den Bereich der Gefahrenabwehr fällt[1]. Insoweit wird der Rechtsschutz gegen die Maßnahme der präventiv-polizeilichen E-Mail-Überwachung und gegen die polizeiliche Anordnung, nach der sich die E-Mail-

1 Die Unterscheidung, ob die polizeiliche Maßnahme der Gefahrenabwehr oder der Strafverfolgung dient, bestimmt den einschlägigen Rechtsweg (*Schoch*, JURA 2001, S. 628 (629)).

Provider an dem präventiv-polizeilichen Zugriff auf die E-Mail-Kommunikation beteiligen müssen, durch die Verwaltungsgerichtsbarkeit gewährt.

B. Rechtsschutz gegen eine noch laufende oder zukünftige Maßnahme präventiv-polizeilicher E-Mail-Überwachung

I. Allgemeine Leistungsklage als statthafte Klageart

Wegen der Heimlichkeit des Zugriffs auf die E-Mail-Kommunikation bemerken die betroffenen Nutzer der E-Mail-Dienste in der Regel nicht, dass sich eine polizeiliche Überwachungsmaßnahme gegen sie richtet. Allerdings ist es möglich, dass sie zufällig Kenntnis von der noch laufenden oder zukünftigen polizeilichen Informationserhebung erhalten. Insoweit scheidet die Möglichkeit des Rechtsschutzes gegen eine gegenwärtige oder drohende präventiv-polizeiliche E-Mail-Überwachung nicht grundsätzlich aus.

Da die präventiv-polizeiliche E-Mail-Überwachung als Realakt zu qualifizieren ist, stellt die allgemeine Leistungsklage, die in § 43 Abs. 2 VwGO vorausgesetzt wird[2], die statthafte Klageart dar[3]. Dadurch begehren die betroffenen Nutzer der E-Mail-Dienste, die fortdauernde Beeinträchtigung, die sich aus der noch laufenden präventiv-polizeilichen E-Mail-Überwachung ergibt, zu beseitigen[4]. Darüber hinaus können sie durch die Erhebung einer einfachen Unterlassungsklage (allgemeinen Unterlassungsklage), die ein Unterfall der allgemeinen Leistungsklage ist[5], die Unterlassung (der Wiederholung) des Eingriffs begehren[6]. In der Konstellation, dass eine erstmalige Maßnahme präventiv-polizeilicher E-Mail-Überwachung droht, ist eine vorbeugende Unterlassungsklage, die sich auch als Unterform der

2 *von Albedyll*, in: Bader/Funke-Kaiser/Kuntze/von Albedyll, VwGO, § 42 Rn. 113; *Detterbeck*, AllgVerwR, Rn. 1390; *Ehlers*, JURA 2006, S. 351; *Gersdorf*, Verwaltungsprozessrecht, Rn. 100; *Happ*, in: Eyermann, VwGO, § 42 Rn. 62; *Hufen*, Verwaltungsprozessrecht, § 16 Rn. 3; *J. Ipsen*, AllgVerwR, Rn. 1102; *Kopp/W.-R. Schenke*, VwGO, § 43 Rn. 26 ff.; *Lorenz*, Verwaltungsprozessrecht, § 23 Rn. 2; *von Nicolai*, in: Redeker/von Oertzen, VwGO, § 42 Rn. 153; *Pietzcker*, in: Schoch/Schmidt-Aßmann/Pietzner, VwGO, § 42 Abs. 1 Rn. 150; *W.-R. Schenke*, Verwaltungsprozessrecht, Rn. 345; *Schmitt Glaeser/Horn*, Verwaltungsprozessrecht, Rn. 371; *Sodan*, in: Sodan/Ziekow, VwGO, § 42 Rn. 39; *Steiner*, JuS 1984, S. 853; *Würtenberger*, Verwaltungsprozessrecht, Rn. 375.

3 Vgl. *Deutsch*, Erhebung von Informationen, S. 281.

4 *W.-R. Schenke*, PolR, Rn. 663.

5 *von Albedyll* (Fn. 2), § 42 Rn. 117; *Gersdorf* (Fn. 2), Rn. 102; *Hufen* (Fn. 2), § 16 Rn. 1; *Schenke* (Fn. 2), Rn. 354; *Schmitt Glaeser/Horn* (Fn. 2), Rn. 377; *Sodan* (Fn. 2), § 42 Rn. 53.

6 Die einfache Unterlassungsklage (allgemeine Unterlassungsklage) ist statthaft, wenn eine erfolgte Beeinträchtigung bereits vorliegt und der Kläger die Wiederholung eines derartigen Eingriffs abwehren will (*von Albedyll* (Fn. 2), § 42 Rn. 118; *Ehlers* (Fn. 2), S. 351 (354); *Gersdorf* (Fn. 2), Rn. 102; *Pietzcker* (Fn. 2), § 42 Abs. 1 Rn. 162; *Schmitt Glaeser/Horn* (Fn. 2), Rn. 378; *Würtenberger* (Fn. 2), Rn. 486).

allgemeinen Leistungsklage ansehen lässt[7], statthaft[8], weil die vorbeugende Unterlassungsklage darauf gerichtet ist, einen erstmals drohenden rechtswidrigen Realakt zu verhindern[9].

II. Klagebefugnis

Die Klagebefugnis stellt eine Zulässigkeitsvoraussetzung der allgemeinen Leistungsklage dar[10]. Dies ist die Folge der analogen Anwendung von § 42 Abs. 2 VwGO[11], weil die Verpflichtungsklage nach § 42 Abs. 1 VwGO unter dem Aspekt der Klagestruktur eine „besondere Leistungsklage" gegenüber der allgemeinen Leistungsklage ist[12]. Die betroffenen Nutzer der E-Mail-Dienste sind klagebefugt, wenn die Möglichkeit gegeben ist, dass die laufende oder zukünftige präventiv-polizeiliche E-Mail-Überwachung sie rechtswidrig in ihren Rechten verletzt[13].

III. Rechtsschutzbedürfnis

Das Rechtsschutzbedürfnis für eine vorbeugende Unterlassungsklage kann bejaht werden, wenn die Gefahr, dass eine präventiv-polizeiliche E-Mail-Überwachung in Zukunft durchgeführt wird, besteht[14]. In der Konstellation, dass der Kläger vor Klageerhebung nicht bei der Polizeibehörde, die die Maßnahme präventiver E-Mail-Überwachung ergreift, die Unterlassung der Beeinträchtigung, die sich aus der laufenden oder einer zukünftigen präventiv-polizeilichen E-Mail-Überwachung ergibt, oder die Unterlassung des zukünftigen Zugriffs auf seine E-Mail-Kommunikation beantragt, ist das Rechtsschutzbedürfnis zu verneinen[15].

---

7 *von Albedyll* (Fn. 2), § 42 Rn. 117; *Detterbeck* (Fn. 2), Rn. 1444; *Gersdorf* (Fn. 2), Rn. 102; *Hufen* (Fn. 2), § 16 Rn. 1; *Schenke* (Fn. 2), Rn. 354; *Schmitt Glaeser/Horn* (Fn. 2), Rn. 377; *Sodan* (Fn. 2), § 42 Rn. 53; *Würtenberger* (Fn. 2), Rn. 485.

8 Vgl. *Schenke* (Fn. 4), Rn. 663.

9 *von Albedyll* (Fn. 2), § 42 Rn. 119; *Ehlers* (Fn. 2), S. 351 (354); *Gersdorf* (Fn. 2), Rn. 102; *Pietzcker* (Fn. 2), § 42 Abs. 1 Rn. 162; *Schenke* (Fn. 2), Rn. 354; *Schmitt Glaeser/Horn* (Fn. 2), Rn. 379; *Würtenberger* (Fn. 2), Rn. 486. Nach *H. Sodan* ist die terminologische Unterscheidung zwischen einfacher (oder: allgemeiner) und vorbeugender Unterlassungsklage nicht zutreffend, weil die einfache Unterlassungsklage (allgemeine Unterlassungsklage) auch das Ziel hat, der Beeinträchtigung vorzubeugen (*Sodan* (Fn. 2), § 42 Rn. 53).

10 A. A. *Lorenz* (Fn. 2), § 23 Rn. 15.

11 *Detterbeck* (Fn. 2), Rn. 1447; *Ehlers*, VerwArch. 84 (1993), S. 139 (143); *Gersdorf* (Fn. 2), Rn. 103; *Hufen* (Fn. 2), § 16 Rn. 12; *Kopp/Schenke* (Fn. 2), § 42 Rn. 62; *Schenke* (Fn. 2), Rn. 492; *Schmidt-Kötters*, in: Posser/Wolff, VwGO, § 42 Rn. 132; *Sodan* (Fn. 2), § 42 Rn. 371; *Steiner* (Fn. 2), S. 853 (856); *Würtenberger* (Fn. 2), Rn. 390; a. A. *Achterberg*, DVBl. 1981, S. 278 (279), *Erichsen*, DVBl. 1982, S. 95 (100); *Schoch*, JuS 1987, S. 783 (789 f.).

12 *Ehlers* (Fn. 11), S. 139 (143); *Sodan* (Fn. 2), § 42 Rn. 371.

13 Vgl. *Schenke* (Fn. 4), Rn. 663.

14 Vgl. *Detterbeck* (Fn. 2), Rn. 1449.

15 Vgl. *Hufen* (Fn. 2), § 17 Rn. 11; *Lorenz* (Fn. 2), § 23 Rn. 16; *Pietzcker* (Fn. 2), § 42 Abs. 1 Rn. 156; *Schmitt Glaeser/Horn* (Fn. 2), Rn. 388; *Würtenberger* (Fn. 2), Rn. 393; a. A. *Ehlers*

C. Rechtsschutz gegen die erledigte Maßnahme präventiv-polizeilicher E-Mail-Überwachung

I. Feststellungsklage als statthafte Klageart

In den meisten Fällen erfahren die in den polizei- und ordnungsgesetzlichen Ermächtigungsvorschriften zur Telekommunikationsüberwachung genannten Zielpersonen erst durch ihre nachträgliche Benachrichtigung von dem polizeilichen Zugriff auf ihre E-Mail-Kommunikation. Die Beeinträchtigung, die sich aus der präventiv-polizeilichen E-Mail-Überwachung ergibt, ist also bereits abgeschlossen.

Gegen ein solches erledigtes Verwaltungshandeln lässt sich eine Fortsetzungsfeststellungsklage (§ 113 Abs. 1 S. 4 VwGO) oder eine Feststellungsklage (§ 43 Abs. 1 VwGO) erheben. Da die Fortsetzungsfeststellungsklage die Feststellung der Rechtswidrigkeit eines erledigten Verwaltungsakts betrifft, stellt sie keine statthafte Klageart gegen die erledigte Maßnahme präventiv-polizeilicher E-Mail-Überwachung, deren Rechtsnatur Realakt ist, dar[16]. Der Auffassung, dass § 113 Abs. 1 Satz 4 VwGO für eine Klage auf Feststellung der Rechtswidrigkeit eines erledigten Realakts analog anwendbar sein könne[17], ist nicht zuzustimmen[18]. Denn einerseits fehlt mangels des Verwaltungsaktbezugs ein systematischer Zusammenhang zu § 113 Abs. 1 Satz 1 VwGO, der eine analoge Anwendung des § 113 Abs. 1 Satz 4 VwGO rechtfertigen würde[19]. Andererseits wird der Rechtsschutz gegen einen erledigten Realakt bereits durch die Feststellungsklage des § 43 Abs. 1 VwGO sichergestellt[20].

Da die (negative) Feststellungsklage nach § 43 Abs. 1 VwGO auf die Feststellung des Nichtbestehens eines Rechtsverhältnisses gerichtet ist, ist sie als statthafte Klageart gegen die erledigte Maßnahme präventiv-polizeilicher E-Mail-Überwachung zu betrachten[21]. Wie im 6. Kapitel ausgeführt wurde, wird ein Rechtsverhältnis zwischen der überwachenden Polizei-

(Fn. 2), S. 351 (356); *Happ* (Fn. 2), § 42 Rn. 69; *Schenke* (Fn. 2), Rn. 363; *Schenke* (Fn. 4), Rn. 664; *Sodan* (Fn. 2), § 42 Rn. 45.

16 Vgl. *Deutsch* (Fn. 3), S. 281; *Schenke* (Fn. 4), Rn. 667.

17 So *Hufen* (Fn. 2), § 18 Rn. 44; *Redeker*, in: Redeker/von Oertzen, VwGO, § 113 Rn. 36; *Schmidt*, in: Eyermann, VwGO, § 113 Rn. 106.

18 *Detterbeck* (Fn. 2), Rn. 1424; *Ehlers*, JURA 2001, S. 415 (419); *Gersdorf* (Fn. 2), Rn. 88; *Kopp/Schenke* (Fn. 2), § 113 Rn. 116; *Lorenz* (Fn. 2), § 22 Rn. 53; *Rozek*, JuS 1995, S. 414 (416); *Schenke* (Fn. 2), Rn. 337; *Sodan* (Fn. 2), § 42 Rn. 71; *Würtenberger* (Fn. 2), Rn. 645.

19 *Detterbeck* (Fn. 2), Rn. 1424; *Ehlers* (Fn. 18), S. 415 (419); *Gersdorf* (Fn. 2), Rn. 88; *Schenke* (Fn. 2), Rn. 337.

20 *Detterbeck* (Fn. 2), Rn. 1424; *Ehlers* (Fn. 18), S. 415 (419); *Gersdorf* (Fn. 2), Rn. 88; *Kopp/Schenke* (Fn. 2), § 113 Rn. 116; *Schenke* (Fn. 2), Rn. 337; *Schenke* (Fn. 4), Rn. 667; *Sodan* (Fn. 2), § 42 Rn. 71; *Würtenberger* (Fn. 2), Rn. 645.

21 Vgl. *Deutsch* (Fn. 3), S. 281; *Schenke* (Fn. 4), Rn. 667.

behörde und der Zielperson, deren E-Mail-Kommunikation von der Polizeibehörde beobachtet wird, durch die als Realakt zu qualifizierende Maßnahme präventiv-polizeilicher E-Mail-Überwachung begründet. Dies entspricht dem Begriff des Rechtsverhältnisses im Sinne des § 43 Abs. 1 VwGO, der eine aus einem konkreten Sachverhalt aufgrund einer Rechtsnorm des öffentlichen Rechts sich ergebende rechtliche Beziehung einer Person zu einer anderen Person verlangt[22]. Obwohl es um ein vergangenes Rechtsverhältnis geht, kann es einen Gegenstand der Feststellungsklage nach § 43 Abs. 1 VwGO darstellen[23].

Zwar greift die Durchführung einer präventiv-polizeilichen E-Mail-Überwachung, wie im 6. Kapitel dargelegt wurde, auch in das Fernmeldegeheimnis der betroffenen Nichtzielpersonen, deren E-Mails über den kontrollierten E-Mail-Knoten übermittelt und vom E-Mail-Filter virtuell überprüft werden, ein, allerdings werden sie nach der Beendigung präventiv-polizeilicher E-Mail-Überwachung nicht über diesen verdeckten polizeilichen Zugriff auf ihre E-Mail-Kommunikation unterrichtet. In diesem Zusammenhang ist es faktisch kaum möglich, dass diese mitbetroffenen Nichtzielpersonen nachträglich durch die Erhebung einer Feststellungsklage gerichtlichen Rechtsschutz begehren. Die (unbeteiligten) Kommunikationspartner der Zielpersonen und die mitbetroffenen Dritten, deren E-Mails aufgrund technischen Fehlers des Überwachungsprogramms von der Polizei mitgelesen wurden, können durch eine Klage nach § 43 Abs. 1 VwGO die Feststellung der Rechtswidrigkeit der erledigten präventiv-polizeilichen E-Mail-Überwachung, die in ihr Fernmeldegeheimnis eingreift, begehren. Wie im 6. Kapitel ausgeführt wurde[24], sind die Kommunikationspartner der Zielpersonen und die mitbetroffenen Dritten, deren E-Mail (Kopie) wegen technischer Fehler auf den Server der überwachenden Polizeibehörde übertragen wird, nach dem Abschluss der Überwachungsmaßnahme über den beendeten polizeilichen Zugriff auf ihren E-Mail-Verkehr zu unterrichten. Die nachträgliche Benachrichtigung stellt die Basis für die Möglichkeit des gerichtlichen Rechtsschutzes dar.

---

22 Dazu BVerwGE 100, 262 (264); *von Albedyll* (Fn. 2), § 43 Rn. 7; *Brüning*, JuS 2004, S. 882 f.; *Detterbeck* (Fn. 2), Rn. 1395; *Ehlers*, JURA 2007, S. 179 (180); *Gersdorf* (Fn. 2), Rn. 118; *Happ* (Fn. 2), § 43 Rn. 12; *Hufen* (Fn. 2), § 18 Rn. 4, 9 f.; *Ipsen* (Fn. 2), Rn. 1114; *Kopp/Schenke* (Fn. 2), § 43 Rn. 11; *Lorenz* (Fn. 2), § 22 Rn. 3; *Möstl*, in: Posser/Wolff, VwGO, § 43 Rn. 1; *von Nicolai* (Fn. 2), § 43 Rn. 3; *Pietzcker* (Fn. 2), § 43 Rn. 5; *Schenke* (Fn. 2), Rn. 378 ff.; *Schmitt Glaeser/Horn* (Fn. 2), Rn. 328; *Sodan* (Fn. 2), § 43 Rn. 7 f.; *Würtenberger* (Fn. 2), Rn. 400.

23 BVerwGE 92, 172 (174); *von Albedyll* (Fn. 2), § 43 Rn. 21; *Ehlers* (Fn. 22), S. 179 (183); *Gersdorf* (Fn. 2), Rn. 118; *Happ* (Fn. 2), § 43 Rn. 18; *Lorenz* (Fn. 2), § 22 Rn. 11; *Möstl* (Fn. 22), § 43 Rn. 7; *von Nicolai* (Fn. 2), § 43 Rn. 8; *Pietzcker* (Fn. 2), § 43 Rn. 13; *Schenke* (Fn. 4), Rn. 667; *Schmitt Glaeser/Horn* (Fn. 2), Rn. 330; *Sodan* (Fn. 2), § 43 Rn. 16; *Sodan/Kluckert*, VerwArch. 94 (2003), S. 3 (4 ff.); *Würtenberger* (Fn. 2), Rn. 404.

24 Siehe 6. Kapitel A IV.

II. Subsidiarität der Feststellungsklage

Gemäß § 43 Abs. 2 Satz 1 VwGO ist die Feststellungsklage gegenüber der Gestaltungsklage[25] und der Leistungsklage[26] subsidiär[27]. D. h., wenn eine Rechtsschutzmöglichkeit durch eine andere Klageart besteht, ist die Feststellungsklage unzulässig[28]. Da die Rechtsnatur der Maßnahme der präventiv-polizeilichen E-Mail-Überwachung keinen Verwaltungsakt, sondern Realakt darstellt, kann Rechtsschutz gegen diese heimliche polizeiliche Informationserhebung nicht durch die Anfechtungsklage oder die Verpflichtungsklage begehrt werden. Auch die allgemeine Leistungsklage kommt nicht in Betracht, weil die Beeinträchtigung, die sich aus dem präventiv-polizeilichen Zugriff auf die E-Mail-Kommunikation ergibt, bereits beendet ist und nicht mehr durch eine allgemeine Leistungsklage beseitigt werden kann. Demzufolge verletzt die Erhebung der Feststellungsklage gegen eine erledigte Maßnahme präventiv-polizeilicher E-Mail-Überwachung die Subsidiaritätsklausel des § 43 Abs. 2 Satz 1 VwGO nicht.

III. Feststellungsinteresse

Nach § 43 Abs. 1 VwGO ist die Erhebung der Feststellungsklage zulässig, wenn der Kläger ein berechtigtes Interesse an der baldigen Feststellung hat. Der Begriff des „berechtigten Interesses" im Sinne des § 43 Abs. 1 VwGO umfasst nicht nur rechtliche Interessen. Vielmehr umfasst er auch jedes schutzwürdige Interesse wirtschaftlicher oder ideeller Art[29]. Da die präventiv-polizeiliche E-Mail-Überwachung darauf basiert, dass die Zielpersonen die polizeilichen Schutzgüter gefährden und sogar potenzielle Straftäter darstellen, führt diese heimliche polizeiliche Informationserhe-

25 Die Gestaltungsklage im Sinne des § 43 Abs. 2 S. 1 VwGO meint in erster Linie die Anfechtungsklage (*Detterbeck* (Fn. 2), Rn. 1399; *Happ* (Fn. 2), § 43 Rn. 40; *Möstl* (Fn. 22), § 43 Rn. 11).

26 Die Leistungsklage im Sinne des § 43 Abs. 2 S. 1 VwGO umfasst sowohl die Verpflichtungsklage als auch die allgemeine Leistungsklage (*Detterbeck* (Fn. 2), Rn. 1399; *Happ* (Fn. 2), § 43 Rn. 40; *Möstl* (Fn. 22), § 43 Rn. 11).

27 Dazu *Klenke*, NWVBl. 2003, S. 170 ff.; *von Mutius*, VerwArch. 63 (1972), S. 229 ff.

28 *von Albedyll* (Fn. 2), § 43 Rn. 28; *Brüning* (Fn. 22), S. 882 (883); *Detterbeck* (Fn. 2), Rn. 1399; *Ehlers* (Fn. 22), S. 179 (184); *Gersdorf* (Fn. 2), Rn. 119; *Happ* (Fn. 2), § 43 Rn. 41; *Hufen* (Fn. 2), § 18 Rn. 5; *Ipsen* (Fn. 2), Rn. 1116; *Kopp/Schenke* (Fn. 2), § 43 Rn. 26; *Möstl* (Fn. 22), § 43 Rn. 11 f.; *von Nicolai* (Fn. 2), § 43 Rn. 25; *Pietzcker* (Fn. 2), § 43 Rn. 40; *Schenke* (Fn. 2), Rn. 416; *Schmitt Glaeser/Horn* (Fn. 2), Rn. 337; *Sodan* (Fn. 2), § 43 Rn. 113; *Würtenberger* (Fn. 2), Rn. 412.

29 BVerwGE 74, 1 (4); *von Albedyll* (Fn. 2), § 43 Rn. 18; *Brüning* (Fn. 22), S. 882 (885); *Ehlers* (Fn. 22), S. 179 (186); *Gersdorf* (Fn. 2), Rn. 125; *Happ* (Fn. 2), § 43 Rn. 30; *Hufen* (Fn. 2), § 18 Rn. 13; *Ipsen* (Fn. 2), Rn. 1119; *Möstl* (Fn. 22), § 43 Rn. 19; *Schenke* (Fn. 2), Rn. 571; *Kopp/Schenke* (Fn. 2), § 43 Rn. 23.

bung zur Diskriminierung[30]. Wenn man berücksichtigt, dass die diskriminierende Wirkung der erledigten präventiv-polizeilichen E-Mail-Überwachung durch die gerichtliche Entscheidung der Feststellungsklage beseitigt werden kann, ist das Feststellungsinteresse (hier: ideelles Interesse bzw. die Rehabilitierung) der Zielperson, deren E-Mail-Kommunikation von der Polizeibehörde beobachtet worden ist, zu bejahen[31]. Das Feststellungsinteresse mitbetroffener Dritter (Kommunikationspartner der Zielperson oder andere betroffene Nutzer der E-Mail-Dienste) ist auch zu bejahen, weil sie durch die Entscheidung des Gerichts feststellen lassen können, dass die Polizeibehörde nicht mit ihnen ein Rechtsverhältnis, in dem in ihr Fernmeldegeheimnis eingegriffen wird, begründen durfte[32]. In Bezug auf das Feststellungsinteresse kann die Annahme, dass die Gefahr der Wiederholung des polizeilichen Zugriffs auf den E-Mail-Verkehr bestehe[33], zutreffend sein, wenn der Kläger nur die gerichtliche Feststellung der erledigten Überwachungsmaßnahmen, die möglicherweise wiederholt werden, begehrt. In dieser Situation kann Art. 10 Abs. 1 GG (Schutz des Fernmeldegeheimnisses) aufgrund der möglichen Wiederholung der Überwachungsmaßnahme als Grundlage für das Feststellungsinteresse angesehen werden. Wenn der Kläger die Unterlassung (der Wiederholung) der Überwachungsmaßnahmen begehrt, ist eine vorbeugende Unterlassungsklage zu erheben. In dieser Konstellation ist die Erhebung der Feststellungsklage aufgrund der Subsidiaritätsklausel des § 43 Abs. 2 Satz 1 VwGO unzulässig[34].

IV. Klagebefugnis?

Ob der Kläger bei der Erhebung der Feststellungsklage behaupten muss, dass die Maßnahme präventiv-polizeilicher E-Mail-Überwachung, die die Entstehungsbedingung des feststellungsfähigen Rechtsverhältnisses darstellt, ihn in seinen Rechten beeinträchtigt, ist umstritten. Nach Ansicht des Bundesverwaltungsgerichts ist das Erfordernis der Klagebefugnis für die Feststellungsklage nach § 43 Abs. 1 VwGO ein Ergebnis der analogen

30 Vgl. BVerwG NJW 1997, S. 2534; *von Albedyll* (Fn. 2), § 43 Rn. 18, 21; *Schenke* (Fn. 4), Rn. 669.

31 Vgl. BVerwG NJW 1997, S. 2534; *von Albedyll* (Fn. 2), § 43 Rn. 18, 21; *Schenke* (Fn. 4), Rn. 669.

32 Die „Unvermeidbarkeitsklausel", die in polizei- und ordnungsgesetzlichen Ermächtigungsvorschriften zur Telekommunikationsüberwachung enthalten ist, kann als solche den Eingriff in das Fernmeldegeheimnis mitbetroffener Dritter nicht rechtfertigen. Wie im 6. Kapitel betont wurde (siehe 6. Kapitel A II 1 a)), besagt die „Unvermeidbarkeitsklausel" nur, dass die Möglichkeit des Eingriffs in Grundrechte mitbetroffener Dritter, der sich aus technischem Grund ergibt, keine negative Voraussetzung der Durchführung einer präventiv-polizeilichen Telekommunikationsüberwachung darstellt. Dabei geht es nicht um die Frage nach der Verfassungsmäßigkeit des Eingriffs in Grundrechte mitbetroffener Dritter.

33 Vgl. *Schenke* (Fn. 4), Rn. 669.

34 Dies ist allerdings streitig. Zum Streitstand *Würtenberger* (Fn. 2), Rn. 485.

Anwendung von § 42 Abs. 2 VwGO[35]. Diese vom Bundesverwaltungsgericht vertretene Meinung überzeugt jedoch nicht[36]. Denn es fehlt an einer Regelungslücke, die die Voraussetzung der analogen Anwendung von § 42 Abs. 2 VwGO ist[37]. § 43 Abs. 1 VwGO verlangt ausdrücklich nur, dass der Kläger ein berechtigtes Interesse an der baldigen Feststellung besitzen muss[38]. Berücksichtigt man, dass der Begriff des „berechtigten Interesses" im Sinne des § 43 Abs. 1 VwGO nicht nur ein rechtliches, sondern auch ein wirtschaftliches oder ideelles Interesse enthält, ist nicht zu verneinen, dass § 43 Abs. 1 VwGO eine eigene, weniger strenge Sonderregelung gegenüber § 42 Abs. 2 VwGO schafft[39].

V. Begründetheit

Die negative Feststellungsklage ist begründet, wenn das streitige Rechtsverhältnis nicht besteht[40]. Zu prüfen ist vor allem, ob die Maßnahme präventiv-polizeilicher E-Mail-Überwachung, die als die Entstehungsbedingung des Rechtsverhältnisses zwischen der überwachenden Polizeibehörde und den betroffenen Nutzern der E-Mail-Dienste angesehen wird, rechtsmäßig ist.

D. Rechtsschutz der E-Mail-Provider gegen die polizeiliche Anordnung der Mitwirkung

I. Anfechtungsklage als statthafte Klageart

Die Anfechtungsklage nach § 42 Abs. 1 VwGO zielt auf die Aufhebung eines Verwaltungsakts. Deswegen setzt die Erhebung der Anfechtungsklage voraus, dass ein (belastender) Verwaltungsakt existiert[41]. Da die Anordnung, durch die die Polizeibehörde den E-Mail-Providern die konkrete Mit-

35 BVerwGE 100, 262 (271); 111, 276 (279); vgl. auch *von Albedyll* (Fn. 2), § 43 Rn. 24; *Brüning* (Fn. 22), S. 882 (884 f.); *Ehlers* (Fn. 22), S. 179 (188).

36 *Gersdorf* (Fn. 2), Rn. 120; *Hufen* (Fn. 2), § 18 Rn. 17; *Ipsen* (Fn. 2), Rn. 1122; *Kopp/Schenke* (Fn. 2), § 42 Rn. 63; *Laubinger*, VerwArch. 82 (1991), S. 459 (491 ff.); *Schenke* (Fn. 2), Rn. 410; *Schmitt Glaeser/Horn* (Fn. 2), Rn. 341; *Schoch* (Fn. 11), S. 783 (789 f.); *Sodan* (Fn. 2), § 42 Rn. 374; *Würtenberger* (Fn. 2), Rn. 425.

37 *Hufen* (Fn. 2), § 18 Rn. 17; *Ipsen* (Fn. 2), Rn. 1122; *Kopp/Schenke* (Fn. 2), § 42 Rn. 63; *Schenke* (Fn. 2), Rn. 410; *Sodan* (Fn. 2), § 42 Rn. 374; *Würtenberger* (Fn. 2), Rn. 425.

38 *Würtenberger* (Fn. 2), Rn. 425.

39 *Würtenberger* (Fn. 2), Rn. 425. Folgt man der Meinung, dass § 42 Abs. 2 VwGO bei der Klage nach § 43 VwGO analog anzuwenden sei, wäre die Erhebung einer Feststellungsklage, deren Zweck die Sicherung rein wirtschaftlicher oder ideeller Interessen ist, praktisch ausgeschlossen (*Gersdorf* (Fn. 2), Rn. 120).

40 *Hufen* (Fn. 2), § 29 Rn. 3; *Schenke* (Fn. 2), Rn. 870; *Schmitt Glaeser/Horn* (Fn. 2), Rn. 351; *Würtenberger* (Fn. 2), Rn. 430.

41 *Detterbeck* (Fn. 2), Rn. 1350; *Hufen* (Fn. 2), § 14 Rn. 2; *Schenke* (Fn. 2), Rn. 182; *Sodan* (Fn. 2), § 42 Rn. 16; *Würtenberger* (Fn. 2), Rn. 269.

wirkungspflicht auferlegt, als Verwaltungsakt zu qualifizieren ist, stellt die Anfechtungsklage die statthafte Klageart gegen diese polizeiliche Anordnung der Mitwirkung dar.

II. Klagebefugnis

Gemäß § 42 Abs. 2 VwGO muss der Kläger geltend machen, dass seine Rechte durch den Verwaltungsakt möglicherweise verletzt sind. Wenn die vom Kläger geltend gemachte Rechtsverletzung möglich ist, ist der Kläger klagebefugt (Möglichkeitstheorie)[42]. Der E-Mail-Provider, der Adressat des polizeilichen Verwaltungsakts ist und damit bei der Durchführung der präventiv-polizeilichen E-Mail-Überwachung mithelfen muss, ist, wie im 6. Kapitel dargelegt wurde, kein Grundrechtsvertreter der betroffenen Nutzer der E-Mail-Dienste. Bei der Erhebung der Anfechtungsklage kann er nicht die Verletzung des Grundrechts der betroffenen Telekommunikationsteilnehmer geltend machen. Die Verletzung des Fernmeldegeheimnisses, die sich aus der Durchführung der präventiv-polizeilichen E-Mail-Überwachung ergibt, muss von den betroffenen Nutzern der E-Mail-Dienste selbst durch Erhebung der entsprechenden Klagen festgestellt oder unterbunden werden. Davon abgesehen sind E-Mail-Provider als Adressaten eines möglicherweise rechtswidrigen Eingriffs in Art. 12 Abs. 1 GG klagebefugt.

III. Aufschiebende Wirkung

Nach § 80 Abs. 1 Satz 1 VwGO haben Widerspruch und Anfechtungsklage aufschiebende Wirkung. Wenn ein Widerspruch oder eine Anfechtungsklage gegen die polizeiliche Anordnung, durch die der E-Mail-Provider (Kläger) bei der Durchführung einer präventiv-polizeilichen E-Mail-Überwachung mithelfen muss, erhoben wird, kann die Polizeibehörde diesen Verwaltungsakt vorläufig nicht vollstrecken[43]. Dem kann aber durch die Anordnung der sofortigen Vollziehbarkeit begegnet werden.

---

42 BVerwGE 95, 333 (334 f.); *von Albedyll* (Fn. 2), § 42 Rn. 100; *Detterbeck* (Fn. 2), Rn. 1351; *Gersdorf* (Fn. 2), Rn. 28; *Happ* (Fn. 2), § 42 Rn. 93; *Hufen* (Fn. 2), § 14 Rn. 108; *Ipsen* (Fn. 2), Rn. 1052 f.; *Kopp/Schenke* (Fn. 2), § 42 Rn. 66; *Lorenz*, § 18 Rn. 11; *von Nicolai* (Fn. 2), § 42 Rn. 20; *Schenke* (Fn. 2), Rn. 494; *Schmitt Glaeser/Horn* (Fn. 2), Rn. 155; *Schmidt-Kötters* (Fn. 11), § 42 Rn. 175; *Sodan* (Fn. 2), § 42 Rn. 379; *Würtenberger* (Fn. 2), Rn. 274.

43 In Bezug auf die Bedeutung der aufschiebenden Wirkung nach § 80 Abs. 1 S. 1 VwGO gibt es einen Meinungsstreit zwischen der strengen Wirksamkeitstheorie (*Erichsen/Klenke*, DÖV 1976, S. 833 (834 ff.); *Erichsen*, JURA 1984, S. 414 (423)), der eingeschränkten Wirksamkeitstheorie (*Funke-Kaiser*, in: Bader/Funke-Kaiser/Kuntze/von Albedyll, VwGO, § 80 Rn. 20; *Kopp/Schenke* (Fn. 2), § 80 Rn. 22; *Puttler*, in: Sodan/Ziekow, VwGO, § 80 Rn. 35; *Schenke* (Fn. 2), Rn. 950; *Schmidt* (Fn. 17), § 80 Rn. 6; *Schoch*, in: Schoch/Schmidt-Aßmann/Pietzner, VwGO, § 80 Rn. 85 ff.) und der Vollziehbarkeitstheorie (BVerwGE 13, 1 (5 ff.); 66, 218 (222); *Detterbeck* (Fn. 2), Rn. 1478; *Gersdorf*, in: Posser/Wolff, VwGO, § 80 Rn. 29; *Gersdorf* (Fn. 2),

IV. Anhörung der Adressaten der präventiv-polizeilichen E-Mail-Überwachung im Widerspruchsverfahren und ihre Beteiligung im Anfechtungsklageverfahren?

Schließlich stellt sich die Frage: Kann die Anhörungspflicht im Widerspruchsverfahren[44] und im Verfahren der Anfechtungsklage, die der betroffene E-Mail-Provider gegen die polizeiliche Anordnung erhebt[45], auch für die Person, deren E-Mail-Verkehr von der Polizeibehörde durch technische Hilfe der E-Mail-Provider überwacht wird, gelten? Eine Anhörung der Zielpersonen, die die Adressaten der präventiv-polizeilichen E-Mail-Überwachung sind, ist wegen des Geheimhaltungsbedarfs der Überwachungsmaßnahme doch logisch nicht möglich. Aus der Sicht der Rechtsdogmatik ist die Anwendbarkeit der in § 71 VwGO vorgeschriebenen Anhörung für die Adressaten der präventiv-polizeilichen E-Mail-Überwachung ebenfalls abzulehnen. Unter dem Begriff des „Betroffenen" im Sinne des § 71 VwGO wird derjenige verstanden, der durch die Aufhebung des angefochtenen Verwaltungsakts oder durch dessen Änderung durch einen Abhilfe- oder Widerspruchsbescheid beschwert wird[46]. Erfasst werden sowohl der Widerspruchsführer selbst als auch ein bislang Drittbegünstigter[47]. Da der Adressat der präventiv-polizeilichen E-Mail-Überwachung weder den Widerspruchsführer noch eine durch die Anfechtung des angefochtenen Verwaltungsakts beschwerte dritte Person darstellt[48], ist § 71 VwGO nicht anwendbar.

Rn. 141; *Hufen* (Fn. 2), § 32 Rn. 3; *Redeker* (Fn. 17), § 80 Rn. 4; *Schmitt Glaeser/Horn* (Fn. 2), Rn. 250). Allerdings besteht in der Praxis nur ein geringer Unterschied zwischen der eingeschränkten Wirksamkeitstheorie und der Vollziehbarkeitstheorie (*Detterbeck* (Fn. 2), Rn. 1478; *Lorenz* (Fn. 2), § 28 Rn. 8; *Redeker* (Fn. 17), § 80 Rn. 5). Berücksichtigt man, dass die aufschiebende Wirkung nach § 80 Abs. 1 S. 1 VwGO einen vorläufigen Rechtsschutz gegen Verwaltungsakte gewährt, ist die eingeschränkte Wirksamkeitstheorie zutreffend. Denn nach der Vollziehbarkeitstheorie verliert § 80 Abs. 1 S. 1 VwGO seine Funktion des vorläufigen Rechtsschutzes, wenn der Gegenstand des Widerspruchs oder der Anfechtungsklage ein rechtsgestaltender oder feststellender Verwaltungsakt ist.

44 Nach § 71 VwGO soll der Betroffene vor Erlass des Abhilfebescheids oder des Widerspruchsbescheids gehört werden, wenn die Aufhebung oder Änderung eines Verwaltungsakts im Widerspruchsverfahren erstmalig mit einer Beschwer verbunden ist.

45 Gemäß § 84 Abs. 1 S. 2 VwGO sind die Beteiligten vor dem Erlass eines Gerichtsbescheids anzuhören.

46 *Funke-Kaiser* (Fn. 43) § 71 Rn. 2; *Hüttenbrink*, in: Posser/Wolff, VwGO, § 71 Rn. 2; *Kothe*, in: Redeker/von Oertzen, VwGO, § 71 Rn. 2; *Rennert*, in: Eyermann, VwGO, § 71 Rn. 2.

47 *Funke-Kaiser* (Fn. 43), § 71 Rn. 2; *Hüttenbrink* (Fn. 46), § 71 Rn. 2; *Kopp/Schenke* (Fn. 2), § 71 Rn. 2; *Kothe* (Fn. 46), § 71 Rn. 1a; *Rennert* (Fn. 46), § 71 Rn. 2f.

48 Gerade umgekehrt: Wenn der Verwaltungsakt, der eine Mitwirkung der E-Mail-Provider am präventiv-polizeilichen Zugriff auf die E-Mail-Kommunikation regelt, aufgehoben wird, hat die Person, deren E-Mail-Kommunikation von der Polizeibehörde durch technische Hilfe der E-Mail-Provider überwacht wird, dadurch einen Vorteil.

Eine andere Frage ist, ob die Zielpersonen polizeilicher Telekommunikationsüberwachung in einem Anfechtungsverfahren der E-Mail-Provider beizuladen sind und somit rechtliches Gehör erhalten. Nach § 63 Nr. 3 VwGO fällt auch der Beigeladene unter den Begriff der Beteiligten. Bei der Beiladung lässt sich zwischen einfacher (§ 65 Abs. 1 VwGO) und notwendiger (§ 65 Abs. 2 VwGO) Beiladung differenzieren[49]. Bei der einfachen Beiladung geht es darum, dass die rechtlichen Interessen eines Dritten durch die gerichtliche Entscheidung des Rechtsstreits berührt werden. Im Vergleich dazu wird eine notwendige Beiladung angenommen, wenn der beizuladende Dritte an dem streitigen Rechtsverhältnis derart beteiligt ist, dass die gerichtliche Entscheidung auch ihm gegenüber nur einheitlich ergehen kann. Notwendig beizuladen ist im Verfahren der Anfechtungsklage derjenige, der durch die Aufhebung des angefochtenen Verwaltungsakts unmittelbar rechtlich beschwert wird[50]. Streitgegenstand des Anfechtungsverfahrens ist allein die Mitwirkungspflicht der E-Mail-Provider an der polizeilichen Überwachungsmaßnahme. Ob diese besteht, berührt keinesfalls die rechtlichen Interessen von Zielpersonen. Demzufolge werden die Voraussetzungen bereits der einfachen Beiladung nicht erfüllt. Eine notwendige Beiladung liegt auch nicht vor, weil die gerichtliche Entscheidung der vom E-Mail-Provider erhobenen Anfechtungsklage getroffen werden kann, ohne dass dadurch gleichzeitig unmittelbar und zwangsläufig Rechte einer Zielperson, deren E-Mail-Kommunikation von der Polizeibehörde überwacht wird, negativ betroffen werden[51]. Da die in den polizei- und ordnungsgesetzlichen Ermächtigungsvorschriften zur Telekommunikationsüberwachung genannten Zielpersonen im Verfahren der vom E-Mail-Provider erhobenen Anfechtungsklage nicht beizuladen sind und daher dem Begriff des Beteiligten (§ 63 Nr. 3 in Verbindung mit § 65 Abs. 1 und 2 VwGO) nicht entsprechen, erlangen sie keine verfahrensrechtliche Sicherung.

E. Zusammenfassung des 7. Kapitels

Die statthafte Klageart gegen die polizeiliche Maßnahme hängt von der Rechtsnatur des streitigen polizeilichen Handelns ab. Gegen eine Maß-

49 Zur Beiladung im Verwaltungsprozess *Nottbusch*, Beiladung; *Stober*, in: Erichsen, FS Menger, S. 401 ff.

50 *Czybulka*, in: Sodan/Ziekow, VwGO, § 65 Rn. 127; *Kintz*, in: Posser/Wolff, VwGO, § 65 Rn. 13; *Redeker* (Fn. 17), § 65 Rn. 8; *Kopp/Schenke* (Fn. 2), § 65 Rn. 17; *Schmidt* (Fn. 17), § 65 Rn. 16.

51 Dies ist selbstverständlich, weil die polizeiliche Anordnung, durch die sich die E-Mail-Provider an der Durchführung präventiv-polizeilicher E-Mail-Überwachung beteiligen müssen, die in den polizei- und ordnungsgesetzlichen Ermächtigungsvorschriften zur Telekommunikationsüberwachung genannten Zielpersonen nicht begünstigt.

nahme der präventiv-polizeilichen E-Mail-Überwachung kommt die allgemeine Leistungsklage oder die Feststellungsklage in Betracht, weil es sich um einen Realakt handelt. Im Vergleich dazu können die E-Mail-Provider nur durch eine Anfechtungsklage Rechtsschutz gegen die als Verwaltungsakt zu qualifizierende Anordnung, durch die die Polizeibehörde ihnen eine Mitwirkungspflicht auferlegt, begehren.

8. Kapitel: Zusammenfassung

Die Ergebnisse dieser Arbeit werden im Folgenden noch einmal zusammengefasst.

Zum 2. Kapitel

1. Im Digitalzeitalter haben territoriale Grenzen immer weniger Bedeutung für den Informationsaustausch. Die im Internet übermittelten Informationen sind wegen der Digitalisierung der Daten grundsätzlich weltweit abrufbar. Da das Internet nach seiner technischen Entwicklung eine weltumspannende Allgemeinzugänglichkeit hat, lässt es sich als Informationsquelle im Sinne des Art. 5 Abs. 1 Satz 1 Hs. 2 GG ansehen. Der Umstand, dass das Internet als eine Informationsquelle betrachtet wird, ist zugleich von Bedeutung für den Schutz anderer Grundrechte. Insoweit wird das Internet aufgrund seines Charakters als Informationsquelle zu einem bedeutsamen Raum der Grundrechte. Berücksichtigt man die Wechselwirkung zwischen öffentlicher Meinung und dem Staatswillen, trägt das Internet auch zur Demokratie in der Informationsgesellschaft bei. Denn das Internet bietet die Möglichkeit des weltumspannenden Informationsaustauschs. Dies befördert die pluralistische öffentliche Meinungsbildung.

2. Aufgrund des Missbrauchs wird das Internet nach und nach zu einem Gefahrenträger. Das Internet bietet Möglichkeiten für die Computer-, bzw. Internet- Kriminalität. Zudem nehmen verbotene Inhalte des Internets (z. B. Pornografie oder Extremismus) zu. Ferner erschwert das Internet die Bekämpfung des Terrorismus, wenn Terroristen zum Informationsaustausch anonyme Internetdienste verwenden. Diese im Internet bestehenden Gefährdungslagen schädigen mit hinreichender Wahrscheinlichkeit die polizeilichen Schutzgüter. Sie entsprechen dem Begriff der Gefahr im Sinne des Polizeirechts. Insoweit führt der Umstand, dass das Internet einen Gefahrenträger darstellt, dazu, dass das Internet ein neuer Zuständigkeitsraum der Polizei im Digitalzeitalter ist.

3. Aus der objektiv-rechtlichen Grundrechtsdimension ergibt sich die Schutzpflicht des Staates. Danach ist der Staat verpflichtet, eine Verletzung der grundrechtlich geschützten Rechtsgüter, die von privaten Dritten verursacht wird, zu verhindern. Da das Internet zu einem Gefahrenträger in der Informationsgesellschaft wird, gilt die Grundrechtsfunktion der staatlichen Schutzpflicht auch im Internet. Der Staat ist verpflichtet, die grundrechtlichen Gefährdungslagen, die sich im Internet aus Aktivitäten von pri-

vaten Dritten ergeben, zu verhindern. Unter dem Aspekt des Untermaßverbots, das bei der Erfüllung der staatlichen Schutzpflicht zu beachten ist, ist der Gesetzgeber verpflichtet, der Exekutive hinreichende Ermächtigungsgrundlagen zu geben, um die staatliche Schutzpflicht im Internet effektiv und wirksam zu erfüllen. Da das Ziel der staatlichen Schutzpflicht darin liegt, dass die aus den Tätigkeiten von privaten Dritten hergeleitete Verletzung der grundrechtlich geschützten Rechtsgüter „verhindert" werden kann, haben präventive Schutzmaßnahmen einen Vorrang gegenüber repressiven Schutzmaßnahmen. Insoweit muss der Gesetzgeber der Polizei hinreichende Befugnisse zur Gefahrenabwehr im Internet einräumen. Bei der Erfüllung der staatlichen Schutzpflicht darf keine verfassungswidrige Schutzmaßnahme gewählt werden. Dieser Grundsatz ist insbesondere bei der Wahl der Mittel zur Gefahrenabwehr im Internet zu beachten.

4. Unter dem Begriff der Telekommunikation in Art. 73 Abs. 1 Nr. 7 und Art. 87 f n. F. GG versteht man die körperlose Übermittlung der Informationen mit technischen Mitteln. Dem entspricht die Legaldefinition der Telekommunikation in § 3 Nr. 22 TKG. Aufgrund des körperlosen Übertragungsvorgangs der digitalen Informationen ist der E-Mail-Verkehr von der Legaldefinition der Telekommunikation in § 3 Nr. 22 TKG erfasst. Mithin sind die E-Mail-Dienste als Telekommunikationsdienste (§ 3 Nr. 24 TKG) zu qualifizieren. Darüber hinaus fallen die E-Mail-Dienste medienrechtlich in den Begriffsbereich der Telemedien, die nach § 1 Abs. 1 TMG auch die „überwiegend" in der Übertragung von Signalen über Telekommunikationsnetze bestehenden Telekommunikationsdienste umfassen. Denn die E-Mail-Dienste bieten neben der Übertragungsdienstleistung noch eine inhaltliche Dienstleistung an.

5. Zur Gefahrenabwehr im Internet kommt zunächst die Verhinderung und Beseitigung der verbotenen Internetinhalte in Betracht. Darüber hinaus ist auch die Überwachung der Internet-basierten Telekommunikation zu berücksichtigen. Ferner ist an die Online-Durchsuchung zu denken. Da gemäß § 59 Abs. 2 und Abs. 3 RStV nur die nach Landesrecht bestimmte Aufsichtsbehörde für die Überwachung telemedienrechtlicher Vorschriften und die Durchführung erforderlicher Maßnahmen gegenüber dem Anbieter zuständig ist, hat die Polizeibehörde in diesem Bereich keine Zuständigkeiten. Wegen der Struktur der virtuellen Welt erleichtern die Mittel der Online-Telekommunikation die Übertragung „gefährlicher Informationen". Dies führt dazu, dass die Überwachung der Internet-basierten Telekommunikation zu einer neuen Möglichkeit der Gefahrenabwehr im Digitalzeitalter wird. Allerdings trifft der präventiv-polizeiliche Zugriff auf die Online-Telekommunikation, der in den meisten Bundesländern eine Rechtsgrundlage findet, den sensiblen Nerv der Grundrechte, weil die Daten der Internet-basierten Telekommunikation (z. B. IP- oder E-Mail-Adresse), die als personenbezogene Daten anzusehen sind, heimlich erho-

ben werden. Von der Überwachung der Online-Telekommunikation zu unterscheiden ist die Online-Durchsuchung, die eine Durchsuchung eines Computers nach in ihm gespeicherten Daten darstellt. Die Online-Durchsuchung stellt keine Überwachung der Telekommunikation, sondern eine Überwachung durch Telekommunikation dar. Die Online-Durchsuchung hat eine Ergänzungsfunktion gegenüber der Telekommunikationsüberwachung. Zurzeit findet die präventive Online-Durchsuchung ihre Rechtsgrundlage in § 20 k BKA-Gesetz und Art. 34 d bayPAG.

6. Das häufigste technische Mittel der E-Mail-Überwachung ist das Abfangen der Datenpakete. Mit der Suche nach einschlägigen Stichworten (z. B. bestimmte Namen oder E-Mail-Adressen) kann der von der überwachenden Polizeibehörde eingesetzte E-Mail-Filter die über den kontrollierten Internet-Knoten übermittelten E-Mail-Datenpakete analysieren und damit „gefährliche" E-Mails finden. Die Kopie der so gefundenen E-Mails wird durch die „Sina-Box" auf den Server der überwachenden Polizeibehörde übertragen. Da das Abfangen der E-Mail technisch dazu führt, dass die Kopfzeile und der Inhalt der E-Mail zugleich mitgelesen werden, handelt es sich bei der E-Mail-Überwachung sowohl um die Erhebung der Telekommunikationsverkehrsdaten (§ 3 Nr. 30 TKG) als auch um die Erhebung der Telekommunikationsinhaltsdaten. Die bei der E-Mail-Überwachung erhobenen Telekommunikationsverkehrsdaten sind z. B. die E-Mail-Adresse des Absenders und Empfängers und der Zeitpunkt des Absendens der E-Mail.

7. Die präventiv-polizeiliche E-Mail-Überwachung hat in den meisten Bundesländern eine ausdrückliche Rechtsgrundlage. In Baden-Württemberg, Bayern, Brandenburg, Hamburg, Hessen, Mecklenburg-Vorpommern, Niedersachsen, Rheinland-Pfalz, Saarland, Schleswig-Holstein und Thüringen gibt es polizei- und ordnungsgesetzliche Ermächtigungsvorschriften zum präventiv-polizeilichen Zugriff auf die Telekommunikation. Obwohl die E-Mail-Dienste dem Begriff der Telemedien entsprechen, kann § 59 RStV, nach dem die zuständige Aufsichtsbehörde bei einem Verstoß gegen die Bestimmungen des TMG die zur Beseitigung des Verstoßes erforderlichen Maßnahmen gegenüber dem Anbieter ergreifen kann, nicht als eine Rechtsgrundlage für die präventiv-polizeiliche E-Mail-Überwachung betrachtet werden. Denn die Polizeibehörde ist nicht Aufsichtsbehörde im Sinne des § 59 RStV. Aus dieser Vorschrift kann die Polizeibehörde keine Befugnis ableiten. Zudem beziehen sich die in § 59 Abs. 3 RStV vorgeschriebenen „zur Beseitigung des Verstoßes erforderlichen Maßnahmen" auf die Untersagung oder die Sperrung der Diensteangebote. Die E-Mail-Überwachung ist begrifflich jedoch keine Unterbrechung der E-Mail-Kommunikationsverbindung.

Zum 3. Kapitel

1. In Deutschland gilt ein Dualismus polizeilicher Aufgaben. Einerseits weist § 163 StPO der Polizei die Aufgabe der Strafverfolgung zu. Andererseits gehört die Gefahrenabwehr nach den Polizei- und Ordnungsgesetzen gleichfalls zu den Aufgaben der Polizei. Die Strafverfolgung, die eine bereits geschehene Straftat voraussetzt, ist die repressive Aufgabe der Polizei. Dagegen stellt die Gefahrenabwehr, deren Ausgangspunkt zukunftsgerichtete Prognose ist, die präventive Aufgabe der Polizei dar. Aufgrund dieser Zwecksdifferenzierung ist die in den Polizei- und Ordnungsgesetzen vorgeschriebene Telekommunikationsüberwachung ein präventiv-polizeilicher Zugriff auf die Telekommunikation. Diese präventive Maßnahme dient der Gefahrenabwehr.

2. Über die Gefahrenabwehr hinaus verfolgen einige polizei- und ordnungsgesetzliche Ermächtigungsvorschriften zur Telekommunikationsüberwachung auch den Zweck der vorbeugenden Straftatenbekämpfung. Unter dem Begriff der vorbeugenden Straftatenbekämpfung versteht man sowohl die Straftatenverhütung als auch die Strafverfolgungsvorsorge. Die Straftatenverhütung stellt eine Gefahrenvorsorge, die in den Bereich der Gefahrenabwehr fällt, dar. Deswegen überschreitet eine in den Polizei- und Ordnungsgesetzen vorgeschriebene Telekommunikationsüberwachung, die der Straftatenverhütung dient, die Grenze zur Strafverfolgung nicht.

3. Der Ausgangspunkt der Strafverfolgungsvorsorge liegt darin, die künftigen strafprozessualen Ermittlungen oder Aufklärungen zu ermöglichen oder zu erleichtern. Da die Strafverfolgungsvorsorge die Situation betrifft, in der die Verletzung des Strafrechts (in der Zukunft) realisiert und nicht mehr zu verhindern ist, steht sie im Widerspruch zur Gefahrenabwehr. Aus diesem Grund ist die Strafverfolgungsvorsorge der Strafverfolgung zuzuordnen.

4. Da sich der in den Polizei- und Ordnungsgesetzen verwendete Begriff der vorbeugenden Straftatenbekämpfung nur auf die Straftatenverhütung bezieht, stellt die vorbeugende Straftatenbekämpfung einen Teil der Gefahrenabwehr dar. Eine im Vorfeld der Gefahr durchgeführte präventiv-polizeiliche Telekommunikationsüberwachung, die der vorbeugenden Straftatenbekämpfung dient, überschreitet die Grenze zur Strafverfolgung nicht.

Zum 4. Kapitel

1. Da die E-Mail unkörperlich durch die Internet-Technik übertragen wird, fällt eine E-Mail-Kommunikation in den Schutzbereich des Fernmeldegeheimnisses des Art. 10 Abs. 1 GG. Geschützt sind nicht nur Inhalte der E-Mail, sondern auch die Umstände der E-Mail-Kommunikation (= Kommunikationsverkehrsdaten im Sinne des TKG). Die präventiv-polizeiliche

E-Mail-Überwachung greift in das Fernmeldegeheimnis ein, weil dadurch sowohl die Inhaltsdaten als auch die Verkehrsdaten des E-Mail-Verkehrs erhoben werden. Unzutreffend ist die Meinung, dass die E-Mail-Kommunikation aufgrund der einsehbaren Übertragung der Datenpakete keinen Schutzgegenstand des Fernmeldegeheimnisses darstelle. Denn digitale Datenpakete können nicht ohne Zuhilfenahme technischer Mittel unmittelbar dechiffriert werden. Dementsprechend hinkt der bisweilen gezogene Vergleich von E-Mails mit offenen Postkarten. Ebenfalls abzulehnen ist die Auffassung, dass die im Mailserver der Provider ruhende und noch nicht vom Empfänger abgerufene E-Mail nicht durch das Fernmeldegeheimnis geschützt wird. Denn in dieser Phase der E-Mail-Übermittlung befindet sich die E-Mail nicht im Herrschaftsbereich der Telekommunikationsteilnehmer. Nach dem Beherrschbarkeitskriterium ist der Vorgang der E-Mail-Kommunikation in dieser Phase nicht unterbrochen.

2. Das Recht auf informationelle Selbstbestimmung, das sich aus Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 Satz 1 GG ergibt, gewährleistet die Befugnis des Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen. Dabei geht es um Datenschutz (Schutz der personenbezogenen Daten). Zum Schutzbereich des Rechts auf informationelle Selbstbestimmung gehört auch der Schutz der Verkehrsdaten der Telekommunikation. Da die E-Mail-Adresse und IP-Adresse den Begriff der personenbezogenen Daten erfüllen, werden sie durch das Recht auf informationelle Selbstbestimmung geschützt. Berücksichtigt man, dass der Staat durch die präventiv-polizeiliche E-Mail-Überwachung die E-Mail-Adressen (ggf. IP-Adressen) der Telekommunikationsteilnehmer erheben kann, greift diese verdeckte polizeiliche Maßnahme zur Informationsgewinnung in das Recht auf informationelle Selbstbestimmung ein.

3. Ein Schutz vor der präventiv-polizeilichen E-Mail-Überwachung durch das vom Bundesverfassungsgericht entwickelte Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme (Computergrundrecht) ist nicht notwendig. Denn die grundrechtliche Selbstständigkeit dieses neu entwickelten Computergrundrechts, das der Erfüllung von Schutzlücken des Fernmeldegeheimnisses und des Rechts auf informationelle Selbstbestimmung dienen soll, ist zu verneinen.

4. Die Inhalte der überwachten E-Mail-Kommunikation können Geschäfts- und Betriebsgeheimnisse enthalten. Die Geschäfts- und Betriebsgeheimnisse werden durch Art. 14 Abs. 1 GG geschützt, weil sie einen durch den Einsatz von Kapital und Arbeit erwirtschafteten Vermögenswert darstellen. Obwohl der Staat durch die präventiv-polizeiliche E-Mail-Überwachung betriebsbezogene Daten erheben kann, bewirkt diese polizeiliche Informationserhebung, von der die staatliche Offenbarung der betriebsbezogenen Daten zu unterscheiden ist, keine Beeinträchtigung der vermögens-

werten Rechtsposition. Deswegen greift der präventiv-polizeiliche Zugriff auf die E-Mail-Kommunikation nicht in das von Art. 14 Abs. 1 GG geschützte Eigentum ein.

5. Die präventiv-polizeiliche E-Mail-Überwachung führt auch nicht zum Eingriff in den Schutzbereich des Art. 5 Abs. 1 S. 1 GG. Ein Eingriff in die Meinungsfreiheit des Art. 5 Abs. 1 Satz 1 Hs. 1 GG liegt vor, wenn die Meinungsäußerung per E-Mail durch staatliche Anordnung verboten wird. Die präventiv-polizeiliche E-Mail-Überwachung verhindert nicht die zu überwachende E-Mail-Kommunikation. Außerdem ist zweifelhaft, ob der Empfang einer E-Mail eine Kommunikationsaufnahme „aus allgemein zugänglichen Quellen" darstellt, obwohl sich das Internet als eine Informationsquelle im Sinne des Art. 5 Abs. 1 Satz 1 Hs. 2 GG betrachten lässt. Ferner wird die Kommunikationsaufnahme nicht durch die präventiv-polizeiliche E-Mail-Überwachung gehindert. Insoweit greift diese verdeckte polizeiliche Maßnahme zur Informationserhebung nicht in die Informationsfreiheit des Art. 5 Abs. 1 Satz 1 Hs. 2 GG ein.

6. Die präventiv-polizeiliche E-Mail-Überwachung führt sowohl zum Eingriff in das Fernmeldegeheimnis als auch zum Eingriff in das Recht auf informationelle Selbstbestimmung. Diese Grundrechtskonkurrenz ist keine Idealkonkurrenz, sondern eine Gesetzeskonkurrenz, weil das Fernmeldegeheimnis lex specialis gegenüber dem Recht auf informationelle Selbstbestimmung ist. Nach Abschluss des Vorgangs der E-Mail-Kommunikation endet der Schutz des Fernmeldegeheimnisses. Insoweit greift die polizeiliche Maßnahme zur Erhebung der Daten einer abgeschlossenen E-Mail-Kommunikation nicht in das Fernmeldegeheimnis, sondern in das Recht auf informationelle Selbstbestimmung ein, soweit die erhobenen Daten personenbezogene Daten darstellen. Der nach Abschluss des Telekommunikationsvorgangs durchgeführte heimliche Zugriff auf Computer-Festplatten der Telekommunikationsteilnehmer ist jedoch keine E-Mail-Überwachung (Überwachung einer laufenden E-Mail-Kommunikation), sondern eine Online-Durchsuchung.

7. Da die polizei- und ordnungsgesetzlichen Vorschriften zur Telekommunikationsüberwachung eine Mitwirkungspflicht der Diensteanbieter regeln, führt die Durchführung einer präventiv-polizeilichen E-Mail-Überwachung auch zum Eingriff in das Grundrecht der E-Mail-Provider. Betroffen ist die Berufs(ausübungs)freiheit der E-Mail-Provider. Nicht beeinträchtigt ist das Eigentum der Diensteanbieter, weil sich die Mithilfe der E-Mail-Provider nicht auf das Erworbene, sondern auf den Erwerb bezieht. Darüber hinaus stellt die technische Mithilfe der E-Mail-Provider keine unentgeltliche Indienstnahme Privater dar.

Zum 5. Kapitel

1. In Bezug auf die formelle Verfassungsmäßigkeit der präventiv-polizeilichen E-Mail-Überwachung ist zu prüfen, ob diese polizeiliche Maßnahme zur Informationserhebung eine gesetzliche Rechtsgrundlage, die der Kompetenzverteilung zwischen Bund und Ländern im Grundgesetz entspricht, hat. Zunächst kommen die geltenden Ermächtigungsvorschriften zur Telekommunikationsüberwachung, die als ausdrückliche Rechtsgrundlagen des präventiv-polizeilichen Zugriffs auf die E-Mail-Kommunikation angesehen werden, in Betracht. Diese polizei- und ordnungsgesetzlichen Ermächtigungsvorschriften dienen der Gefahrenabwehr. Sie sind kompetenzgemäß, weil der Landesgesetzgeber im Ergebnis aus Art. 70 Abs. 1 GG die Gesetzgebungsbefugnis für die Gefahrenabwehr hat.

2. Die Bundesgesetzgebungskompetenz nach Art. 73 Abs. 1 Nr. 7 GG bezieht sich nur auf die technische Seite der Telekommunikationsinfrastruktur und der Informationsübermittlung. Zwar geht es bei der Telekommunikationsüberwachung auch um die Erhebung der Telekommunikationsverkehrsdaten, jedoch kann sich keine Gesetzgebungskompetenz des Bundes für die Telekommunikationsüberwachung (im Rahmen der Erhebung der Verkehrsdaten) aus Art. 73 Abs. 1 Nr. 7 GG ergeben. Denn die Telekommunikation als solche stellt nicht den Zweck einer Telekommunikationsüberwachung dar.

3. Die ungeschriebene Bundeskompetenz kraft Sachzusammenhangs kann anerkannt werden, wenn sie eine unerlässliche Voraussetzung für die Ausübung einer im Grundgesetz ausdrücklich normierten Bundeskompetenz darstellt. In Bezug auf das Verhältnis zwischen präventiv-polizeilicher Telekommunikationsüberwachung und dem Gegenstand der in Art. 73 Abs. 1 Nr. 7 GG vorgeschriebenen Gesetzgebungskompetenz (Fernmeldetechnik) ist die Telekommunikationsüberwachung keine Voraussetzung der Telekommunikationstechnik. Vielmehr setzt die Durchführung einer präventiv-polizeilichen Telekommunikation umgekehrt die Funktionsfähigkeit der Fernmeldetechnik voraus. Deswegen kann keine an Art. 73 Abs. 1 Nr. 7 GG anknüpfende ungeschriebene Bundeskompetenz kraft Sachzusammenhangs für die präventiv-polizeiliche Telekommunikationsüberwachung anerkannt werden.

4. Eine ungeschriebene Bundeskompetenz kraft Annexes, die als ein Unterfall der Kompetenz kraft Sachzusammenhangs anzusehen ist, liegt vor, wenn sie für die Vorbereitung und Durchführung einer geschriebenen Bundeskompetenz erforderlich ist und damit in einem unlösbaren Zusammenhang zur geschriebenen Bundeskompetenz steht. Zwar kann der Bund durch seine Annexkompetenz spezielles Ordnungs- und Polizeirecht im entsprechenden Sachgebiet regeln, jedoch erschöpft sich die an Art. 73 Abs. 1 Nr. 7 GG knüpfende Annexkompetenz des Bundes für das Polizei-

recht in der Abwehr der von der technischen Seite der Telekommunikation herrührenden Gefahren (z. B. Elektrosmog). Im Vergleich dazu betrifft die präventiv-polizeiliche Telekommunikationsüberwachung die durch die Inhalte der Telekommunikation verursachte Gefahr. Folglich hat der Bund keine an Art. 73 Abs. 1 Nr. 7 GG knüpfende Annexkompetenz für die präventiv-polizeiliche Telekommunikationsüberwachung.

5. Der Bund besitzt nach Art. 73 Abs. 1 Nr. 9a GG (Abwehr des internationalen Terrorismus) ausnahmsweise eine ausdrücklich normierte Gesetzgebungskompetenz für die Gefahrenabwehr. Jedoch ist diese Bundesgesetzgebungskompetenz nur subsidiär gegenüber der Landesgesetzgebungszuständigkeit für die Gefahrenabwehr. Demzufolge wird die Landeskompetenz für die Gefahrenabwehr nicht durch diese neue Bundeskompetenz verdrängt. Obwohl der Bundesgesetzgeber dem BKA eine Befugnis für die präventive Telekommunikationsüberwachung einräumen kann, darf diese Befugnis des BKA nicht die Grenze zur allgemeinen Gefahrenabwehr überschreiten. Insoweit verdrängt § 20 l BKAG, der die Befugnis des BKA für die präventive Telekommunikationsüberwachung regelt, die polizei- und ordnungsgesetzlichen Vorschriften der Länder zur Telekommunikationsüberwachung, die auf die allgemeine Gefahrenabwehr abzielen, nicht.

6. Laut der Literatur und Rechtsprechung muss die Anerkennung der Bundeskompetenzen kraft Natur der Sache, die keine Anknüpfung an eine geschriebene Bundeskompetenz hat, begriffsnotwendig sein. Die Begriffsnotwendigkeit soll durch eine die gesamte Verfassung umfassende systematische Auslegung oder durch eine Analogie festgestellt werden. Allerdings ist diese Meinung nicht überzeugend. Denn Art. 70 Abs. 1 GG steht der Möglichkeit der Rechtslücke im Bereich der Gesetzkompetenzverteilung entgegen. Zudem kann man gemäß Art. 70 Abs. 2 GG nicht durch eine Auslegung der „gesamten“ Verfassung eine Bundeskompetenz schaffen. Da es nach hier vertretener Ansicht keine verfassungsrechtliche Grundlage der Bundeskompetenz kraft Natur der Sache gibt, ist eine Bundeskompetenz kraft Natur der Sache für die präventiv-polizeiliche Telekommunikationsüberwachung zu verneinen.

7. Da der Bund keine Kompetenz hat, die die Landesgesetzgebungskompetenz für die präventiv-polizeiliche Telekommunikationsüberwachung zur Gefahrenabwehr verdrängen kann, sind die polizei- und ordnungsgesetzlichen Ermächtigungsvorschriften zur Telekommunikationsüberwachung formell verfassungsmäßig.

8. Unter dem Aspekt des Gesetzesvorbehalts ist der präventiv-polizeiliche Zugriff auf die E-Mail-Kommunikation formell verfassungsmäßig, soweit eine Ermächtigungsvorschrift vorliegt. In den Bundesländern, in denen eine ausdrückliche polizei- und ordnungsgesetzliche Ermächtigungsvorschrift zur Telekommunikationsüberwachung fehlt, kann weder

eine andere Vorschrift der polizeilichen Standardmaßnahmen noch die polizeirechtliche Generalklausel als Rechtsgrundlage der präventiv-polizeilichen E-Mail-Überwachung angesehen werden. Dies lässt sich u. a. damit begründen, dass der Gesetzgeber dieser Bundesländer im Anwendungsbereich des Polizei- und Ordnungsgesetzes das Fernmeldegeheimnis des Art. 10 Abs. 1 GG nicht als ein einschränkbares Grundrecht betrachtet. Aufgrund des Zitiergebots (Art. 19 Abs. 1 Satz 2 GG) kann die präventiv-polizeiliche E-Mail-Überwachung in diesen Bundesländern keine Rechtsgrundlage finden.

9. Hinsichtlich der materiellen Verfassungsmäßigkeit der geltenden polizei- und ordnungsgesetzlichen Ermächtigungsvorschriften zur Telekommunikationsüberwachung ist zunächst zu prüfen, ob diese dem rechtsstaatlichen Bestimmtheitsgebot entsprechen. Da der Betroffene wegen der Heimlichkeit der Überwachungsmaßnahmen nicht unverzüglich den derzeitigen Eingriff in seine Grundrechte erfährt, muss die gesetzliche Ermächtigung jedenfalls so hinreichend bestimmt sein, dass er erkennen kann, bei welchen Anlässen und unter welchen Voraussetzungen ein Risiko der Überwachung besteht. Berücksichtigt man, dass die präventiv-polizeiliche Telekommunikationsüberwachung in einigen Bundesländern der Prävention im Vorfeld der Gefahr dient, ist die große Bedeutung der Bestimmtheit der Gesetze für diese verdeckte polizeiliche Maßnahme zur Informationserhebung nicht zu übersehen. Wenn eine präventiv-polizeiliche Telekommunikationsüberwachung im Vorfeld der Gefahr durchgeführt wird, erhöht sich das Risiko einer Fehlprognose. Durch die Bestimmtheit der Ermächtigungsvorschriften kann das Risiko einer Fehlprognose reduziert werden.

10. Durch sein Urteil vom 27. 7. 2005 erklärte das Bundesverfassungsgericht § 33a Abs. 1 Nr. 2 und 3 ndsSOG a. F. für nichtig. Dies ist eine Leitentscheidung für die Verfassungsmäßigkeit der gesetzlichen Ermächtigungsgrundlagen zur präventiv-polizeilichen Überwachung der Telekommunikation in anderen Bundesländern, weil das Bundesverfassungsgericht detailliert das Bestimmtheitsdefizit der angegriffenen niedersächsischen Regelungen aufgezeigt hat. Nach diesem Urteil ist § 33a Abs. 1 Nr. 2 ndsSOG a. F. mit dem Bestimmtheitsgebot nicht vereinbar. Denn in dieser Ermächtigungsvorschrift fehle ein hinreichend bestimmter Indikator des hypothetischen Kausalverlaufs. Zudem sei der Begriff der „Straftat von erheblicher Bedeutung“, der auch § 2 Nr. 10 ndsSOG a. F. betreffe, nicht hinreichend bestimmt, weil unklar sei, wie sich die Erheblichkeit der ungenannten Straftaten durch die sehr unscharfe Vergleichbarkeit ergebe. Man könne auch nicht genau wissen, wann ein Verhalten auf die künftige Begehung einer „Straftat von erheblicher Bedeutung“ hindeute. Da der Begriff der in § 33a Abs. 1 Nr. 3 ndsSOG a. F. verwendeten „Kontakt- und Begleitperson“ einen engen Zusammenhang mit den obigen nicht hinreichend

bestimmten Begriffen habe, lasse sich auch sehr schwer festzulegen, wer dem Begriff der „Kontakt- und Begleitperson“ entspreche.

11. Die meisten polizei- und ordnungsgesetzlichen Ermächtigungsvorschriften zur Telekommunikationsüberwachung entsprechen dem Bestimmtheitsgebot. In den Ermächtigungsvorschriften, die der Straftatenverhütung dienen, werden bestimmte Indikatoren des hypothetischen Kausalverlaufs vorgeschrieben. Dagegen sind die brandenburgischen Ermächtigungsvorschriften zur im Vorfeld von Gefahr durchgeführten präventiv-polizeilichen Telekommunikationsüberwachung nicht hinreichend bestimmt.

12. Da die präventiv-polizeiliche Telekommunikationsüberwachung zu einem schweren Grundrechtseingriff führt, muss das Gewicht der durch diese polizeiliche Maßnahme geschützten Rechtsgüter – nach der je-desto-Formel – hinreichend groß sein, um der Verhältnismäßigkeit im engeren Sinne zu entsprechen. Die Anforderung an das erhebliche Gewicht der zu schützenden Rechtsgüter ist besonders zu betonen, wenn die präventiv-polizeiliche Telekommunikationsüberwachung im Vorfeld einer Gefahr durchgeführt wird, weil der polizeiliche Zugriff auf die Telekommunikation hier bereits bei geringerem Wahrscheinlichkeitsgrad des Schadenseintritts erfolgen kann. Die Rechtsgutsabwägung, die bei der Angemessenheitsprüfung erfolgt, basiert auf den hinreichend bestimmten Tatbeständen der polizei- und ordnungsgesetzlichen Ermächtigungsvorschriften zur Telekommunikationsüberwachung. Falls ein Bestimmtheitsdefizit in den polizei- und ordnungsgesetzlichen Ermächtigungsvorschriften zur Telekommunikationsüberwachung vorliegt, ist die Prüfung der Angemessenheit mangels der gesetzlichen Anhaltspunkte für die Abwägung der Rechtsgüter nicht möglich. In diesem Zusammenhang stellen die brandenburgischen Ermächtigungsvorschriften zur im Vorfeld der Gefahr durchgeführten präventiv-polizeilichen Telekommunikationsüberwachung wegen des Bestimmtheitsdefizits keine einer Abwägung zugänglichen Normen dar. Im Gegensatz dazu sind die meisten Ermächtigungsvorschriften zur präventiv-polizeilichen Telekommunikationsüberwachung, die hinreichend bestimmt sind, verhältnismäßig, weil sie dem Schutz besonders hochrangiger Rechtsgüter dienen.

13. Durch sein Urteil vom 27. 7. 2005 verlangte das Bundesverfassungsgericht, dass die Ermächtigungsvorschriften zur präventiv-polizeilichen Telekommunikationsüberwachung hinreichende Vorkehrungen zum Schutz des Kernbereichs privater Lebensgestaltung regeln müssen. Das Bundesverfassungsgericht erklärte einerseits, dass der Kernbereich privater Lebensgestaltung absolut geschützt sei. Andererseits legte es dar, dass die Berührung des Kernbereichs zum Schutz des besonders hochrangigen gefährdeten Rechtsguts ein hinzunehmendes Risiko sei. Im Urteil des Bundesverfassungsgerichts gibt es erhebliche Widersprüche. Dem Risiko, dass

der Kernbereich privater Lebensgestaltung durch die Durchführung präventiv-polizeilicher Telekommunikationsüberwachung berührt wird, kann nach der Auffassung des Bundesverfassungsgerichts durch die Vorkehrungen zum Schutz des Kernbereichs (z. B. Abbruch der Überwachung und Verbot der Verwertung sowie Löschung der erhobenen Daten) nachträglich abgeholfen werden. Ob diese Vorkehrungen zum Schutz des Kernbereichs privater Lebensgestaltung effektiv sind, ist jedoch zweifelhaft. Denn sie werden erst dann getroffen, wenn ein Eingriff in den Kernbereich bereits vorliegt. Ihre Funktion ist nicht die Verhinderung des Eingriffs in den Kernbereich, sondern nur die Verminderung der bereits realisierten Kernbereichsverletzung.

14. Hinsichtlich des Eingriffs in das Fernmeldegeheimnis (Art. 10 Abs. 1 GG) erfüllen die geltenden polizei- und ordnungsgesetzlichen Ermächtigungsvorschriften zur Telekommunikationsüberwachung das Zitiergebot (Art. 19 Abs. 1 Satz 2 GG). Dagegen gibt es in den Polizei- und Ordnungsgesetzen, die die Mitwirkungspflicht der Diensteanbieter regeln, keine Zitierklausel, die Art. 12 Abs. 1 GG nennt. Dies führt jedoch nicht zur Verfassungswidrigkeit der polizei- und ordnungsgesetzlichen Regelungen über die Mitwirkungspflicht der Diensteanbieter, weil Art. 19 Abs. 1 Satz 2 GG nach der Rechtsprechung des Bundesverfassungsgerichts nicht für Art. 12 Abs. 1 GG gilt. Rechtsdogmatisch ist diese Ausnahme von der Anwendung des Zitiergebots allerdings nach hier vertretener Ansicht abzulehnen.

Zum 6. Kapitel

1. Das Rechtsverhältnis zwischen der überwachenden Polizeibehörde und der Zielperson, deren E-Mail-Kommunikation zu überwachen ist, wird nicht durch die polizei- und ordnungsgesetzlichen Ermächtigungsvorschriften zur Telekommunikationsüberwachung, sondern durch die exekutive Maßnahme der präventiv-polizeilichen E-Mail-Überwachung begründet. Da sich die Maßnahme der präventiv-polizeilichen E-Mail-Überwachung nicht auf die Anordnung von Geboten oder Verboten bezieht, mangelt es am Merkmal „Regelung“ im Sinne des § 35 Satz 1 VwVfG. Deswegen ist die Maßnahme des präventiv-polizeilichen Zugriffs auf den E-Mail-Verkehr, die die Entstehungsbedingung des Rechtsverhältnisses zwischen der überwachenden Polizeibehörde und den Zielpersonen darstellt, als Realakt zu qualifizieren. Die Auffassung, dass der polizeiliche Überwachungseingriff aus einem konkludenten Verwaltungsakt und einem Realakt, der die Ausführung dieses konkludenten Verwaltungsakts darstelle, bestehe, ist unzutreffend. Denn der Inhalt eines solchen „konkludenten Verwaltungsakts“ ist unklar. Berücksichtigt man, dass es bei der Durchführung einer präventiv-polizeilichen E-Mail-Überwachung wegen der Heimlichkeit des Zugriffs an einer Bekanntgabe fehlt, lässt sich festhalten, dass

die Meinung, dass die Maßnahme der polizeilichen verdeckten Informationserhebung als Verwaltungsakt einzustufen sei, abzulehnen ist. Denn ein Verwaltungshandeln, das die Voraussetzungen des § 35 VwVfG erfüllt, ist (noch) kein Verwaltungsakt, wenn es noch nicht bekannt gegeben wird. In einem Rechtsstaat darf niemand durch einen noch nicht bekannt gegebenen Verwaltungsakt verpflichtet werden.

2. Ob sich die Zielpersonen im Dienstbezirk der überwachenden Polizeibehörde befinden, spielt keine Rolle für die Durchführung der präventivpolizeilichen E-Mail-Überwachung. Vielmehr ist die Frage maßgeblich, ob die abzuwehrende Gefahr, die die Zielpersonen verursachen, im Dienstbezirk der überwachenden Polizeibehörde auftritt. Da nicht die Zielperson als solche, sondern die E-Mail-Kommunikation der Zielperson das Objekt der Überwachung darstellt, ist die Frage, ob der Provider, der der Zielperson die E-Mail-Dienste anbietet, einen Firmensitz im örtlichen Zuständigkeitsgebiet der überwachenden Polizeibehörde hat, von größerer Bedeutung – gegenüber der Frage nach dem Sitz der Zielperson – für die Durchführung einer präventiv-polizeilichen E-Mail-Überwachung.

3. Im Bereich der klassischen Gefahrenabwehr ist die Zielperson, deren E-Mail-Kommunikation zu überwachen ist, in der Regel Störer im Sinne des Polizeirechts. Ein Nichtstörer kann nur Adressat der präventiv-polizeilichen E-Mail-Überwachung sein, wenn die Voraussetzungen des polizeilichen Notstands erfüllt werden. Nach Art. 34a Abs. 3 Satz 1 Nr. 1 bayPAG und § 34a Abs. 1 Satz 1 Nr. 2 mvSOG kann sich die präventiv-polizeiliche E-Mail-Überwachung gegen die Personen, deren Leben oder Gesundheit gefährdet ist, richten. Diese beiden polizei- und ordnungsgesetzlichen Vorschriften können zur Verhinderung eines Selbstmordes angewendet werden. Da der Suizidwillige durch seinen Selbsttötungsversuch eine Gefahr (Gefährdung des Rechts auf Leben) verursacht, erfüllt er den Begriff des Störers im Sinne des Polizeirechts. Falls er sich in einer die freie Willensentschließung ausschließenden psychischen Ausnahmesituation befindet, ist er nicht verantwortlich für die Gefahr, die er verursacht. In dieser Konstellation ist eine präventiv-polizeiliche E-Mail-Überwachung nach Art. 34a Abs. 3 Satz 1 Nr. 1 bayPAG oder § 34a Abs. 1 Satz 1 Nr. 2 mvSOG, die sich gegen einen Suizidwilligen richtet, als eine polizeiliche Maßnahme, die im polizeilichen Notstand ergriffen wird, zu betrachten.

Nach Art. 34 a Abs. 1 Satz 1 Nr. 3 bayPAG und § 34 a Abs. 3 Satz 1 Nr. 3 thürPAG kann sich die präventiv-polizeiliche E-Mail-Überwachung gegen Kontakt- und Begleitpersonen im Bereich der klassischen Gefahrenabwehr richten. Da die abzuwehrende Gefahr nicht von den Kontakt- und Begleitpersonen verursacht wird, sind sie Nichtstörer. Die Polizei kann gemäß Art. 34a Abs. 1 Satz 1 Nr. 3 bayPAG und § 34a Abs. 3 Satz 1 Nr. 3 thürPAG im Bereich der klassischen Gefahrenabwehr den E-Mail-Verkehr der Kon-

takt- und Begleitpersonen nur überwachen, wenn die Voraussetzungen des polizeilichen Notstands erfüllt werden.

4. Da im Vorfeld der Gefahr noch keine Gefahr besteht, fehlt im Vorfeld der Gefahr ein Verursacher der Gefahr. Deswegen sind die Zielpersonen der präventiv-polizeilichen E-Mail-Überwachung, die im Vorfeld der Gefahr durchgeführt wird, als Nichtstörer zu betrachten. Die polizei- und ordnungsgesetzlichen Ermächtigungsvorschriften zur Telekommunikationsüberwachung im Vorfeld der Gefahr stellen spezielle Voraussetzungen eines qualifizierten polizeilichen Notstands dar. Allerdings sind diese Vorschriften mangels hinreichender Bestimmtheit verfassungsrechtlich bedenklich.

5. Ein Nutzer der E-Mail-Dienste, der keine Zielperson der präventiv-polizeilichen E-Mail-Überwachung ist, kann ebenfalls durch die Überwachungsmaßnahme betroffen werden. Im Fall des präventiv-polizeilichen Zugriffs auf die E-Mail-Kommunikation ist die Zahl der betroffenen Nichtzielpersonen besonders groß. Zunächst wird zugleich in das Fernmeldegeheimnis der Kommunikationspartner, denen die Zielperson die von der Polizeibehörde überwachte E-Mail schickt, eingegriffen. Zudem werden E-Mails unbeteiligter Dritter, die über den kontrollierten E-Mail-Knoten übermittelt werden, durch das von der überwachenden Polizeibehörde eingesetzte Überwachungsprogramm überprüft. Obwohl die Überprüfung der E-Mail durch einen E-Mail-Filter ein „virtuelles Lesen“ ist, führt sie bereits zum Zugriff auf den Vorgang der E-Mail-Kommunikation unbeteiligter Dritter. Der Eingriff in das Fernmeldegeheimnis unbeteiligter mitbetroffener Dritter ist gering, weil unbeteiligte mitbetroffene Dritte in den meisten Fällen nicht identifiziert werden.

6. Wenn die E-Mails der Nichtzielpersonen durch den von der überwachenden Polizeibehörde (mit Hilfe des Diensteanbieters) in kontrollierten E-Mail-Knoten eingesetzten E-Mail-Filter virtuell überprüft werden, liegt ein Rechtsverhältnis zwischen diesen Nichtzielpersonen und der überwachenden Polizeibehörde vor. Dieses Rechtsverhältnis entsteht durch einen Realakt. Da unbeteiligte Dritte keine Gefahr verursachen, sind sie Nichtstörer. Allerdings ist die Konstellation, dass die E-Mails unbeteiligter Dritter im kontrollierten E-Mail-Knoten virtuell überprüft werden, keine Inanspruchnahme nichtverantwortlicher Dritter. Denn diese Konstellation ist nur die Folge der technischen Unvermeidbarkeit bei der Durchführung der präventiv-polizeilichen E-Mail-Überwachung, die sich gegen die Zielperson richtet.

7. Das Rechtsverhältnis zwischen der überwachenden Polizeibehörde und den betroffenen Nutzern der E-Mail-Dienste ist asymmetrisch. Bei der Durchführung einer präventiv-polizeilichen E-Mail-Überwachung hat die überwachende Polizeibehörde eine übermächtige Informationsbefugnis. Da das Rechtsverhältnis zwischen der überwachenden Polizeibehörde und

den betroffenen Nutzern der E-Mail-Dienste durch Realakt entsteht, kann der Rechtsschutz nicht durch Ausübung der in VwVfG oder Landesverwaltungsverfahrensgesetzen vorgeschriebenen Verfahrensrechte gewährleistet werden. Auch wenn eine analoge Anwendung der Verfahrensrechte anerkannt werden kann, ist eine Verfahrensbeteiligung praktisch unmöglich, weil die Bewahrung der Heimlichkeit für den Zugriff auf die E-Mail-Kommunikation notwendig ist. Aufgrund der Heimlichkeit der Überwachungsmaßnahme ist der gerichtliche Rechtsschutz im Laufe der Durchführung einer Überwachungsmaßnahme kaum möglich. Unter dem Gesichtspunkt effektiven Rechtsschutzes ist die Eröffnung des Verwaltungsrechtswegs erst nach der Beendigung der Überwachungsmaßnahme wenig befriedigend.

8. Die Anordnung der Überwachung unter Richtervorbehalt, die in den geltenden polizei- und ordnungsgesetzlichen Ermächtigungsvorschriften zur Telekommunikationsüberwachung geregelt wird, kann vorbeugend eine willkürliche polizeiliche Entscheidung über den Zugriff auf die E-Mail-Kommunikation verhindern. Ob der Richtervorbehalt ein wirklich effektives Mittel zur Verbesserung der Asymmetrie des Rechtsverhältnisses zwischen der überwachenden Polizeibehörde und betroffenen Nutzern der E-Mail-Dienste darstellen kann, ist jedoch zweifelhaft. Zunächst kann die vorbeugende gerichtliche Kontrolle aufgrund des Gewaltenteilungsgrundsatzes nicht die polizeiliche Gefahrenprognose ersetzen. Davon abgesehen wird eine einseitige polizeiliche Entscheidung über die Durchführung einer Überwachungsmaßnahme faktisch zugelassen, falls der Richter die Dichte der vorbeugenden Kontrolle in erheblichem Umfang reduziert. Zudem kann das rechtliche Gehör der Zielpersonen bei der vorbeugenden Gerichtskontrolle aufgrund der Heimlichkeit der Überwachungsmaßnahme nicht gewährt werden. Dies hat zur Folge, dass die richterliche Entscheidung nur auf den Informationen, die die Polizeibehörde vorlegt, basieren kann. In der Praxis wird der Antrag eines Zugriffs auf die Telekommunikation selten vom Richter abgelehnt. Demzufolge lässt sich die Effizienz der gerichtlichen vorbeugenden Kontrolle nicht abschließend beurteilen.

9. Nach Beendigung des auf Gefahrenabwehr zielenden Rechtsverhältnisses zwischen der überwachenden Polizeibehörde und den betroffenen Nutzern der E-Mail-Dienste entsteht die Unterrichtungspflicht der Polizei. Zu unterrichten sind nicht nur Zielpersonen, sondern auch ihre Kommunikationspartner, weil die E-Mail-Adressen der Kommunikationspartner, die dem Begriff der personenbezogenen Daten entsprechen, auch durch die früher durchgeführte Maßnahme präventiv-polizeilicher E-Mail-Überwachung erhoben wurden. Die nachträgliche Benachrichtigung gilt auch für unbeteiligte Dritte, deren E-Mails über den kontrollierten E-Mail-Knoten übermittelt und von der Polizei wegen eines technischen Fehlers des Überwachungsprogramms mitgelesen wurden. Nicht zu unterrichten sind die

betroffenen Nutzer der E-Mail-Dienste, deren E-Mails nur vom im kontrollierten E-Mail-Knoten eingesetzten E-Mail-Filter virtuell überprüft und nicht auf den Server der überwachenden Polizeibehörde übertragen wurden. Grund ist, dass die für die Benachrichtigung notwendige Identifizierung eines unbeteiligten mitbetroffenen Dritten den Grundrechtseingriff verstärken würde. Die nachträgliche Benachrichtigungspflicht braucht nach § 23 a Abs. 8 S. 1 in Verbindung mit § 23 Abs. 6 Satz 5 Nr. 2 bwPolG, § 29 Abs. 6 Satz 3 hessSOG und § 34 Abs. 10 Satz 1 Nr. 2 thürPAG zur Vermeidung von Verwaltungsaufwand oder zum Schutz von Vermögensgütern nicht erfüllt zu werden. Dadurch ist die Möglichkeit des gerichtlichen Rechtsschutzes gegen den schweren Eingriff in das Fernmeldegeheimnis gesperrt. Ob eine solche Einschränkung der polizeilichen Unterrichtungspflicht angemessen ist, ist sehr fragwürdig.

10. Das Rechtsverhältnis zwischen dem Rechtsträger der überwachenden Polizeibehörde und den E-Mail-Providern wird durch die polizeiliche Anordnung der technischen Hilfe begründet. Da die überwachende Polizeibehörde durch diese Anordnung im Einzelfall die konkreten Inhalte der Mitwirkungspflicht der E-Mail-Provider bestimmt, ist sie als Verwaltungsakt zu qualifizieren. Die Möglichkeit, dass dieses Rechtsverhältnis durch einen Verwaltungsvertrag begründet wird, ist zu verneinen. Denn die (allgemeine) Mitwirkungsverpflichtung wird bereits durch polizei- und ordnungsgesetzliche Vorschriften zwangsweise auferlegt. Ein Verwaltungsvertrag, dessen Abschluss die Vertragsfreiheit des Bürgers verletzt, ist nicht anzuerkennen. Zudem bezieht sich der Inhalt des Verwaltungsvertrags zwischen der überwachenden Polizeibehörde und den E-Mail-Providern auf die Ermöglichung eines präventiv-polizeilichen Zugriffs auf die E-Mail-Kommunikation, der in das Grundrecht Dritter (d. h. in das Fernmeldegeheimnis betroffener Nutzer der E-Mail-Dienste) eingreift. Gemäß § 58 Abs. 1 VwVfG wird ein in Rechte Dritter eingreifender Verwaltungsvertrag erst wirksam, wenn der Dritte schriftlich zustimmt. Wegen der Heimlichkeit der Überwachungsmaßnahme ist die Zustimmung betroffener Dritter vor dem Abschluss der präventiv-polizeilichen E-Mail-Überwachung faktisch unmöglich.

11. Gemäß des Wortlauts der polizei- und ordnungsgesetzlichen Ermächtigungsvorschriften zur präventiven Telekommunikationsüberwachung erstreckt sich die Mitwirkungspflicht der Diensteanbieter auf jeden E-Mail-Provider, der den Zielpersonen E-Mail-Dienste anbietet. Insoweit scheiden die E-Mail-Provider, die nur in einem anderen Bundesland ihren Sitz haben, nicht aus. Die überwachende Polizeibehörde kann durch einen Verwaltungsakt einem solchen E-Mail-Provider eine konkrete Mitwirkungspflicht auferlegen, soweit dieser E-Mail-Provider den Zielpersonen, die im Bezirk der überwachenden Polizeibehörde eine Gefahr bewirken, E-Mail-Dienste anbietet. Ein solcher nationaler grenzüberschreitender Anspruch

der Polizei auf die technische Hilfe der E-Mail-Provider erfolgt nicht aufgrund einer kompetenzwidrigen Geltung eines Landesgesetzes in einem anderen Bundesland, sondern zielt auf eine notwendige Maßnahme zur Abwehr der Gefahren, die im Gebiet der örtlichen Zuständigkeit der überwachenden Polizeibehörde auftreten. Die Auffassung, dass das Nachbarbundesland aufgrund des Grundsatzes der Bundestreue die grenzüberschreitende Gefahrenabwehrmaßnahme der Telekommunikationsüberwachung dulden müsse, überzeugt nicht. Der Grundsatz der Bundestreue dient der Schließung einer positiv-rechtlichen Regelungslücke. Da die Polizei- und Ordnungsgesetze ausdrücklich regeln, dass die Zustimmung des betroffenen Nachbarbundeslandes die Voraussetzung der nationalen grenzüberschreitenden polizeilichen Tätigkeit eines Bundeslandes darstellt, gibt es allerdings keine Regelungslücke. Deswegen hat das betroffene Nachbarbundesland keine Duldungspflicht, die sich aus dem Grundsatz der Bundestreue ergibt. Falls das betroffene Bundesland die Zustimmung der nationalen grenzüberschreitenden polizeilichen Tätigkeit versagt, liegt eine verwaltungsrechtliche Streitigkeit vor, weil es um ein in den Polizei- und Ordnungsgesetzen vorgeschriebenes Verhältnis zwischen Bundesländern geht. Wegen der Heimlichkeit der Überwachungsmaßnahme ist in der Praxis fraglich, ob eine solche Verwaltungsklage, die die Durchführung einer präventiv-polizeilichen E-Mail-Überwachung bekannt werden lässt, zielführend sein kann.

12. Unter dem Gesichtspunkt der örtlichen Zuständigkeit kann die überwachende Polizeibehörde theoretisch einem ausländischen E-Mail-Provider, der in Deutschland keinen Sitz hat, eine Mitwirkungspflicht auferlegen, um den präventiven Zugriff auf die E-Mail-Kommunikation zu ermöglichen. Zu beachten ist, dass die nationale Grenzen überschreitende polizeiliche Tätigkeit einer völkerrechtlichen Vereinbarung oder einer europarechtlichen Grundlage bedarf. Da der ausländische E-Mail-Provider, der in Deutschland keinen Sitz hat, keine telekommunikationsgesetzlichen Pflichten hat, ist eine präventiv-polizeiliche E-Mail-Überwachung durch die Mitwirkung eines ausländischen E-Mail-Providers praktisch schwierig.

13. Bei der technischen Mitwirkung der E-Mail-Provider handelt es sich nicht um eine Übertragung der polizeilichen Befugnis, sondern um eine Vollzugsunterstützung des polizeilichen Zugriffs auf die E-Mail-Kommunikation der Zielpersonen. Zudem bezieht sich die Erfüllung der Mitwirkungspflicht der E-Mail-Provider nicht auf eine untergeordnete Tätigkeit nach fachlicher Weisung der Polizeibehörde, weil die Mithilfe der E-Mail-Provider eine fachmännische technische Unterstützung polizeilicher Überwachungsmaßnahmen ist. Ferner ist die technische Mitwirkung eine Wahrnehmung von Verwaltungsaufgaben gegen den Willen der E-Mail-Provider. Die technische Mithilfe der E-Mail-Provider ist damit eine sog. Indienstnahme Privater.

14. In Baden-Württemberg, Bayern, Brandenburg, Mecklenburg-Vorpommern, Niedersachsen, Saarland, Schleswig-Holstein und Thüringen haben die E-Mail-Provider, die sich an einer Durchführung präventiv-polizeilicher E-Mail-Überwachung beteiligen, gegenüber der Polizeibehörde einen Entschädigungsanspruch bezüglich der Kosten für die konkrete Überwachung eines E-Mail-Verkehrs. Obwohl der Entschädigungsanspruch der Diensteanbieter in Hamburg, Hessen und Rheinland-Pfalz nicht ausdrücklich geregelt wird, besteht er auch hier. Denn die Mitwirkung der Diensteanbieter stellt eine Inanspruchnahme nichtverantwortlicher Dritter dar. Die „Sachnähe" gilt nicht für die E-Mail-Provider, die durch ihre technische Mithilfe den präventiv-polizeilichen Zugriff auf die E-Mail-Kommunikation ermöglichen, weil die Gefahrenabwehr, an der sich die E-Mail-Provider beteiligen, die originäre Aufgabe der Polizei ist.

15. Das Rechtsverhältnis zwischen den E-Mail-Providern und ihren Kunden, die die E-Mail-Dienste nutzen, wird durch privatrechtliche Verträge begründet. Die privatrechtliche Natur des Rechtsverhältnisses wird nicht durch die Beteiligung der E-Mail-Provider an der Durchführung einer präventiv-polizeilichen E-Mail-Überwachung verändert. Die Tätigkeiten, die die E-Mail-Provider im Rahmen ihrer Mitwirkungspflicht ausüben, werden der überwachenden Polizeibehörde zugerechnet. Insoweit gibt es zwischen den E-Mail-Providern und den betroffenen Nutzern der E-Mail-Dienste kein öffentlich-rechtliches Rechtsverhältnis, das aufgrund einer präventiv-polizeilichen Überwachung des E-Mail-Verkehrs begründet wird. Da die E-Mail-Provider nicht zu den Teilnehmern der Telekommunikation zählen, können sie nicht für ihre Kunden das Fernmeldegeheimnis nach Art. 10 Abs. 1 GG geltend machen und damit die technische Mitwirkung ablehnen. Die etwaige Begründetheit einer Klage, die die E-Mail-Provider gegen die polizeiliche Anordnung der Mitwirkung erheben, ergibt sich nicht aus der Verletzung des Fernmeldegeheimnisses, sondern aus der Verletzung der Berufsfreiheit.

Zum 7. Kapitel

1. Die Möglichkeit des Rechtsschutzes gegen gegenwärtige oder drohende präventiv-polizeiliche E-Mail-Überwachung scheidet nicht aus, weil es möglich sein kann, dass die betroffenen Nutzer von E-Mail-Diensten Kenntnis von der noch laufenden oder zukünftigen polizeilichen Informationserhebung erhalten. Da die Rechtsnatur der Maßnahme präventiv-polizeilicher E-Mail-Überwachung ein Realakt ist, stellt die allgemeine Leistungsklage die statthafte Klageart dar. Durch die Erhebung der allgemeinen Leistungsklage können die betroffenen Nutzer begehren, die fortdauernde Beeinträchtigung, die sich aus der noch laufenden präventiv-polizeilichen E-Mail-Überwachung ergibt, zu beseitigen. Zudem können sie durch

eine einfache Unterlassungsklage, die einen Unterfall der allgemeinen Leistungsklage darstellt, die Unterlassung der Wiederholung des Eingriffs begehren. Ferner können sie eine vorbeugende Unterlassungsklage, die sich als ein Unterfall der allgemeinen Leistungsklage ansehen lässt, erheben, wenn die erstmalige Maßnahme präventiv-polizeilicher E-Mail-Überwachung droht. Die betroffenen Nutzer der E-Mail-Dienste sind klagebefugt, wenn die Möglichkeit vorliegt, dass die laufende oder zukünftige präventiv-polizeiliche E-Mail-Überwachung sie rechtswidrig in ihren Rechten verletzt. Falls der Kläger vor Klageerhebung nicht bei der Polizeibehörde, die die Maßnahme präventiver E-Mail-Überwachung ergreift, die Beseitigung der Beeinträchtigung oder die Unterlassung des zukünftigen Zugriffs auf seine E-Mail-Kommunikation beantragt, ist das Rechtsschutzbedürfnis zu verneinen.

2. Gegen die erledigte Maßnahme der präventiv-polizeilichen E-Mail-Überwachung, deren Rechtsnatur der Realakt ist, ist eine (negative) Feststellungsklage nach § 43 Abs. 1 VwGO zu erheben. Durch die Erhebung der auch für ein vergangenes Rechtsverhältnis geltenden Feststellungsklage nach § 43 Abs. 1 VwGO kann der Kläger das Rechtsschutzziel verfolgen, feststellen zu lassen, ob die überwachende Polizeibehörde aufgrund der bestehenden rechtlichen Regelungen zur E-Mail-Überwachung berechtigt war. Die nachträgliche Benachrichtigung stellt die Basis für die faktische Möglichkeit des gerichtlichen Rechtsschutzes dar. Da die betroffenen Nichtzielpersonen, deren E-Mails über den kontrollierten E-Mail-Knoten übermittelt und vom E-Mail-Filter virtuell überprüft werden, nach dem Abschluss der Überwachungsmaßnahme nicht über diesen verdeckten polizeilichen Zugriff auf ihre E-Mail-Kommunikation unterrichtet werden, ist es für sie praktisch unmöglich, nachträglich durch die Erhebung einer Feststellungsklage gerichtlichen Rechtsschutz zu begehren. Im Gegensatz dazu ist die Möglichkeit nicht abzulehnen, dass die (unbeteiligten) Kommunikationspartner der Zielpersonen und die mitbetroffenen Dritten, deren E-Mails aufgrund eines technischen Fehlers des Überwachungsprogramms von der Polizei mitgelesen wurden, eine Feststellungsklage gegen die erledigte präventiv-polizeiliche E-Mail-Überwachung erheben.

3. Die Erhebung der Feststellungsklage gegen eine erledigte Maßnahme präventiv-polizeilicher E-Mail-Überwachung entspricht der Subsidiaritätsklausel des § 43 Abs. 2 Satz 1 VwGO. Da die Maßnahme präventiv-polizeilicher E-Mail-Überwachung nicht als Verwaltungsakt, sondern als Realakt einzustufen ist, ist die Erhebung einer Anfechtungsklage oder einer Verpflichtungsklage nicht statthaft. Zudem kann die Beeinträchtigung, die sich aus dem präventiv-polizeilichen Zugriff auf die E-Mail-Kommunikation ergibt, nicht (mehr) durch eine allgemeine Leistungsklage beseitigt werden, weil der Eingriff bereits beendet ist.

4. Der Begriff des „berechtigten Interesses“ im Sinne des § 43 Abs. 1 VwGO umfasst nicht nur ein rechtliches Interesse, sondern auch jedes schutzwürdige Interesse wirtschaftlicher oder ideeller Art. Da die präventiv-polizeiliche E-Mail-Überwachung darauf basiert, dass die Zielpersonen die polizeilichen Schutzgüter gefährden und sogar potenzielle Straftäter sind, führt diese heimliche polizeiliche Informationserhebung zur Diskriminierung. Das Feststellungsinteresse der Zielperson, deren E-Mail-Kommunikation von der Polizeibehörde beobachtet worden ist, ist zu bejahen, weil die diskriminierende Wirkung der erledigten präventiv-polizeilichen E-Mail-Überwachung durch die gerichtliche Entscheidung über ihre Feststellungsklage beseitigt werden kann. Da die mitbetroffenen Dritten durch die Entscheidung des Gerichts feststellen lassen können, dass die Polizeibehörde nicht mit ihnen ein Rechtsverhältnis, in dem in ihr Fernmeldegeheimnis eingegriffen wird, begründen darf, ist auch das Feststellungsinteresse mitbetroffener Dritter nicht zu verneinen.

5. Da die Anordnung, durch die die Polizeibehörde den E-Mail-Providern die konkrete Mitwirkungspflicht auferlegt, als Verwaltungsakt zu qualifizieren ist, ist die Anfechtungsklage nach § 42 Abs. 1 VwGO die statthafte Klageart gegen eine solche polizeiliche Anordnung der Mitwirkung. Um seine Klagebefugnis zu begründen, muss der E-Mail-Provider vortragen, dass seine Berufsfreiheit möglicherweise durch den Verwaltungsakt verletzt wird. Er kann bei der Erhebung der Anfechtungsklage nicht die Verletzung des Grundrechts der betroffenen Telekommunikationsteilnehmer geltend machen, weil er nicht die Grundrechte seiner Kunden vertritt.

6. Im Widerspruchsverfahren und im Verfahren der Anfechtungsklage, die der betroffene E-Mail-Provider gegen die polizeiliche Anordnung der Mitwirkung erhebt, erfolgt weder eine Anhörung noch eine Beiladung der Zielpersonen. Einerseits sind Zielpersonen nicht „Betroffene“ im Sinne des § 71 VwGO, weil sie keine durch den Verwaltungsakt beschwerte dritte Person sind. Andererseits sind sie auch im Verwaltungsprozess nicht beizuladen. Denn sie sind nicht Beteiligte i. S. d. § 63 Nr. 3 in Verbindung mit § 65 Abs. 1 und 2 VwGO.

Literaturverzeichnis

Achterberg, Norbert, Die Klagebefugnis – eine entbehrliche Sachurteilsvoraussetzung? DVBl. 1981, S. 278 ff.

Albers, Marion, Informationelle Selbstbestimmung, Baden-Baden 2005; zitiert: *Albers*, Informationelle Selbstbestimmung.

– Die Determination polizeilicher Tätigkeit in den Bereichen der Straftatenverhütung und der Verfolgungsvorsorge, Berlin 1999; zitiert: *Albers*, Determination polizeilicher Tätigkeit.

Alberts, Hans W., Staatsfreiheit von Versammlungen, NVwZ 1989, S. 839 ff.

Albrecht, Hans-Jörg/Dorsch, Claudia/Krüpe, Christiane, Rechtswirklichkeit und Effizienz der Überwachung der Telekommunikation nach den §§ 100a, 100b StPO und anderer verdeckter Ermittlungsmaßnahmen, Freiburg im Breisgau 2003; zitiert: *Albrecht/Dorsch/Krüpe*, Rechtswirklichkeit und Effizienz.

Alexy, Robert, Theorie der Grundrechte, 2. Aufl., Frankfurt am Main 1994; zitiert: *Alexy*, Theorie der Grundrechte.

Arndt, Hans-Wolfgang/Fetzer, Thoma/Scherer, Joachim (Hrsg.), Telekommunikationsgesetz-Kommentar, Berlin 2008; zitiert: *Bearbeiter*, in: Arndt/Fetzer/Scherer, TKG.

Aulehner, Josef, Polizeiliche Gefahren- und Informationsvorsorge, Berlin 1998; zitiert: *Aulehner*, Informationsvorsorge.

Axmann, Mario/Degen, Thomas A., Kanzlei-Homepages und elektronische Mandatsbearbeitung – Anwaltsstrategien zur Minimierung rechtlicher Risiken, NJW 2006, S. 1457 ff.

Backes, Otto/Gusy, Christoph, Wer kontrolliert die Telefonüberwachung?: eine empirische Untersuchung zum Richtervorbehalt bei der Telefonüberwachung, Frankfurt am Main (u. a.) 2003; zitiert: *Backes/Gusy*, Telefonüberwachung.

Bader, Johann/Funke-Kaiser, Michael/Kuntze, Stefan/von Albedyll, Jörg, Verwaltungsgerichtsordnung-Kommentar, 4. Aufl., Heidelberg 2007; zitiert: *Bearbeiter*, in: Bader/Funke-Kaiser/Kuntze/von Albedyll, VwGO.

Badura, Peter, Staatsrecht, 3. Aufl., München 2003; zitiert: *Badura*, Staatsrecht.

Badura, Peter/von Danwitz, Thomas/Herdegen, Matthias/Sedemund, Jochim/Stern, Klaus (Hrsg.), Beck'scher PostG-Kommentar, 2. Aufl., München 2004; zitiert: *Bearbeiter*, in: Badura/von Danwitz/Herdegen/Sedemund/Stern, PostG.

Bär, Wolfgang, Anmerkung zu BVerfG U. v. 27. 2. 2008 – 1 BvR 370/07 –, MMR 2008, S. 325 ff.

– Anmerkung zu BVerfG B. v. 11. 3. 2008 – 1 BvR 256/08 –, MMR 2008, S. 307 f.

– Telekommunikationsüberwachung und andere verdeckte Ermittlungsmaßnahmen – Gesetzliche Neuregelungen zum 1. 1. 2008, MMR 2008, S. 215 ff.

– Aktuelle Rechtsfragen bei strafprozessualen Eingriffen in die Telekommunikation, MMR 2000, S. 472 ff.
Bauer, Hartmut, Die Bundestreue, Tübingen 1992; zitiert: *Bauer*, Bundestreue.
Beater, Axel, Medienrecht, Tübingen 2007; zitiert: *Beater*, Medienrecht.
Behling, Thorsten B., Der Zugang elektronischer Willenserklärungen in modernen Kommunikationssystemen, Baden-Baden 2007; zitiert: *Behling*, Zugang elektronischer Willenserklärungen.
Berner, Georg/Köhler, Gerd Michael, Polizeiaufgabengesetz-Kommentar, 19. Aufl., Berlin 2008; zitiert: *Bearbeiter*, in: Berner/Köhler, PAG.
Bethge, Herbert, Grundrechtsverwirklichung und Grundrechtssicherung durch Organisation und Verfahren – Zu einigen Aspekten der aktuellen Grundrechtsdiskussion, NJW 1982, S. 1 ff.
– Probleme des Zitiergebots des Art. 19 Abs. 1 Satz 2 GG, DVBl. 1972, S. 365 ff.
Beulke, Werner, Strafprozessrecht, 10. Aufl., Heidelberg 2008; zitiert: *Beulke*, Strafprozessrecht.
Bleckmann, Albert, Zum materiellrechtlichen Gehalt der Kompetenzbestimmungen des Grundgesetzes, DÖV 1983, S. 129 ff.
Böckenförde, Ernst-Wolfgang, Grundrechte als Grundsatznormen, Der Staat 29 (1990), S. 1 ff.
Breuer, Rüdiger, Rechtsprobleme der Altlasten, NVwZ 1987, S. 751 ff.
Britz, Gabriele, Vertraulichkeit und Integrität informationstechnischer Systeme. Einige Fragen zu einem „neuen Grundrecht", DÖV 2008, S. 411 ff.
Brüning, Christoph, Die Konvergenz der Zulässigkeitsvoraussetzungen der verschiedenen verwaltungsgerichtlichen Klagearten, JuS 2004, S. 882 ff.
Brüning, Christoph/Helios, Marcus, Die verfassungsprozessuale Durchsetzung grundrechtlicher Schutzpflichten am Beispiel des Internets, JURA 2001, S. 155 ff.
Buermeyer, Ulf, Die Online-Durchsuchung. Technischer Hintergrund des verdeckten hoheitlichen Zugriffs auf Computersysteme, HRRS 2007, S. 154 ff., http://www.hrr-strafrecht.de.
Bull, Hans Peter, Neue Bewegung im Datenschutz – Missbrauchsbekämpfung oder Ausbau bereichsspezifischer Regelungen?, ZRP 2008, S. 233 ff.
Bull, Hans Peter/Mehde, Veith, Allgemeines Verwaltungsrecht mit Verwaltungslehre, 8. Aufl., Heidelberg 2009; zitiert: *Bull/Mehde*, AllgVerwR.
Burgi, Martin, Funktionale Privatisierung und Verwaltungshilfe, Tübingen 1999; zitiert: *Burgi*, Funktionale Privatisierung.
Butzer, Hermann, Flucht in die polizeiliche Generalklausel?, VerwArch 93 (2002), S. 506 ff.
Cremer, Wolfram, Rechtfertigung legislativer Eingriffe in Grundrechte des Grundgesetzes und Grundfreiheiten des EG-Vertrags nach Maßgabe objektiver Zwecke, NVwZ 2004, S. 668 ff.
– Freiheitsgrundrechte, Tübingen 2003; zitiert: *Cremer*, Freiheitsgrundrechte.
– Gewinnstreben als öffentliche Unternehmen legitimierender Zweck: Die Antwort des Grundgesetzes, DÖV 2003, S. 921 ff.

Czinczoll, Rupert, Solidaritätspflichten bei der Selbsttötung, Bonn 1984; zitiert: *Czinczoll*, Solidaritätspflichten.
Czychowski, Christian/Nordemann, Jan Bernd, Vorratsdaten und Urheberrecht – Zulässige Nutzung gespeicherter Daten, NJW 2008, S. 3095 ff.
von Danwitz, Thomas, Zu Funktion und Bedeutung der Rechtsverhältnislehre, Die Verwaltung 30 (1997), S. 339 ff.
Degenhart, Christoph, Staatsrecht I Staatsorganisationsrecht, 25. Aufl., Heidelberg 2009; zitiert: *Degenhart*, Staatsorganisationsrecht.
– Die Neuordnung der Gesetzgebungskompetenzen durch die Föderalismusreform, NVwZ 2006, S. 1209 ff.
Determann, Lothar, Kommunikationsfreiheit im Internet: Freiheitsrechte und gesetzliche Beschränkungen, Baden-Baden 1999; zitiert: *Determann*, Kommunikationsfreiheit.
Detterbeck, Steffen, Allgemeines Verwaltungsrecht, 7. Aufl., München 2009; zitiert: *Detterbeck*, AllgVerwR.
Deutsch, Markus, Die heimliche Erhebung von Informationen und deren Aufbewahrung durch die Polizei, Heidelberg 1992; zitiert: *Deutsch*, Erhebung von Informationen.
Di Fabio, Udo, Verwaltung und Verwaltungsrecht zwischen gesellschaftlicher Selbstregulierung und staatlicher Steuerung, VVDStRL 56 (1997), S. 235 ff.
– Gefahr, Vorsorge, Risiko: Die Gefahrenabwehr unter dem Einfluss des Vorsorgeprinzips, JURA 1996, S. 566 ff.
Dörr, Dieter/Schwartmann, Rolf, Medienrecht, 2. Aufl., Heidelberg 2008; zitiert: *Dörr/Schwartmann*, Medienrecht.
Dörr, Dieter/Kreile, Johannes/Cole, Mark D. (Hrsg.), Handbuch Medienrecht, Frankfurt am Main 2008; zitiert: *Bearbeiter*, in: Dörr/Kreile/Cole, Medienrecht.
Dorsch, Claudia, Die Effizienz der Überwachung der Telekommunikation nach den §§ 100a, 100b StPO, Berlin 2005; zitiert: *Dorsch*, Effizienz der Überwachung der Telekommunikation.
Dreier, Horst (Hrsg.), Grundgesetz-Kommentar, Bd. 3, 2. Aufl., Tübingen 2008; zitiert: *Bearbeiter*, in: Dreier, GG, Bd. 3.
– Grundgesetz-Kommentar, Bd. 2, 2. Aufl., Supplementum, Tübingen 2007; zitiert: *Bearbeiter*, in: Dreier, GG, Bd. 2 Supplementum.
– Grundgesetz-Kommentar, Bd. 2, 2. Aufl., Tübingen 2006; zitiert: *Bearbeiter*, in: Dreier, GG, Bd. 2.
– Grundgesetz-Kommentar, Bd. 1, 2. Aufl., Tübingen 2004; zitiert: *Bearbeiter*, in: Dreier, GG, Bd. 1.
Dreier, Horst, Hierarchische Verwaltung im demokratischen Staat, Tübingen 1991; zitiert: *Dreier*, Hierarchische Verwaltung.
Dürscheid, Christa, E-Mail und SMS – ein Vergleich, in: Arne Ziegler/Christa Dürscheid (Hrsg.), Kommunikationsform E-Mail, Tübingen 2007, S. 93 ff.; zitiert: *Dürscheid*, in: Ziegler/Dürscheid, Kommunikationsform E-Mail.

Eberle, Carl-Eugen/Rudolf, Walter/Wasserburg, Klaus (Hrsg.), Mainzer Rechtshandbuch der Neuen Medien, Heidelberg 2003; zitiert: *Bearbeiter*, in: Eberle/Rudolf/Wasserburg, Mainzer Rechtshandbuch.

Ehlers, Dirk, Verwaltungsgerichtliche Feststellungsklage, JURA 2007, S. 179 ff.

– Die allgemeine verwaltungsgerichtliche Leistungsklage, JURA 2006, S. 351 ff.

– Die Fortsetzungsfeststellungsklage, JURA 2001, S. 415 ff.

– Ungeschriebene Kompetenzen, JURA 2000, S. 323 ff.

– Die Klagebefugnis nach deutschem, europäischem Gemeinschafts- und U.S.-amerikanischem Recht, VerwArch. 84 (1993), S. 139 ff.

– Verwaltung in Privatrechtsform, Berlin 1984; zitiert: *Ehlers*, Verwaltung in Privatrechtsform.

Eifert, Martin, Informationelle Selbstbestimmung im Internet – Das BVerfG und die Online-Durchsuchung, NVwZ 2008, S. 521 ff.

Eisenberg, Ulrich, Kriminologie, 6. Aufl., München 2005; zitiert: *Eisenberg*, Kriminologie.

Eisenberg, Ulrich/Puschke, Jens, Anmerkung zum Urteil des BVerwG vom 23. 11. 2005 – 6 C 2.05. , JZ 2006, S. 729 ff.

Engel-Flechsig, Stefan/Maennel, Frithjof A./Tettenborn, Alexander, Das neue Informations- und Kommunikationsdienste-Gesetz, NJW 1997, S. 2981 ff.

Epping, Volker, Grundrechte, 4. Aufl., Heidelberg (u. a.) 2009; zitiert: *Epping*, Grundrechte.

Epping, Volker/Hillgruber, Christian (Hrsg.), Grundgesetz-Kommentar, München 2009; zitiert: *Bearbeiter*, in: Epping/Christian, GG.

Erichsen, Hans-Uwe, Polizeiliche Standardmaßnahmen, JURA 1993, S. 45 ff.

– Vorläufiger Rechtsschutz nach § 80 Abs. 1–4 VwGO, JURA 1984, S. 414 ff.

– Die Umsetzung von Beamten, DVBl. 1982, S. 95 ff.

Erichsen, Hans-Uwe/Ehlers, Dirk (Hrsg.), Allgemeines Verwaltungsrecht, 13. Aufl., Berlin 2006; zitiert: *Bearbeiter*, in: Erichsen/Ehlers, AllgVerwR.

Erichsen, Hans-Uwe/Klenke, Reiner, Rechtsfragen der „aufschiebenden Wirkung" des § 80 VwGO, DÖV 1976, S. 833 ff.

Ermert, Monika, Lauschverhalten unter der Lupe, c't 1/2006, S. 44 f.

Ernst, Stefan, Das neue Computerstrafrecht, NJW 2007, S. 2661 ff.

Eyermann, Erich (Begr.), Verwaltungsgerichtsordnung-Kommentar, 12. Aufl., München 2006; zitiert: *Bearbeiter*, in: Eyermann, VwGO.

Fahr, Robert, Die Neuregelung der Telekommunikationsüberwachung – Steuerberater fahren beim Zeugnisverweigerungsrecht künftig nur noch „zweiter Klasse", DStR 2008, S. 375 ff.

Fechner, Frank, Medienrecht, 10. Aufl., Stuttgart 2009; zitiert: *Fechner*, Medienrecht.

Fink, Udo, Selbstbestimmung und Selbsttötung: verfassungsrechtliche Fragestellungen im Zusammenhang mit Selbsttötungen, München (u. a.) 1992; zitiert: *Fink*, Selbstbestimmung und Selbsttötung.

Fleury, Roland, Verfassungsprozessrecht, 8. Aufl., München (u. a.) 2009; zitiert: *Fleury*, Verfassungsprozessrecht.

Friedrich, Dirk, Die Verpflichtung privater Telekommunikationsunternehmen, die staatliche Überwachung und Aufzeichnung der Telekommunikation zu ermöglichen, Aachen 2001; zitiert: *Friedrich*, Verpflichtung privater Telekommunikationsunternehmen.

Geis, Ivo/Geis, Esther, Beschlagnahme von E-Mails im Serverbereich – Wie weit reicht der Schutzbereich von Art. 10 Abs. 1 GG?, MMR 2006 Heft 11, S. X f.

Geppert, Martin/Piepenbrock, Hermann-Josef/Schütz, Raimund/Schuster, Fabian (Hrsg.), Beck'scher Telekommunikationsgesetz-Kommentar, 3. Aufl., München 2006; zitiert: *Bearbeiter*, in: Geppert/Piepenbrock/Schütz/Schuster, TKG.

Gercke, Marco, Heimliche Online-Durchsuchung: Anspruch und Wirklichkeit, CR 2007, S. 245 ff.

Germann, Michael, Gefahrenabwehr und Strafverfolgung im Internet, Berlin 2000; zitiert: *Germann*, Gefahrenabwehr und Strafverfolgung.

Gersdorf, Hubertus, Verwaltungsprozessrecht, 4. Aufl., Heidelberg 2009; zitiert: *Gersdorf*, Verwaltungsprozessrecht.

Gietl, Andreas, Störerhaftung für ungesicherte Funknetze – Voraussetzungen und Grenzen, MMR 2007, S. 630 ff.

Götz, Volkmar, Allgemeines Polizei- und Ordnungsrecht, 14. Aufl., München 2008; zitiert: *Götz*, PolR.

Gola, Peter/Schomerus, Rudolf, Bundesdatenschutzgesetz, 9. Aufl., München 2007; zitiert: *Gola/Schomerus*, BDSG.

Gostomzyk, Tobias, Grundrechte als objektiv-rechtliche Ordnungsidee, JuS 2004, S. 949 ff.

Graulich, Kurt, Telekommunikationsgesetz und Vorratsdatenspeicherung (Zugleich Anmerkung zu BVerfG, B. v. 11. 3. 2008 – 1 BvR 256/08 –), NVwZ 2008, S. 485 ff.

– Die Novellierung des Hessischen Gesetzes über die öffentliche Sicherheit und Ordnung im Jahr 2004, NVwZ 2005, S. 271 ff.

Greiner, Arved, Die Verhinderung verbotener Internetinhalte im Wege polizeilicher Gefahrenabwehr, Hamburg 2001; zitiert: *Greiner*, Verhinderung verbotener Internetinhalte.

Griesbeck, Michael, Die materielle Polizeipflicht des Zustandsstörers und die Kostentragungspflicht nach unmittelbarer Ausführung und Ersatzvornahme, Berlin 1991; zitiert: *Griesbeck*, Kostentragungspflicht.

Gröpl, Christoph, Staatsrecht I, München 2008; zitiert: *Gröpl*, Staatsrecht.

Gröschner, Rolf, Vom Nutzen des Verwaltungsrechtsverhältnisses, Die Verwaltung 30 (1997), S. 301 ff.

Gröseling, Nadine/Höfinger, Frank Michael, Computersabotage und Vorfeldkriminalisierung – Auswirkungen des 41. StrÄndG zur Bekämpfung der Computerkriminalität, MMR 2007, S. 626 ff.

Groß, Thomas, Die Schutzwirkung des Brief-, Post- und Fernmeldegeheimnisses nach der Privatisierung der Post, JZ 1999, S. 326 ff.

Günther, Ralf, Zur strafprozessualen Erhebung von Telekommunikationsdaten – Verpflichtung zur Sachverhaltsaufklärung oder verfassungsrechtlich unkalkulierbares Wagnis?, NStZ 2005, S. 485 ff.

Gusy, Christoph, Polizei- und Ordnungsrecht, 7. Aufl., Tübingen 2009; zitiert: *Gusy*, PolR.

– Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme. Neuer Grundrechtsname oder neues Grundrechtsschutzgut?, DuD 2009, S. 33 ff.

– Präventiv-polizeiliche Telekommunikationsüberwachung, Die Polizei 2004, S. 61 ff.

– Überwachung der Telekommunikation unter Richtervorbehalt – Effektiver Grundrechtsschutz oder Alibi?, ZRP 2003, S. 275 ff.

– Verfassungsfragen vorbeugenden Rechtsschutzes, JZ 1998, S. 167 ff.

Härting, Niko, IT-Sicherheit in der Anwaltskanzlei – Das Anwaltsgeheimnis im Zeitalter der Informationstechnologie, NJW 2005, S. 1248 ff.

Hain, Karl-Eberhard, Der Gesetzgeber in der Klemme zwischen Übermaß- und Untermaßverbot?, DVBl. 1993, S. 982 ff.

von Hammerstein, Christian, Kostentragung für staatliche Überwachungsmaßnahmen nach der TKG-Novelle, MMR 2004, S. 222 ff.

Hannich, Rolf (Hrsg.), Karlsruher Kommentar zur Strafprozessordnung, 6. Aufl., München 2008; zitiert: *Bearbeiter*, in: Hannich, StPO.

Haug, Volker, Grundwissen Internetrecht, Stuttgart 2005; *Haug*, Internetrecht.

Haurand, Günter/Vahle, Jürgen, Rechtliche Aspekte der Gefahrenabwehr in Entführungsfällen, NVwZ 2003, S. 513 ff.

Heghmanns, Michael/Scheffler, Uwe (Hrsg.), Handbuch zum Strafverfahren, München 2008; zitiert: *Bearbeiter*, in: Heghmanns/Scheffler, Handbuch zum Strafverfahren.

von Heimburg, Sibylle, Verwaltungsaufgaben und Private, Berlin 1982; zitiert: *von Heimburg*, Verwaltungsaufgaben.

Heintzen, Markus, Was standardisieren Standardmaßnahmen?, DÖV 2005, S. 1038 ff.

– Beteiligung Privater an der Wahrnehmung öffentlicher Aufgaben und staatliche Verantwortung, VVDStRL 62 (2003), S. 220 ff.

Hellermann, Johannes, Die sogenannte negative Seite der Freiheitsrechte, Berlin 1993; zitiert: *Hellermann*, Negative Seite der Freiheitsrechte.

Hermes, Georg, Das Grundrecht auf Schutz von Leben und Gesundheit, Heidelberg 1987; zitiert: *Hermes*, Grundrecht.

Heun, Sven-Erik (Hrsg.), Handbuch Telekommunikationsrecht, 2. Aufl., Köln 2007; zitiert: *Bearbeiter*, in: Heun, Handbuch Telekommunikationsrecht.

Hillgruber, Christian/Goos, Christoph, Verfassungsprozessrecht, 2. Aufl., Heidelberg 2006; zitiert: *Hillgruber/Goos*, Verfassungsprozessrecht.

Hirsch, Burkhard, Das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme – Zugleich Anmerkung zu BVerfG, NJW 2008, 822, NJOZ 2008, S. 1907 ff.

Hömig, Dieter, „Neues" Grundrecht, neue Fragen? Zum Urteil des BVerfG zur Online-Durchsuchung (Anmerkung zu BVerfG U. v. 27. 2. 2008 – 1 BvR 370/07 –), JURA 2009, S. 207 ff.

Hömig, Dieter (Hrsg.), Grundgesetz-Kommentar, 8. Aufl., Baden-Baden 2007; zitiert: *Bearbeiter*, in: Hömig, GG.

Hoeren, Thomas, Vorratsdaten und Urheberrecht – Keine Nutzung gespeicherter Daten, NJW 2008, S. 3099 ff.

– Das Telemediengesetz, NJW 2007, S. 801 ff.

– Grundzüge des Internetrechts, 2. Aufl., München 2002; zitiert: *Hoeren*, Grundzüge des Internetrechts.

Hoeren, Thomas/Sieber, Ulrich (Hrsg.), Handbuch Multimedia-Recht, München, Stand: Oktober 2008; zitiert: *Bearbeiter*, in: Hoeren/Sieber, Multimedia-Recht.

Hoffmann, Helmut, Zivilrechte Haftung im Internet, MMR 2002, S. 284 ff.

Hoffmann-Riem, Wolfgang, Der grundrechtliche Schutz der Vertraulichkeit und Integrität eigengenutzter informationstechnischer Systeme, JZ 2008, S. 1009 ff.

– Verwaltungsrecht in der Informationsgesellschaft – Einleitende Problemskizze, in: Wolfgang Hoffmann-Riem/Eberhard Schmidt-Aßmann (Hrsg.), Verwaltungsrecht in der Informationsgesellschaft, Baden-Baden 2000, S. 9 ff.; zitiert: *Hoffmann-Riem*, in: Hoffmann-Riem/Schmidt-Aßmann, Informationsgesellschaft.

Hoffmann-Riem, Wolfgang/Schmidt-Aßmann, Eberhard/Voßkuhle, Andreas (Hrsg.), Grundlagen des Verwaltungsrechts, Bd. 3, München 2009; zitiert: *Bearbeiter*, in: Hoffmann-Riem/Schmidt-Aßmann/Voßkuhle, GVwR, Bd. 3.

– Grundlagen des Verwaltungsrechts, Bd. 2, München 2008; zitiert: *Bearbeiter*, in: Hoffmann-Riem/Schmidt-Aßmann/Voßkuhle, GVwR, Bd. 2.

– Grundlagen des Verwaltungsrechts, Bd. 1, München 2006; zitiert: *Bearbeiter*, in: Hoffmann-Riem/Schmidt-Aßmann/Voßkuhle, GVwR, Bd. 1.

Hoffmann-Riem, Wolfgang/Schulz, Wolfgang/Held, Thorsten, Konvergenz und Regulierung, Baden-Baden 2000; zitiert: *Hoffmann-Riem/Schulz/Held*, Konvergenz und Regulierung.

Hofmann, Manfred, Die Online-Durchsuchung – staatliches „Hacken" oder zulässige Ermittlungsmaßnahme?, NStZ 2005, S. 121 ff.

Hollands, Martin, Gefahrenzurechnung im Polizeirecht, Berlin 2005; zitiert: *Hollands*, Gefahrenzurechnung.

Holznagel, Bernd, Konvergenz der Medien – Herausforderung an das Recht, NJW 2002, S. 2351 ff.

Holznagel, Bernd/Ricke, Thorsten, Die Aufsicht im Internet – Wer hat noch nicht, wer will noch mal?, MMR 2008, S. 18 ff.

Holznagel, Bernd/Bonnekoh, Mareike, Voice over IP – Regulierungsbedarf und erste Lösungen, MMR 2005, S. 585 ff.

Horn, Hans-Detlef, Vorbeugende Rasterfahndung und informationelle Selbstbestimmung, DÖV 2003, S. 746 ff.

Hornung, Gerrit, Ein neues Grundrecht. Der verfassungsrechtliche Schutz der „Vertraulichkeit und Integrität informationstechnischer Systeme", CR 2008, S. 299 ff.
– Wireless und speicherpflichtig? Die Vorratsdatenspeicherung und der Betrieb von W-LAN-Systemen, MMR 2007 Heft 12, S. XIII.
– Ermächtigungsgrundlage für die „Online-Durchsuchung"? Verfassungsrechtliche Anforderungen an und Grenzen für den heimlichen Zugriff auf IT-Systeme im Ermittlungsverfahren, DuD 2007, S. 575 ff.
– Zwei runde Geburtstage: Das Recht auf informationelle Selbstbestimmung und das WWW, MMR 2004, S. 3 ff.
Huber, Bertold, Heimliche „Online-Durchsuchung" nach dem Nordrhein-Westfälischen Verfassungsschutzgesetz, NVwZ 2007, S. 880 ff.
Hufen, Friedhelm, Staatsrecht II Grundrechte, 2. Aufl., München 2009; zitiert: *Hufen*, Grundrechte.
– Verwaltungsprozessrecht, 7. Aufl., München 2008; zitiert: *Hufen*, Verwaltungsprozessrecht.
– Schutz der Persönlichkeit und Recht auf informationelle Selbstbestimmung, in: Peter Badura/Horst Dreier (Hrsg.), Festschrift 50 Jahre BVerfG, Bd. 2, Tübingen 2001, S. 105 ff.; zitiert: *Hufen*, in: Badura/Dreier, FS BVerfG.
Ipsen, Hans Peter, Gesetzliche Indienstnahme Privater für Verwaltungsaufgaben, in: Um Recht und Gerechtigkeit: Festgabe für Erich Kaufmann zu seinem 70. Geburtstag, Stuttgart (u. a.) 1950, S. 141 ff.; zitiert: *H. P. Ipsen*, in: FS Kaufmann.
Ipsen, Jörn, Staatsrecht I Staatsorganisationsrecht, 21. Aufl., München (u. a.) 2009; zitiert: *J. Ipsen*, Staatsorganisationsrecht.
– Staatsrecht II Grundrechte, 12. Aufl., München (u. a.) 2009; zitiert: *J. Ipsen*, Grundrechte.
– Allgemeines Verwaltungsrecht, 6. Aufl., München 2009; zitiert: *J. Ipsen*, AllgVerwR.
– Die Kompetenzverteilung zwischen Bund und Ländern nach der Föderalismusnovelle, NJW 2006, S. 2801 ff.
Isensee, Josef/Kirchhof, Paul (Hrsg.), Handbuch des Staatsrechts der Bundesrepublik Deutschland, Bd. 7, 3. Aufl., Heidelberg 2009; zitiert: *Bearbeiter*, in: Isensee/Kirchhof, HStR, Bd. 7.
– Handbuch des Staatsrechts der Bundesrepublik Deutschland, Bd. 6, 3. Aufl., Heidelberg 2008; zitiert: *Bearbeiter*, in: Isensee/Kirchhof, HStR, Bd. 6, 3. Aufl.
– Handbuch des Staatsrechts der Bundesrepublik Deutschland, Bd. 5, 3. Aufl., Heidelberg 2007; zitiert: *Bearbeiter*, in: Isensee/Kirchhof, HStR, Bd. 5, 3. Aufl.
– Handbuch des Staatsrechts der Bundesrepublik Deutschland, Bd. 4, 3. Aufl., Heidelberg 2006; zitiert: *Bearbeiter*, in: Isensee/Kirchhof, HStR, Bd. 4.
– Handbuch des Staatsrechts der Bundesrepublik Deutschland, Bd. 3, 3. Aufl., Heidelberg 2005; zitiert: *Bearbeiter*, in: Isensee/Kirchhof, HStR, Bd. 3.
– Handbuch des Staatsrechts der Bundesrepublik Deutschland, Bd. 2, 3. Aufl., Heidelberg 2004; zitiert: *Bearbeiter*, in: Isensee/Kirchhof, HStR, Bd. 2.

– Handbuch des Staatsrechts der Bundesrepublik Deutschland, Bd. 6, 2. Aufl., Heidelberg 2001; zitiert: *Bearbeiter*, in: Isensee/Kirchhof, HStR, Bd. 6, 2. Aufl.
– Handbuch des Staatsrechts der Bundesrepublik Deutschland, Bd. 5, 2. Aufl., Heidelberg 2000; zitiert: *Bearbeiter*, in: Isensee/Kirchhof, HStR, Bd. 5, 2. Aufl.
Jahn, Matthias, Strafprozessuale Eingriffsmaßnahmen im Lichte der aktuellen Rechtsprechung des BVerfG- – Unter besonderer Berücksichtigung der in BVerfGK 1–5 veröffentlichten Entscheidungen –, NStZ 2007, S. 255 ff.
Jandt, Silke, Das neue TMG – Nachbesserungsbedarf für den Datenschutz im Mehrpersonenverhältnis, MMR 2006, S. 652 ff.
Jarass, Hans D., Indienstnahme Privater und Systemgerechtigkeit im Sozialrecht, VSSR 2007, S. 103 ff.
– Allgemeine Probleme der Gesetzgebungskompetenz des Bundes, NVwZ 2000, S. 1089 ff.
Jarass, Hans D./Pieroth, Bodo, Grundgesetz-Kommentar, 10. Aufl., München 2009; zitiert: *Bearbeiter*, in: Jarass/Pieroth, GG.
Jehke, Christian, Bestimmtheit und Klarheit im Steuerrecht, Berlin 2005; zitiert: *Jehke*, Bestimmtheit und Klarheit.
Käß, Robert, Die Einführung der präventiven Telekommunikationsüberwachung im Bayerischen Polizeiaufgabengesetz (PAG), BayVBl. 2008, S. 225 ff.
Kastner, Berthold, Verdachtsunabhängige Personenkontrollen im Lichte des Verfassungsrechts, VerwArch 92 (2001), S. 216 ff.
Kemper, Martin, Die Beschlagnahmefähigkeit von Daten und E-Mails, NStZ 2005, S. 538 ff.
Kindhäuser, Urs, Strafprozessrecht, Baden-Baden 2006; zitiert: *Kindhäuser*, Strafprozessrecht.
Klein, Hans H., Die grundrechtliche Schutzpflicht, DVBl. 1994, S. 489 ff.
Kleine-Voßbeck, Bernd, Electronic Mail und Verfassungsrecht, Marburg 2000; *Kleine-Voßbeck*, Electronic Mail.
Klenke, Reinhard, Zur sogenannten Subsidiarität der Feststellungsklage, NWVBl. 2003, S. 170 ff.
Kloepfer, Michael, Informationsrecht, München 2002; zitiert: *Kloepfer*, Informationsrecht.
Kluth, Winfried (Hrsg.), Föderalismusreformgesetz, Baden-Baden 2007; zitiert: *Bearbeiter*, in: Kluth, Föderalismusreformgesetz.
Knack, Hans Joachim (Begr.), Verwaltungsverfahrensgesetz-Kommentar, 9. Aufl., München (u. a.) 2010; zitiert: *Bearbeiter*, in: Knack/Henneke, VwVfG.
Knemeyer, Franz-Ludwig, Polizei- und Ordnungsrecht, 11. Aufl., München 2007; zitiert: *Knemeyer*, PolR.
– Datenerhebung, Datenverarbeitung und Datennutzung als Kernaufgaben polizeilicher Vorbereitung auf die Gefahrenabwehr und Straftatenverfolgung (Informationsvorsorge), in: Hans-Wolfgang Arndt/Franz-Ludwig Knemeyer/Dieter Kugelmann/Werner Meng/Michael Schweitzer (Hrsg.), Völkerrecht und deutsches Recht: Festschrift für Walter Rudolf zum 70. Geburtstag, München

2001, S. 483 ff.; zitiert: *Knemeyer*, in: Arndt/Knemeyer/Kugelmann/Meng/Schweitzer, FS Rudolf.
– Der Schutz der Allgemeinheit und der individuellen Rechte durch die polizei- und ordnungsrechtlichen Handlungsvollmachten der Exekutive, VVDStRL 35 (1977), S. 221 ff.
Koch, Martin, Datenerhebung und -verarbeitung in den Polizeigesetzen der Länder, Baden-Baden 1999; zitiert: *Koch*, Datenerhebung.
Köhler, Markus/Arndt, Hans Wolfgang/Fetzer, Thomas, Recht des Internet, 6. Aufl., Heidelberg 2008; zitiert: *Köhler/Arndt/Fetzer*, Recht des Internet.
Kopp, Ferdinand O., Grundrechtliche Schutz- und Förderungspflichten der öffentlichen Hand, NJW 1994, S. 1573 ff.
Kopp, Ferdinand O./Ramsauer, Ulrich, Verwaltungsverfahrensgesetz-Kommentar, 10. Aufl., München 2008; zitiert: *Kopp/Ramsauer*, VwVfG.
Kopp, Ferdinand O./Schenke, Wolf-Rüdiger, Verwaltungsgerichtsordnung-Kommentar, 16. Aufl., München 2009; zitiert: *Kopp/W.-R. Schenke*, VwGO.
Krempl, Stefan, In der Abhörfalle, c't 26/2004, S. 100 ff.
Krüpe-Gescher, Christiane, Die Überwachung der Telekommunikation nach den §§ 100a, 100b StPO in der Rechtspraxis, Berlin 2005; zitiert: *Krüpe-Gescher*, Überwachung der Telekommunikation.
Kühling, Jürgen/Elbracht, Alexander, Telekommunikationsrecht, Heidelberg 2008; zitiert: *Kühling/Elbracht*, Telekommunikationsrecht.
Künast, Renate, Am Anfang steht die Menschenwürde: Ein Grundgesetz für das 21. Jahrhundert, NJW 2009, S. 1723 ff.
Kugelmann, Dieter, Polizei- und Ordnungsrecht, Heidelberg (u. a.) 2006; zitiert: *Kugelmann*, PolR.
– Das Informationsfreiheitsgesetz des Bundes, NJW 2005, S. 3609 ff.
– Der polizeiliche Gefahrenbegriff in Gefahr?, DÖV 2003, S. 781 ff.
Kunig, Philip, Das Rechtsstaatsprinzip: Überlegungen zu seiner Bedeutung für das Verfassungsrecht der Bundesrepublik Deutschland, Tübingen 1986; zitiert: *Kunig*, Rechtsstaatsprinzip.
Kutscha, Martin, Mehr Schutz von Computerdaten durch ein neues Grundrecht?, NJW 2008, S. 1042 ff.
– Überwachungsmaßnahmen von Sicherheitsbehörden im Fokus der Grundrechte, LKV 2008, S. 481 ff.
– Verdeckte „Online-Durchsuchung" und Unverletzlichkeit der Wohnung, NJW 2007, S. 1169 ff.
– Verfassungsrechtlicher Schutz des Kernbereichs privater Lebensgestaltung – nichts Neues aus Karlsruhe?, NJW 2005, S. 20 ff.
– Neue Grenzmarken des Polizeiverfassungsrechts, NVwZ 2005, S. 1231 ff.
– Rechtsschutzdefizite bei Grundrechtseingriffen von Sicherheitsbehörden, NVwZ 2003, 1296 ff.
– Novellierung des Thüringer Polizeiaufgabengesetzes – Mehr Sicherheit durch weniger Grundrechtsschutz?, LKV 2003, S. 114 ff.
Lambiris, Andreas, Klassische Standardbefugnisse im Polizeirecht, Stuttgart (u. a.) 2001; zitiert: *Lambiris*, Klassische Standardbefugnisse.

Lang, Markus, Die Grundrechtsberechtigung der Nachfolgeunternehmen im Eisenbahn-, Post- und Telekommunikationswesen, NJW 2004, S. 3601 ff.
Laubinger, Hans-Werner, Feststellungsklage und Klagebefugnis (§ 42 Abs. 2 VwGO), VerwArch. 82 (1991), S. 459 ff.
Leipold, Klaus, Die Online-Durchsuchung, NJW-Spezial 2007, S. 135 ff.
Leisner, Anna, Die polizeiliche Gefahr zwischen Eintrittswahrscheinlichkeit und Schadenshöhe, DÖV 2002, S. 326 ff.
Leisner, Walter/Görlich, Helmut, Das Recht auf Leben: Untersuchungen zu Artikel 2 Abs. 2 des Grundgesetzes für die Bundesrepublik Deutschland, Hannover 1976; zitiert: *Bearbeiter*, in: Leisner/Görlich, Recht auf Leben.
Lingemann, Michael, Die Gefahrenprognose als Basis eines polizeilichen Beurteilungsprogramms?, Bochum 1985; zitiert: *Lingemann*, Gefahrenprognose.
Lisken, Hans, Zur polizeilichen Rasterfahndung, NVwZ 2002, S. 513 ff.
Lisken, Hans/Denninger, Erhard (Hrsg.), Handbuch des Polizeirechts, 4. Aufl., München 2007; zitiert: *Bearbeiter*, in: Lisken/Denninger, HPolR.
Lorenz, Dieter, Verwaltungsprozessrecht, Heidelberg (u. a.) 2000; zitiert: *Lorenz*, Verwaltungsprozessrecht.
von Mangoldt, Hermann/Klein, Friedrich/Starck, Christian (Hrsg.), Grundgesetz-Kommentar, Bd. 1, 5. Aufl., München 2005; zitiert: *Bearbeiter*, in: von Mangoldt/Klein/Starck, GG, Bd. 1.
– Grundgesetz-Kommentar, Bd. 2, 5. Aufl., München 2005; zitiert: *Bearbeiter*, in: von Mangoldt/Klein/Starck, GG, Bd. 2.
– Grundgesetz-Kommentar, Bd. 3, 5. Aufl., München 2005; zitiert: *Bearbeiter*, in: von Mangoldt/Klein/Starck, GG, Bd. 3.
Manssen, Gerrit, Staatsrecht II Grundrechte, 6. Aufl., München 2009; zitiert: *Manssen*, Grundrechte.
Manssen, Gerrit (Hrsg.), Telekommunikations- und Multimediarecht-Kommentar, Berlin, Stand: 01.2008; zitiert: *Bearbeiter*, in: Manssen, Telekommunikations- und Multimediarecht.
Martensen, Jürgen, Materielle Polizeipflicht und polizeiliche Verpflichtbarkeit des Bürgers in Anscheins- und Verdachtslagen, DVBl. 1996 S. 286 ff.
Masing, Johannes, Transparente Verwaltung: Konturen eines Informationsverwaltungsrechts, VVDStRL 63 (2004), S. 377 ff.
Maunz, Theodor/Dürig, Günter (Begr.), Grundgesetz-Kommentar, München, Stand: Januar 2009; zitiert: *Bearbeiter*, in: Maunz/Dürig, GG.
Maurer, Hartmut, Allgemeines Verwaltungsrecht, 17. Aufl., München 2009; zitiert: *Maurer*, AllgVerwR.
– Staatsrecht I, 5. Aufl., München 2007; zitiert: *Maurer*, Staatsrecht.
Meininghaus, *Florian*, Der Zugriff auf E-Mails im strafrechtlichen Ermittlungsverfahren, Hamburg 2007; zitiert: *Meininghaus*, Zugriff auf E-Mails.
Meinke, Monika M., In Verbindung mit, Berlin 2006; zitiert: *Meinke*, Verbindung.
Merten, Detlef/Papier, Hans-Jürgen (Hrsg.), Handbuch der Grundrechte in Deutschland und Europa, Bd. 2, Heidelberg 2006; zitiert: *Bearbeiter*, in: Merten/Papier, HGR, Bd. 2.

– Handbuch der Grundrechte in Deutschland und Europa, Bd. 1, Heidelberg 2004; zitiert: *Bearbeiter*, in: Merten/Papier, HGR, Bd. 1.
Meyer, Hans-Jürgen, Rechtsfragen im Zusammenhang mit polizeilichen Beobachtungsmaßnahmen, Tübingen 1982; zitiert: *Meyer*, Rechtsfragen.
Meyer-Goßner, Lutz, Strafprozessordnung-Kommentar, 52. Aufl., München 2009; zitiert: *Meyer-Goßner*, StPO.
Michael, Lothar/Morlok, Martin, Grundrechte, Baden-Baden 2008; zitiert: *Michael/Morlok*, Grundrechte.
Michaelis, Rüdiger, Der Beliehene, Münster 1969; zitiert: *Michaelis*, Der Beliehene.
Möstl, Markus, Die neue dogmatische Gestalt des Polizeirechts, DVBl. 2007, S. 581 ff.
– Gefahr und Kompetenz, JURA 2005, S. 48 ff.
von Münch, Ingo, Staatsrecht, Bd. 2, 5. Aufl., Stuttgart (u. a.) 2002; zitiert: *von Münch*, Staatsrecht, Bd. 2.
– Grundrechtsschutz gegen sich selbst?, in: Rolf Stödter (Hrsg.), Hamburg, Deutschland, Europa: Festschrift für Hans Peter Ipsen zum 70. Geburtstag, Tübingen 1977, S. 113 ff.; zitiert: *von Münch*, in: Stödter, FS Ipsen.
von Münch, Ingo/Kunig, Philip (Hrsg.), Grundgesetz-Kommentar, Bd. 3, 5. Aufl., München 2003; zitiert: *Bearbeiter*, in: von Münch/Kunig, GG, Bd. 3.
– Grundgesetz-Kommentar, Bd. 2, 5. Aufl., München 2001; zitiert: *Bearbeiter*, in: von Münch/Kunig, GG, Bd. 2.
– Grundgesetz-Kommentar, Bd. 1, 5. Aufl., München 2000; zitiert: *Bearbeiter*, in: von Münch/Kunig, GG, Bd. 1.
von Münch, Ingo/Mager, Ute, Staatsrecht, Bd. 1, 7. Aufl., Stuttgart (u. a.) 2009; zitiert: *von Münch/Mager*, Staatsrecht, Bd. 1.
von Mutius, Albert, Zur Subsidiarität der Feststellungsklage, VerwArch. 63 (1972), S. 229 ff.
Nottbusch, Claudia, Die Beiladung im Verwaltungsprozess, Berlin 1995; zitiert: *Nottbusch*, Beiladung.
Obermayer, Klaus (Begr.), Verwaltungsverfahrensgesetz-Kommentar, 3. Aufl., Kriftel 1999; zitiert: *Bearbeiter*, in: Obermayer, VwVfG.
Ossenbühl, Fritz, Staatshaftungsrecht, 5. Aufl., München 1998; zitiert: *Ossenbühl*, Staatshaftungsrecht.
– Zur Haftung des Gesamtrechtsnachfolgers für Altlasten, Baden-Baden 1995; zitiert: *Ossenbühl*, Altlasten.
– Grundrechtsschutz im und durch Verfahrensrecht, in: Georg Müller/René A. Rhinow/Gerhard Schmid/Luzius Wildhaber (Hrsg.), Staatsorganisation und Staatsfunktionen im Wandel: Festschrift für Kurt Eichenberger zum 60. Geburtstag, Basel (u. a.) 1982, S. 183 ff.; zitiert: *Ossenbühl*, in: Müller/Rhinow/Schmid/Wildhaber, FS Eichenberger.
– Die Erfüllung von Verwaltungsaufgaben durch Private, VVDStRL 29 (1971), S. 137 ff.
Paeffgen, Hans-Ullrich, Art. 30, 70, 101 I GG – vernachlässigbare Normen?, JZ 1991, S. 437 ff.

Papier, Hans-Jürgen, Aktuelle Fragen der bundesstaatlichen Ordnung, NJW 2007, S. 2145 ff.
– Die richterliche Unabhängigkeit und ihre Schranken, NJW 2001, S. 1089 ff.
– Zur rückwirkenden Haftung des Rechtsnachfolgers für Altlasten, DVBl. 1996, S. 125 ff.
Peine, Franz-Joseph, Allgemeines Verwaltungsrecht, 9. Aufl., Heidelberg 2008; zitiert: *Peine*, AllgVerwR.
– Grenzen der Privatisierung – verwaltungsrechtliche Aspekte, DÖV 1997, S. 353 ff.
– Rüstungsaltlasten, DVBl. 1990, S. 733 ff.
Pestalozza, Christian, Verfassungsprozessrecht, 3. Aufl., München 1991; zitiert: *Pestalozza*; Verfassungsprozessrecht.
Peters, Anne, Die Ausfüllung von Spielräumen der Verwaltung durch Wirtschaftlichkeitserwägungen, DÖV 2001, S. 749 ff.
Petersen, Jens, Medienrecht, 4. Aufl., München 2008; zitiert: *Petersen*, Medienrecht.
Petersen, Jens/Schoch, Friedrich, Einführung in das Informationsrecht und das Medienrecht, JURA 2005, S. 681 ff.
Pieroth, Bodo/Schlink, Bernhard, Grundrechte Staatsrecht II, 25. Aufl., Heidelberg 2009; zitiert: *Pieroth/Schlink*, Grundrechte.
Pieroth, Bodo/Schlink, Bernhard/Kniesel, Michael, Polizei- und Ordnungsrecht, 5. Aufl., München 2008; zitiert: *Pieroth/Schlink/Kniesel*, PolR.
Pietzcker, Jost, Das Verwaltungsrechtsverhältnis – archimedischer Punkt oder Münchhausens Zopf?, Die Verwaltung 30 (1997), S. 281 ff.
– Polizeirechtliche Störerbestimmung nach Pflichtwidrigkeit und Risikosphäre, DVBl. 1984, S. 457 ff.
Poscher, Ralf, Grundrechte als Abwehrrechte: reflexive Regelung rechtlich geordneter Freiheit, Tübingen 2003; zitiert: *Poscher*, Abwehrrechte.
Posser, Herbert/Wolff, Heinrich Amadeus (Hrsg.), Verwaltungsgerichtsordnung-Kommentar, München 2008; zitiert: *Bearbeiter*, in: Posser/Wolff, VwGO.
Puschke, Jens/Singelnstein, Tobias, Telekommunikationsüberwachung, Vorratsdatenspeicherung und (sonstige) heimliche Ermittlungsmaßnahmen der StPO nach der Neuregelung zum 1. 1. 2008, NJW 2008, S. 113 ff.
– Verfassungsrechtliche Vorgaben für heimliche Informationsbeschaffungsmaßnahmen, NJW 2005, 3534 ff.
Randl, Hans, Verfassungsrechtliche Aspekte des neuen Hamburger Polizeirechts, NVwZ 1992, S. 1070 ff.
Redeker, Konrad/von Oertzen, Hans-Joachim (Begr.), Verwaltungsgerichtsordnung-Kommentar, 14. Aufl., Stuttgart (u. a.) 2004; zitiert: *Bearbeiter*, in: Redeker/von Oertzen, VwGO.
Remmert, Barbara, Private Dienstleistungen in staatlichen Verwaltungsverfahren, Tübingen 2003; zitiert: *Remmert*, Private Dienstleistungen.
Rieß, Peter (Hrsg.), Die Strafprozessordnung und das Gerichtsverfassungsgesetz-Kommentar, Bd. 2, 25. Aufl., Berlin 2003; zitiert: *Bearbeiter*, in: Rieß, StPO.

Roggan, Fredrik/Bergemann, Nils, Die „neue Sicherheitsarchitektur" der Bundesrepublik Deutschland – Anti-Terror-Datei, gemeinsame Projektdateien und Terrorismusbekämpfungsergänzungsgesetz, NJW 2007, S. 876 ff.

Rossi, Matthias, Informationszugangsfreiheit und Verfassungsrecht, Berlin 2004; zitiert: *Rossi*, Informationszugangsfreiheit.

Roßnagel, Alexander, Das Telemediengesetz – Neuordnung für Informations- und Kommunikationsdienste, NVwZ 2007, S. 743 ff.

– Datenschutz in der künftigen Verkehrstelematik, NZV 2006, S. 281 ff.

– Neues Recht für Multimediadienste – Informations- und Kommunikationsdienste-Gesetz und Mediendienste-Staatsvertrag, NVwZ 1998, S. 1 ff.

Roßnagel, Alexander/Schnabel, Christoph, Das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme und sein Einfluss auf das Privatrecht, NJW 2008, S. 3534 ff.

Rozek, Jochen, Grundfälle zur verwaltungsgerichtlichen Fortsetzungsfeststellungsklage, JuS 1995, S. 414 ff.

Rux, Johannes, Ausforschung privater Rechner durch die Polizei- und Sicherheitsbehörden, JZ 2007, S. 285 ff.

Sachs, Michael, Verfassungsprozessrecht, 2. Aufl., Frankfurt am Main 2007; zitiert: *Sachs*, Verfassungsprozessrecht.

– Verfassungsrecht II Grundrechte, 2. Aufl., Heidelberg (u. a.) 2003; zitiert: *Sachs*, Grundrechte.

Sachs, Michael (Hrsg.), Grundgesetz-Kommentar, 5. Aufl., München 2009; zitiert: *Bearbeiter*, in: Sachs, GG.

Sachs, Michael/Kring, Thomas, Das neue „Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme", JuS 2008, S. 481 ff.

Säcker, Franz Jürgen (Hrsg.), Berliner Kommentar zum Telekommunikationsgesetz, 2. Aufl., Frankfurt am Main 2009; zitiert: *Bearbeiter*, in: Säcker, TKG.

Sankol, Barry, Das sog. „Raumgespräch" und seine Verwertbarkeit im Strafverfahren, MMR 2007, S. 692 ff.

Saurer, Johannes, Die Ausweitung sicherheitsrechtlicher Regelungsansprüche im Kontext der Terrorismusbekämpfung, NVwZ 2005, S. 275 ff.

Schäfer, Heike, Präventive Telekommunikationsüberwachung, Freiburg im Breisgau 2007; zitiert: *Schäfer*, Präventive Telekommunikationsüberwachung.

Schenke, Wolf-Rüdiger, Polizei- und Ordnungsrecht, 6. Aufl., Heidelberg 2009; zitiert: *W.-R. Schenke*, PolR.

– Verwaltungsprozessrecht, 12. Aufl., Heidelberg 2009; zitiert: *W.-R. Schenke*, Verwaltungsprozessrecht.

– Die Rechtsnatur einer erkennungsdienstlichen Maßnahme gem. § 81b Alt. 2 StPO, JZ 2006, S. 707 ff.

Schenke, Ralf P., Verfassungsrechtliche Probleme einer präventiven Überwachung der Telekommunikation, AöR 125 (2000), S. 1 ff.

Scherzberg, Arno, Die Öffentlichkeit der Verwaltung, Baden-Baden 2000; zitiert: *Scherzberg*, Öffentlichkeit.

Scheurle, Klaus-Dieter/Mayen, Thomas (Hrsg.), Telekommunikationsgesetz-Kommentar, 2. Aufl., München 2008; zitiert: *Bearbeiter*, in: Scheurle/Mayen, TKG.

Schlaich, Klaus/Korioth, Stefan, Das Bundesverfassungsgericht, 7. Aufl., München 2007; zitiert: *Schlaich/Korioth*, Bundesverfassungsgericht.

Schlegel, Stephan, „Beschlagnahme" von E-Mail-Verkehr beim Provider, HRRS 2007, S. 44 ff., http://www.hrr-strafrecht.de.

Schlette, Volker, Die Verwaltung als Vertragspartner: Empirie und Dogmatik verwaltungsrechtlicher Vereinbarungen zwischen Behörde und Bürger, Tübingen 2000; zitiert: *Schlette*, Verwaltung als Vertragspartner.

Schmidt, Otto, E-Mail-Kontrolle durch Arbeitgeber, CR 2003, S. 839 ff.

Schmidt-Aßmann, Eberhard, Das allgemeine Verwaltungsrecht als Ordnungsidee, 2. Aufl., Heidelberg (u. a.) 2004; zitiert: *Schmidt-Aßmann*, Ordnungsidee.

Schmidt-Aßmann, Eberhard/Schoch, Friedrich (Hrsg.), Besonderes Verwaltungsrecht, 14. Aufl., Berlin 2008; zitiert: *Bearbeiter*, in: Schmidt-Aßmann/Schoch, BesVerwR.

Schmidt-Bleibtreu, Bruno/Hofmann, Hans/Hopfauf, Axel (Hrsg.), Grundgesetz-Kommentar, 11. Aufl., München (u. a.) 2008; zitiert: *Bearbeiter*, in: Schmidt-Bleibtreu/Hofmann/Hopfauf, GG.

Schmitt Glaeser, Walter/Horn, Hans-Detlef, Verwaltungsprozessrecht, 15. Aufl., Stuttgart (u. a.) 2000; zitiert: *Schmitt Glaeser/Horn*, Verwaltungsprozessrecht.

Schmitz, Heribert/Jastrow, Serge-Daniel, Das Informationsfreiheitsgesetz des Bundes, NVwZ 2005, S. 984 ff.

Schoch, Friedrich, Das Grundrecht der Informationsfreiheit, JURA 2008, S. 25 ff.

– Abschied vom Polizeirecht des liberalen Rechtsstaats? Vom Kreuzberg-Urteil des Preußischen Oberverwaltungsgerichts zu den Terrorismusbekämpfungsgesetzen unserer Tage, Der Staat 43 (2004), S. 347 ff.

– Das verwaltungsbehördliche Ermessen, JURA 2004, S. 462 ff.

– Informationsfreiheitsgesetz für die Bundesrepublik Deutschland, Die Verwaltung 35 (2002), S. 149 ff.

– Konvergenz der Medien – Sollte das Recht der Medien harmonisiert werden?, JZ 2002, S. 798 ff.

– Rechtsschutz gegen polizeiliche Maßnahmen, JURA 2001, S. 628 ff.

– Öffentlich-rechtliche Rahmenbedingungen einer Informationsordnung, VVDStRL 57 (1998), S. 158 ff.

– Privatisierung von Verwaltungsaufgaben, DVBl. 1994, S. 962 ff.

– Die Verfahrensgedanke im allgemeinen Verwaltungsrecht – Anspruch und Wirklichkeit nach 15 Jahren VwVfG, Die Verwaltung 25 (1992), S. 21 ff.

– Kommunalverfassungsstreit im System des verwaltungsgerichtlichen Rechtsschutzes, JuS 1987, S. 783 ff.

Schoch, Friedrich/Schmidt-Aßmann, Eberhard/Pietzner, Rainer (Hrsg.), Verwaltungsgerichtsordnung-Kommentar, München, Stand: Juli 2009; zitiert: *Bearbeiter*, in: Schoch/Schmidt-Aßmann/Pietzner, VwGO.

Scholz, Rupert, Zur Kostenerstattungspflicht des Staates für gesetzliche Maßnahmen der Telefonüberwachung, ArchPT 1995, S. 169 ff.

Schulze-Fielitz, Helmuth, Nach dem 11. September: An den Leistungsgrenzen eines verfassungsstaatlichen Polizeirechts?, in: Hans-Detlef Horn (Hrsg.), Recht im Pluralismus: Festschrift für Walter Schmitt Glaeser zum 70. Geburtstag, Berlin 2003, S. 407 ff.; zitiert: *Schulze-Fielitz*, in: Horn, FS Schmitt Glaeser.

Schwartmann, Rolf (Hrsg.), Praxishandbuch Medien-, IT- und Urheberrecht, Heidelberg 2008; zitiert: *Bearbeiter*, in: Schwartmann, Praxishandbuch.

Selmer, Peter, Die sogenannte „materielle Polizeipflicht" – Bemerkungen zu einer fragwürdigen Polizeirechtsfigur, in: Reinhard Hendler/Martin Ibler/José Martínez Soria (Hrsg.), Für Sicherheit, für Europa: Festschrift für Volkmar Götz zum 70. Geburtstag, Göttingen 2005, S. 391 ff.; zitiert: *Selmer*, in: Hendler/Ibler/Soria, FS Götz.

Sieber, Ulrich, Verantwortlichkeit im Internet, München 1999; zitiert: *Sieber*, Verantwortlichkeit.

– Die rechtliche Verantwortlichkeit im Internet – Grundlagen, Ziele und Auslegung von § 5 TDG und § 5 MDStV, MMR-Beilage 2/1999, S. 1 ff.

Siebrecht, Michael, Die polizeiliche Datenverarbeitung im Kompetenzstreit zwischen Polizei- und Prozessrecht, JZ 1996, S. 711 ff.

Sievers, Christopher, Telekommunikationsüberwachung in den Landespolizeigesetzen und der Strafprozessordnung, Kiel 2008; zitiert: *C. Sievers*, Telekommunikationsüberwachung.

Sievers, Malte, Der Schutz der Kommunikation im Internet durch Artikel 10 des Grundgesetzes, Baden-Baden 2003; zitiert: *M. Sievers*, Schutz der Kommunikation.

Simitis, Spiros (Hrsg.), Bundesdatenschutzgesetz, 6. Aufl., Baden-Baden 2006; zitiert: *Bearbeiter*, in: Simitis, BDSG.

Sodan, Helge (Hrsg.), Grundgesetz-Kommentar, München 2009; zitiert: *Bearbeiter*, in: Sodan, GG.

Sodan, Helge/Ziekow, Jan (Hrsg.), Verwaltungsgerichtsordnung-Kommentar, 2. Aufl., Baden-Baden 2006; zitiert: *Bearbeiter*, in: Sodan/Ziekow, VwGO.

Sodan, Helge/Kluckert, Sebastian, Die verwaltungsprozessuale Feststellungsfähigkeit von vergangenen und zukünftigen Rechtsverhältnissen, VerwArch. 94 (2003), S. 3 ff.

Son, Jae-Young, Heimliche polizeiliche Eingriffe in das informationelle Selbstbestimmungsrecht, Berlin 2006; zitiert: *Son*, Heimliche polizeiliche Eingriffe.

Spindler, Gerald/Ernst, Stefan, Vertragsgestaltung für den Einsatz von E-Mail-Filtern, CR 2004, S. 437 ff.

Starck, Christian, Neues zur Gesetzgebungskompetenz des Bundes kraft Sachzusammenhangs, in: Max-Emanuel Geis/Dieter Lorenz (Hrsg.), Staat, Kirche, Verwaltung: Festschrift für Hartmut Maurer zum 70. Geburtstag, München 2001, S. 281 ff.; zitiert: *Starck*, in: Geis/Lorenz, FS Maurer.

Starck, Christian (Hrsg.), Föderalismusreform, München 2007; zitiert: *Bearbeiter*, in: Starck, Föderalismusreform.

Staudenmayer, Cornelia, Der Verwaltungsvertrag mit Drittwirkung, Konstanz 1997; zitiert: *Staudenmayer*, Verwaltungsvertrag.

Steiner, Udo (Hrsg.), Besonderes Verwaltungsrecht, 8. Aufl., Heidelberg 2006; zitiert: *Bearbeiter*, in: Steiner, BesVerwR.

– Verwaltungsverfahren und Grundrechte, NZS 2002, S. 113 ff.

– Die allgemeine Leistungsklage im Verwaltungsprozess, JuS 1984, S. 853 ff.

Stelkens, Paul/Bonk, Heinz Joachim/Sachs, Michael (Hrsg.), Verwaltungsverfahrensgesetz-Kommentar, 7. Aufl., München 2008; zitiert: *Bearbeiter*, in: Stelkens/Bonk/Sachs, VwVfG.

Stephan, Ulrich, Zur Verfassungsmäßigkeit der präventiven Telefonüberwachung gem. § 33a Abs. 1 Nr. 2 und 3 Nds.SOG, VBlBW 2005, S. 410 ff.

Stern, Klaus, Das Staatsrecht der Bundesrepublik Deutschland, Bd. IV/1, München 2006; zitiert: *Bearbeiter*, in: Stern, Staatsrecht, Bd. IV/1.

– Die Grundrechte und ihre Schranken, in: Peter Badura/Horst Dreier (Hrsg.), Festschrift 50 Jahre BVerfG, Bd. 2, Tübingen 2001, S. 1 ff.; zitiert: *Stern*, in: Badura/Dreier, FS BVerfG.

– Das Staatsrecht der Bundesrepublik Deutschland, Bd. III/2, München 1994; zitiert: *Stern*, Staatsrecht, Bd. III/2.

– Das Staatsrecht der Bundesrepublik Deutschland, Bd. I, 2. Aufl., München 1984; zitiert: *Stern*, Staatsrecht, Bd. I.

– Das Staatsrecht der Bundesrepublik Deutschland, Bd. II, München 1980; zitiert: *Stern*, Staatsrecht, Bd. II.

Stettner, Rupert, Grundfragen einer Kompetenzlehre, Berlin 1983; zitiert: *Stettner*, Kompetenzlehre.

Stober, Rolf, Beiladung im Verwaltungsprozess, in: Hans-Uwe Erichsen (Hrsg.), System des Verwaltungsgerichtlichen Rechtsschutzes: Festschrift für Christian-Friedrich Menger zum 70. Geburtstag, München (u. a.) 1985, S. 401 ff.; zitiert: *Stober*, in: Erichsen, FS Menger.

Störing, Marc, Strafprozessuale Zugriffsmöglichkeiten auf E-Mail-Kommunikation, Berlin 2007; zitiert: *Störing*, Strafprozessuale Zugriffsmöglichkeiten.

Stuible-Treder, Jutta, Die Beliehene im Verwaltungsrecht, Tübingen 1986; zitiert: *Stuible-Treder*, Die Beliehene.

Sturm, Gerd, Probleme eines Verzichts auf Grundrechte, in: Gerhard Leibholz/Hans Joachim Faller/Paul Mikat/Hans Reis (Hrsg.), Menschenwürde und freiheitliche Rechtsordnung, Festschrift für Willi Geiger zum 65. Geburtstag, Tübingen 1974, S. 173 ff.; zitiert: *Sturm*, in: Leibholz/Faller/Mikat/Reis, FS Geiger.

Terhechte, Jörg Philipp, Rechtsangleichung zwischen Gemeinschafts- und Unionsrecht – die Richtlinie über die Vorratsdatenspeicherung vor dem EuGH, EuZW 2009, S. 199 ff.

Tettinger, Peter J./Erbguth, Wilfried/Mann, Thomas, Besonderes Verwaltungsrecht, 10. Aufl., Heidelberg 2009; zitiert: *Tettinger/Erbguth/Mann*, BesVerwR.

Tettinger, Peter J./Wank, Rolf, Gewerbeordnung-Kommentar, 7. Aufl., München 2004; zitiert: *Tettinger/Wank*, GewO.

Tischer, Birgit, Das System der informationellen Befugnisse der Polizei, Frankfurt am Main 2004; zitiert: *Tischer*, System der informationellen Befugnisse.

Trute, Hans-Heinrich, Grenzen des präventionsorientierten Polizeirechts in der Rechtsprechung des Bundesverfassungsgerichts, Die Verwaltung 42 (2009), S. 85 ff.

– Die Erosion des klassischen Polizeirechts durch die polizeiliche Informationsvorsorge, in: Wilfried Erbguth/Friedrich Müller/Volker Neumann (Hrsg.), Rechtstheorie und Rechtsdogmatik im Austausch: Gedächtnisschrift für Bernd Jeand'Heur, Berlin 1999, S. 403 ff.; zitiert: *Trute*, in: Erbguth/Müller/Neumann, GS Jeand'Heur.

– Öffentlich-rechtliche Rahmenbedingungen einer Informationsordnung, VVDStRL 57 (1998), S. 216 ff.

Vahle, Jürgen, Polizeiliche Aufklärungs- und Observationsmaßnahmen (unter Berücksichtigung der Tätigkeit des Verfassungsschutzes), Bielefeld 1983; zitiert: *Vahle*, Aufklärungs- und Observationsmaßnahmen.

Vogel, Klaus, Öffentliche Wirtschaftseinheiten in privater Hand, Hamburg 1959; zitiert: *Vogel*, Öffentliche Wirtschaftseinheiten.

Volkmann, Uwe, Die Rückeroberung der Allmende, NVwZ 2000, S. 361 ff.

Voßkuhle, Andreas, Beteiligung Privater an der Wahrnehmung öffentlicher Aufgaben und staatliche Verantwortung, VVDStRL 62 (2003), S. 266 ff.

– Der Wandel von Verwaltung und Verwaltungsprozessrecht in der Informationsgesellschaft, in: Wolfgang Hoffmann-Riem/Eberhard Schmidt-Aßmann, Verwaltungsrecht in der Informationsgesellschaft, Baden-Baden 2000, S. 349 ff.; zitiert: *Voßkuhle*, in: Hoffmann-Riem/Schmidt-Aßmann, Informationsgesellschaft.

Waechter, Kay, Die aktuelle Situation des Polizeirechts, JZ 2002, S. 854 ff.

– Die „Schleierfahndung" als Instrument der indirekten Verhaltenssteuerung, DÖV 1999, S. 138 ff.

– Polizeiliches Ermessen zwischen Planungsermessen und Auswahlermessen, VerwArch 88 (1997), S. 298 ff.

– Die Schutzgüter des Polizeirechts, NVwZ 1997, S. 729 ff.

– Bereitstellungspflicht für Fernmeldeanlagenbetreiber, VerwArch 87 (1996), S. 68 ff.

Wahl, Rainer/Appel, Ivo, Prävention und Vorsorge: Von der Staatsaufgabe zur rechtlichen Ausgestaltung, in: Rainer Wahl (Hrsg.), Prävention und Vorsorge, Bonn 1995, S. 1 ff.; zitiert: *Wahl/Appel*, in: Wahl, Prävention und Vorsorge.

Wandtke, Artur-Axel (Hrsg.), Medienrecht Praxishandbuch, Berlin 2008; zitiert: *Bearbeiter*, in: Wandtke, Medienrecht Praxishandbuch.

Warg, Gunter, Auskunftsbefugnisse der Strafverfolgungsbehörden und Anonymität des E-Mail-Anzeigeerstatters, MMR 2006, S. 77 ff.

West, Christian, Der genetische Fingerabdruck als erkennungsdienstliche Standardmaßnahme der Strafverfolgungsvorsorge und die Verwendung des genetischen Phantombildes im Strafverfahren, Stuttgart (u. a.) 2007; zitiert: *West*, Fingerabdruck.

Willer, Christoph/Hoppen, Peter, Computerforensik – Technische Möglichkeiten und Grenzen, CR 2007, S. 610 ff.

Wilms, Heiner/Jäger, York, Menschenwürde und Tötung auf Verlangen, ZRP 1988, S. 41 ff.

Wolf, Heinz/Stephan, Ulrich/Deger, Johannes, Polizeigesetz für Baden-Württemberg Kommentar, 6. Aufl., Stuttgart (u. a.) 2009; zitiert: *Bearbeiter*, in: Wolf/Stephan/Deger, PolG BW.

Wolff, Hans J./Bachof, Otto/Stober, Rolf/Kluth, Winfried/Müller, Martin, Verwaltungsrecht, Bd. 3, 5. Aufl., München 2004; zitiert: *Bearbeiter*, Wolff/Bachof/Stober/Kluth/Müller, VerwR, Bd. 3.

Würtenberger, Thomas, Verwaltungsprozessrecht, 2. Aufl., München 2006; zitiert: *Würtenberger*, Verwaltungsprozessrecht.

Würtenberger, Thomas/Heckmann, Dirk, Polizeirecht in Baden-Württemberg, 6. Aufl., Heidelberg 2005; zitiert: *Würtenberger/Heckmann*, PolR BW.

Wuttke, Alexander, Polizeirecht und Zitiergebot, Hamburg 2004; zitiert: *Wuttke*, Polizeirecht und Zitiergebot.

Ziekow, Jan, Öffentliches Wirtschaftsrecht, 2007; zitiert: *Ziekow*, Öffentliches Wirtschaftsrecht.

– Verwaltungsverfahrensgesetz-Kommentar, Stuttgart (u. a.) 2006; zitiert: *Ziekow*, VwVfG.

Zimmermann, Andreas, Polizeiliche Gefahrenabwehr und das Internet, NJW 1999, S. 3145 ff.

Zippelius, Reinhold/Würtenberger, Thomas, Deutsches Staatsrecht, 32. Aufl., München 2008; zitiert: *Zippelius/Würtenberger*, Staatsrecht.